

BAB I

PENDAHULUAN

A. Latar Belakang

Saat ini kehidupan manusia telah memasuki era transisi menuju “Revolusi Industri 5.0,” suatu era yang menekankan pembangunan sistem yang cerdas, saling terhubung, dan berpusat pada manusia.¹ Revolusi ini bertujuan untuk mengintegrasikan kemampuan manusia dengan kecerdasan mesin melalui pemanfaatan teknologi, seperti *Internet of Things* (IoT), data besar (*big data*), dan kecerdasan buatan atau yang biasa disebut dengan *Artificial Intelligence* (AI).² Jamie Susskind berpendapat bahwa kemajuan teknologi menghasilkan suatu fenomena dimana masyarakat saling terkoneksi secara langsung dan menciptakan suatu dimensi baru yang dikenal sebagai dunia digital.³ Salah satu bentuk dari kemajuan teknologi tersebut adalah *Face Recognition Technology* (FRT).⁴

FRT merupakan sebuah teknologi yang dirancang secara otomatis melalui sistem AI⁵ untuk mengenali individu berdasarkan setiap fitur di wajah mereka yang berguna untuk mengidentifikasi atau memverifikasi diri mereka.⁶ Teknologi ini secara

¹ Tangkas Ageng Nugroho, et al, 2023, “Perkembangan Revolusi Industri 5.0 Dalam Perekonomian Indonesia”, *Manajemen Kreatif Jurnal (MAKREJU)*, Vol. 1, No. 3. hlm. 96.

² *Artificial Intelligence* adalah sistem computer yang bersifat buatan yang mampu beroperasi dengan cara yang dianggap cerdas karena meniru karakteristik yang telah disebutkan sebelumnya terkait perilaku manusia yang cerdas. Lihat, Bruno Zulehner, 2024, “EU Artificial Intelligence Act: Regulating the Use of Facial Recognition Technologies in Publicly Accessible Spaces,” Tesis Magister University of Vienna, Vienna, hlm. 5.

³ Jamie Susskind, 2022, *The Digital Republic: On Freedom and Democracy in the 21st Century*, New York: Pegasus Books, hlm. 8.

⁴ World Economic Forum, “A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigation,” [Investigations 2022.pdf](#), diakses 25 Januari 2026 pukul 20.45.

⁵ Sistem AI adalah mesin yang dapat belajar dan menyesuaikan diri untuk membuat prediksi, rekomendasi, atau keputusan yang memengaruhi dunia nyata maupun digital. Lihat *Article 3 (1) Artificial Intelligence Act*.

⁶ European Data Protection Board, 2023, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, Versi 1.0, European Data Protection Board, Uni Eropa. Hlm. 10.

otomatis dapat membandingkan karakteristik wajah yang teridentifikasi dalam foto atau rekaman video dengan ribuan wajah yang telah dikumpulkan sebelumnya dalam sebuah basis data (*data base*).⁷ Pengaplikasian AI dalam FRT memungkinkan identifikasi yang lebih cepat dan akurat, terutama dalam kondisi pencahayaan buruk atau target yang terhalang. Dikarenakan FRT menggunakan karakteristik fisik unik manusia (ciri wajah) sebagai acuan untuk identifikasi/verifikasi, teknologi ini termasuk dalam kategori teknologi yang menggunakan sebuah data yang disebut “data biometrik”.

Secara regional, data biometrik telah diatur dalam (EU) *General Data Protection Regulation* (GDPR) dan (EU) *Artificial Intelligence Act* (AI Act). *Article 4* (14) GDPR dan *Article 3* (34) AI Act yang memuat definisi yang sama mengenai data biometrik, menyatakan bahwa data biometrik adalah:

“‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;”

Menurut terjemahan bebas penulis maksud dari *Article 4* (14) GDPR dan *Article 3* (34) AI Act adalah:⁸

“data biometrik berarti “data pribadi” yang diperoleh dari pemrosesan teknis tertentu yang berkaitan dengan karakteristik fisik, fisiologis atau perilaku seseorang yang memungkinkan atau mengonfirmasi identifikasi orang tersebut, seperti citra wajah atau sidik jari.”

Dengan demikian, data biometrik dapat dipahami sebagai informasi yang mencakup karakteristik mendasar seseorang, termasuk, gambar wajah, sidik jari, pemindaian iris, pengenalan suara, atau tanda tangan.⁹

⁷ Dalam konteks *Face Recognition Technology*, *database* merupakan tempat penyimpanan data wajah yang tersusun rapi dan digunakan untuk mencocokkan wajah seseorang guna mengenali atau memastikan identitas seseorang.

⁸ Diterjemahkan secara bebas oleh Penulis dengan bantuan *Artificial Intelligence DeepL Translator*.

⁹ *Article 4* (14) *General Data Protection Regulation* dan *Article 3* (34) AI Act

Memasuki abad ke-21, penggunaan FRT berkembang sangat pesat dalam beberapa tahun terakhir dikarenakan adanya AI. FRT banyak digunakan dalam sektor kehidupan, seperti di sektor industri, ritel, transportasi, hingga penegakan hukum. Di Inggris, maskapai penerbangan menerapkan FRT untuk verifikasi identitas penumpang penerbangan dari Amerika Serikat yang memungkinkan *boarding* tanpa paspor atau tiket.¹⁰ Kemudian, dalam penegakan hukum, FRT digunakan untuk mengidentifikasi tersangka, pencarian saksi, menemukan orang yang hilang, serta verifikasi identitas tersangka yang sudah ditangkap, tapi menolak untuk memberikan data pribadi mereka.¹¹

Penggunaan FRT yang kian masif dalam berbagai aspek kehidupan membawa kompleksitas persoalan hukum dan etika, khususnya terkait perlindungan data pribadi.¹² Perlindungan data pribadi merupakan suatu proses untuk melindungi data pribadi yang sensitif, menjaga privasi dan memastikan bahwa informasi yang melekat pada diri seseorang tidak mengalami berbagai tindakan yang berpotensi melanggar hak privasi seseorang.¹³ Namun demikian, perlindungan tersebut menghadapi ancaman yang nyata dalam setiap tahapan mekanisme FRT. Pada tahap awal, yakni *capturing*, sistem secara otomatis mengumpulkan citra wajah melalui kamera CCTV maupun melalui *untargeted scraping*¹⁴ dari media sosial dan situs web. Praktik pengambilan

¹⁰ Kaspersky Lab, “What is Facial Recognition-Definition and Explanation,” What is Facial Recognition & How does it work?, diakses pada tanggal 23 September 2025 pukul 08.33.

¹¹ Engineering National Academies of Sciences and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* (Washington, DC: The National Academies Press, 2024), <https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance>. hlm. 24.

¹² GDPR ADVISOR, “GDPR and Facial Recognition: Privacy Implications and Legal Considerations”, GDPR and Facial Recognition: Privacy Implications and Legal Considerations - GDPR Advisor, diakses pada tanggal 23 September 2025 pukul 08.50.

¹³ GDPR LOCAL, “What is Data Protection? Its Importance and Benefits,” What is Data Protection? Its Importance and Benefits - GDPR Local, Diakses pada tanggal 4 Mei 2026, pukul 15.02.

¹⁴ *Untargeted scraping* adalah pengambilan data wajah secara massal tanpa tujuan khusus menggunakan program otomatis dari berbagai situs web atau media sosial untuk keperluan pengenalan wajah. Lihat Bundesnetzagentur, “Prohibited Practices,” Bundesnetzagentur - Prohibited practices, diakses pada tanggal 23 September 2025 pukul 09.45.

data tanpa persetujuan ini memicu ancaman pengawasan massal (*mass surveillance*)¹⁵ yang dapat mengikis privasi dan perlindungan terhadap data pribadi.¹⁶

Setelah citra wajah didapatkan, sistem memasuki tahap ekstraksi fitur wajah yang mengidentifikasi ciri khas geometris wajah untuk kemudian dicocokkan dengan *database*, risiko terhadap perlindungan data pribadi semakin krusial karena citra wajah yang diekstrak adalah data biometrik yang dikategorikan sebagai data pribadi kategori khusus untuk dilindungi. Tahapan-tahapan ini bermuara pada proses pencocokan dimana FRT mengeluarkan *output* berupa verifikasi atau identifikasi identitas seseorang. Dalam tahap pencocokan ini, FRT berisiko menghasilkan kesimpulan yang bias dan diskriminatif. Hal ini dikarenakan algoritma pencocokan wajah pada FRT yang sering kali tidak akurat dan rentan mengalami kegagalan identifikasi, terutama terhadap kelompok minoritas etnis atau ras tertentu.¹⁷

Uni Eropa (EU) telah merespon tantangan perlindungan data pribadi dengan menerapkan GDPR, regulasi ini berfokus pada perlindungan data seseorang dan pemrosesan data yang sah.¹⁸ Dalam GDPR, data biometrik termasuk kategori data pribadi khusus sebagaimana diatur dalam *Article 9 (1)*, sepanjang data tersebut diproses dengan tujuan untuk mengidentifikasi seseorang dan mengungkapkan aspek-

¹⁵ *Mass surveillance* adalah praktik pengawasan yang dilakukan secara luas terhadap seluruh populasi atau masyarakat, praktik ini biasanya digunakan oleh pemerintah untuk memantau aktivitas, komunikasi, dan perilaku masyarakat secara sistematis. Lihat Sinisa Domazet, “*Mass Surveillance and Private Companies*”, dipresentasikan pada IX International Scientific Professional Conference Security and Crisis Management – Theory and Practice (SecMan) dalam rangka IX International Forum “Safety for the Future”, Belgrade, Republik Serbia, 29 - 30 September 2023. hlm. 46.

¹⁶ Gizem Gültekin-Várkonyi, 2024, “*Facial Recognition Technologies, AI Act and GDPR: A Short Risk-Based Evaluation*”, *Constitutional Discourse*.” <https://constitutionaldiscourse.com/facial-recognition-technologies-ai-act-and-gdpr-a-short-risk-based-evaluation/>, diakses pada tanggal 23 September 2025, pukul 09.12 .

¹⁷ 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(3), 377–387. <https://doi.org/10.1007/s43681-021-00077-w>. hlm. 379.

¹⁸ Gizem Gültekin-Várkonyi, *Loc. cit.*

aspek, seperti asal ras atau etnis, pendapat politik, keyakinan agama, dan berbagai aspek lainnya dari seseorang.¹⁹

Kategori ini, mempertegas bahwa citra dan fitur wajah yang diproses melalui FRT termasuk ke dalam kategori data pribadi yang dilindungi. Oleh karena itu, penggunaannya berpotensi mengurangi kendali atas identitasnya sendiri setiap kali data wajah diperoleh baik dengan paksaan, bujukan, maupun dengan persetujuan individu tersebut.²⁰

Pengaturan mengenai perlindungan data pribadi dalam GDPR tidak hanya terbatas pada aspek defisional, akan tetapi juga menekankan prinsip dan hak fundamental dalam pemrosesan data pribadi yang dirancang untuk melindungi hak individu. Selain itu, GDPR juga melarang pemrosesan data biometrik untuk tujuan mengidentifikasi seseorang secara unik, kecuali dalam kondisi tertentu seperti adanya persetujuan eksplisit dari subjek data atau kepentingan publik yang substansial.²¹ Terakhir, salah satu aspek paling signifikan yang diatur dalam GDPR adalah penerapannya terhadap entitas asing. *Article 3* GDPR menetapkan bahwa regulasi ini tidak hanya kepada organisasi yang berbasis di EU, tetapi juga berlaku bagi organisasi ataupun negara yang berada di luar wilayah EU apabila mereka menawarkan barang atau jasa kepada individu di EU, atau memantau perilaku mereka. Ini berarti setiap perusahaan asing yang mengumpulkan data pribadi dari warga EU tetap tunduk pada GDPR.

Menyadari bahwa GDPR saja tidak cukup untuk menangani kompleksitas dan risiko spesifik yang ditimbulkan oleh AI, pada bulan Juni 2024, EU mengadopsi

¹⁹ Nessa Lynch, 2024, “*Facial Recognition Technology in Policing and Security – Case Studies in Regulation*”, Laws, hlm. 2.

²⁰ Nasakti Ghazali, 2021, *Op. cit.*, hlm. 356. a

²¹ DLA PIPER “*Europe: The EU AI Act’s relationship with data protection law: key takeaways*,” <https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/>, diakses pada tanggal 23 September 2025 pukul 09.12 WIB.

Artificial Intelligence Act (AI Act) sebagai kerangka hukum pertama di dunia yang mengatur AI secara komprehensif dan berfokus untuk menciptakan AI yang dapat dipercaya berdasarkan data yang diproses secara sah.²² AI Act tidak menggantikan GDPR, melainkan melengkapinya dalam memberikan perlindungan data pribadi. Apabila GDPR berfokus pada keabsahan pemrosesan data pribadi, termasuk data biometrik, beserta hak-hak subjek data, AI Act berfokus pada pengaturan sistem AI melalui pendekatan berbasis risiko dengan menetapkan persyaratan mengenai tata kelola data, transparansi, pengawasan manusia, dan manajemen risiko. Dengan demikian, dalam penggunaan FRT, GDPR dan AI Act diterapkan secara bersamaan sehingga membentuk kerangka perlindungan data pribadi yang saling melengkapi.²³

Menurut terjemahan bebas penulis,²⁴ yang dikutip dari pendapat EU Artificial Intelligence Act dalam artikelnya yang berjudul “*High-level summary of the AI Act*” yang menyatakan bahwa *Article 5* AI Act menggunakan pendekatan berbasis risiko yang mengklarifikasikan sistem AI yang dilarang dalam beberapa kategori sebagai berikut:²⁵

- (i) “Sistem AI yang menggunakan teknik-teknik subliminal, manipulatif, atau menipu untuk memengaruhi perilaku dan mengganggu pengambilan keputusan yang tepat, sehingga menyebabkan kerugian yang signifikan;
- (ii) *Exploiting vulnerabilities*. Sistem AI yang memanfaatkan kelemahan yang berkaitan dengan usia, disabilitas, atau keadaan sosial ekonomi untuk memengaruhi perilaku, sehingga menimbulkan kerugian yang signifikan;
- (iii) *Biometric categorisation system*. Sistem AI yang menyimpulkan atribut sensitif (ras, pendapat politik, keanggotaan serikat pekerja, keyakinan agama atau filosofis, kehidupan seksual, atau orientasi seksual), kecuali penandaan

²² Topics European Parliament, “*EU AI Act; first regulation on artificial intelligence*,” EU AI Act: first regulation on artificial intelligence | Topics | European Parliament, diakses pada tanggal 23 September 2025 PUKUL 09.30.

²³ GDPR.LOCAL, “How the EU AI Act Complements GDPR: A Compliance Guide,” How the EU AI Act Complements GDPR: A Compliance Guide - GDPR Local, Diakses pada tanggal 1 Agustus 2026, pukul 16.31.

²⁴ Diterjemahkan secara bebas oleh Penulis dengan bantuan *Artificial Intelligence DeepL* Translator.

²⁵ EU Artificial Intelligence Act, “*High-level summary of the AI Act*,” https://artificialintelligenceact.eu/high-level-summary/#weglot_switcher, diakses pada tanggal 23 September 2025 pukul 09.35.

- atau penyaringan dataset biometrik yang diperoleh secara sah atau ketika penegak hukum mengkategorikan data biometrik;
- (iv) *Social scoring*. Sistem AI yang mengevaluasi atau mengklasifikasikan individu atau kelompok berdasarkan perilaku sosial atau ciri pribadi, yang menyebabkan perlakuan merugikan atau tidak menguntungkan bagi orang-orang tersebut;
 - (v) *Assessing the risk of an individual committing criminal offenses*. Sistem AI yang melakukan penilaian risiko seseorang melakukan tindak pidana hanya berdasarkan profil atau ciri kepribadian, kecuali ketika digunakan untuk melengkapi penilaian manusia berdasarkan fakta objektif dan terverifikasi yang langsung terkait dengan aktivitas kriminal;
 - (vi) *Compiling facial recognition databases*. Sistem AI yang membuat basis data pengenalan wajah melalui pengumpulan acak gambar wajah dari internet atau rekaman CCTV;
 - (vii) *Inferring emotions in workplaces or educational institutions*. Sistem AI yang melakukan penyimpulan emosi di tempat kerja atau lembaga pendidikan, kecuali untuk alasan medis atau keamanan;
 - (viii) *'Real time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement*. Sistem AI yang melakukan identifikasi biometrik jarak jauh (RBI) secara *real-time* di ruang publik yang dapat diakses oleh masyarakat untuk penegakan hukum, kecuali dalam hal tertentu yang diatur dalam AI Act.”

Dalam kerangka ini, FRT secara umum dikategorikan sebagai *Compiling facial recognition databases* dan *RBI in publicly accessible spaces for law enforcement*, penggunaannya bahkan dapat dilarang terutama jika digunakan untuk pengawasan massal (*mass surveillance*).²⁶ AI Act secara eksplisit melarang *untargeted scraping* gambar wajah dari internet atau rekaman CCTV untuk membangun atau memperluas basis data pengenalan wajah. Selain itu, AI Act menekankan prinsip-prinsip, seperti transparansi, akurasi, dan pengawasan manusia yang melengkapi GDPR dengan fokus pada pengelolaan risiko sistem AI itu sendiri.²⁷

Keberadaan GDPR dan AI Act menunjukkan bahwa Uni Eropa telah memiliki kerangka hukum yang mengatur perlindungan data pribadi dan penggunaan sistem kecerdasan buatan, termasuk dalam penggunaan FRT. Meskipun demikian, penerapan

²⁶ Gizem Gültekin-Várkonyi, *Loc. cit.*

²⁷ Marc Schuler, *Et Al.* “How the EU AI Act Supplements GDPR in the Protection of Personal Data,” <https://www.inta.org/perspectives/features/how-the-eu-ai-act-supplements-gdpr-in-the-protection-of-personal-data/>, diakses pada tanggal 23 September 2025 pukul 09.48.

kedua regulasi tersebut dalam praktik masih menimbulkan berbagai persoalan, terutama ketika FRT digunakan untuk mengumpulkan dan memproses data biometrik dalam skala besar oleh entitas yang beroperasi lintas yurisdiksi. Kondisi tersebut menimbulkan pertanyaan mengenai bagaimana ketentuan GDPR dan AI Act diterapkan terhadap penggunaan FRT serta sejauh mana kedua regulasi tersebut mampu memberikan perlindungan terhadap data pribadi. Salah satu contoh penerapan kedua regulasi tersebut dapat dilihat dalam kasus lintas yurisdiksi yang dilakukan oleh salah 1 perusahaan teknologi di Amerika Serikat.

Kasus lintas yurisdiksi dalam penggunaan FRT dapat dilihat dalam kasus Clearview AI Inc. Kasus Clearview AI Inc. berawal dari penyelidikan otoritas perlindungan data Belanda (*Autoriteit Persoonsgegevens* atau disebut AP) yang menerima laporan tentang pemantauan biometrik terhadap warga negara Belanda dan kepemilikan basis data wajah skala besar, yang berisi sekitar 10 miliar citra wajah dari sumber publik online seperti Twitter, Facebook, dan YouTube melalui teknik *web scraping*.²⁸ Clearview AI Inc. merupakan perusahaan swasta asal Amerika Serikat, mengembangkan platform pengenalan wajah berbasis *web scraping*²⁹ untuk membantu lembaga pemerintah dalam investigasi, namun AP menemukan bahwa praktik tersebut mengumpulkan data pribadi, termasuk data biometrik dan lokasi warga Belanda, secara tidak sah tanpa dasar hukum yang memadai dan tanpa menunjuk perwakilan di wilayah EU.

Keputusan AP Belanda pada tanggal 16 Mei 2024 menyatakan bahwa Clearview AI telah melanggar prinsip-prinsip yang terdapat pada *Article 5 (1) GDPR*, khususnya prinsip keabsahan, keadilan, dan transparansi, serta berpotensi melanggar

²⁸ Bo Zhao, 2017, "Web Scraping", dalam *Encyclopedia of Big Data*, Springer International Publishing AG, 2017, hlm. 1.

²⁹ *Web scraping* merupakan sebuah teknik untuk mengekstrak data dari *World Wide Web* dan menyimpannya dalam sistem dokumen atau database untuk dapat dianalisis. *Ibid.*

prinsip-prinsip GDPR lainnya. Selain itu, Clearview AI melanggar *Article 9 (1)* GDPR yang melarang pemrosesan data biometrik untuk keperluan identifikasi unik seseorang tanpa dasar hukum khusus. Lebih lanjut, praktik pengumpulan miliaran gambar wajah dari internet untuk membangun *database* pengenalan wajah berpotensi melanggar AI Act, karena AI Act secara eksplisit melarang sistem AI yang menciptakan atau memperluas basis data wajah melalui pengumpulan tanpa sasaran (*untargeted scraping*) sebagai sistem berisiko tidak dapat diterima. Kasus ini menimbulkan pertanyaan mengenai bagaimana GDPR dan AI Act dapat diterapkan terhadap entitas non-EU yang beroperasi lintas yurisdiksi, serta sejauh mana standar perlindungan data EU dapat dijadikan rujukan bagi negara lain yang belum memiliki kerangka regulasi yang setara.

Penggunaan FRT menawarkan manfaat transformatif di berbagai sektor, tetapi juga membawa risiko serius terhadap privasi, terutama dalam hal perlindungan data pribadi. Meskipun EU telah merespon tantangan ini melalui dua regulasi utama, yaitu GDPR yang berfokus pada perlindungan data pribadi dan AI Act yang secara khusus dirancang untuk mengatur sistem AI berdasarkan tingkat risikonya. Namun, kasus Clearview AI Inc. menunjukkan bahwa penggunaan FRT dapat menimbulkan persoalan hukum, khususnya berkaitan dengan pemrosesan data biometrik dan penerapan regulasi terhadap entitas yang beroperasi lintas yurisdiksi. Oleh karena itu, penting untuk mengkaji bagaimana ketentuan dalam GDPR dan AI Act diterapkan terhadap penggunaan FRT, serta sejauh mana kedua regulasi tersebut memberikan perlindungan terhadap data pribadi dalam praktik. Berdasarkan uraian latar belakang di atas, penulis tertarik untuk mengkaji dan membahas mengenai

“PERLINDUNGAN DATA PRIBADI DALAM PENGGUNAAN TEKNOLOGI PEMINDAIAN WAJAH (*FACE RECOGNITION TECHNOLOGY*) DITINJAU

DARI (EU) *GENERAL DATA PROTECTION REGULATION* DAN (EU) *ARTIFICIAL INTELLIGENCE ACT*”

B. Rumusan Masalah

1. Bagaimana pengaturan *FaceRecognition Technology* menurut (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act*?
2. Bagaimana perlindungan data pribadi terhadap risiko penggunaan *Face Recognition Technology* menurut (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act*?

C. Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka dapat dirumuskan beberapa tujuan dari penelitian ini, yaitu:

1. Untuk meneliti dan membahas pengaturan *Face Recognition Technology* terhadap pengambilan data biometrik menurut (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act*.
2. Untuk meneliti dan membahas perlindungan data pribadi terhadap risiko penggunaan *Face Recognition Technology* menurut (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act*.

D. Manfaat Penelitian

Berdasarkan tujuan penelitian, diharapkan penelitian ini tidak hanya memberikan manfaat bagi para pembaca, namun juga manfaat lainnya, baik secara langsung maupun tidak langsung. Adapun manfaat tersebut dijabarkan sebagai berikut:

1. Manfaat Teoritis.
 - a. Untuk menambah ilmu pengetahuan dan wawasan serta melatih kemampuan penulis dalam melakukan penulisan karya ilmiah khususnya mengenai hukum internasional, yang diharapkan dapat menjadi referensi bagi sesama

mahasiswa, dosen, dan masyarakat yang tertarik dengan permasalahan yang dikaji.

- b. Dapat memberikan, menambah pemahaman, serta memperluas pengetahuan wawasan pemikiran mengenai penggunaan FRT dalam sudut pandang (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act*.
- c. Dapat memberikan pemahaman dasar dan suatu sikap kritis terhadap regulasi yang berkaitan dengan FRT secara internasional.

2. Secara praktis

- a. Bagi penulis, diharapkan hasil penelitian ini dapat menambah dan memperluas wawasan penulis, serta menambah ilmu pengetahuan mengenai pengaturan FRT dan tindakan pengambilan data biometrik pada kasus Clearview AI dilihat dari (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act*.
- b. Bagi Universitas Andalas, hasil penelitian ini dapat menambah koleksi Pustaka dan bahan bacaan bagi Mahasiswa/I Fakultas Hukum khususnya Program Kekhususan Internasional mengenai pengaturan FRT dan bentuk perlindungan data pribadi terhadap risiko penggunaan *Face Recognition Technology* menurut (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act*.

E. Metode Penelitian

Metode adalah suatu proses, yaitu suatu rangkaian langkah-langkah yang mendapatkan jawaban terhadap pertanyaan-pertanyaan tertentu.³⁰ Sementara itu, penelitian merupakan suatu kegiatan ilmiah yang didasarkan pada metode, sistematis

³⁰ Sumandi Suryabrata, 1995, *Metodelogi Penelitian*, Jakarta: Raja Gafindo Persada, hlm.69.

dan pemikiran tertentu yang bertujuan untuk mempelajari suatu atau beberapa gejala hukum tertentu dengan menganalisa.³¹

Menurut Sugiyono, metode penelitian merupakan cara-cara ilmiah guna mendapatkan data valid, yang bertujuan dapat ditemukan, dikembangkan, dan dibuktikan suatu pengetahuan tertentu, sehingga pada saatnya dapat digunakan untuk memahami, memecahkan, dan mengantisipasi masalah.³² Adapun metode penelitian yang digunakan penulis dalam penelitian ini adalah sebagai berikut:

1. Jenis Penelitian

Jenis penelitian yang akan dalam penulisan hukum ini adalah penelitian hukum normatif. Penelitian ini menggunakan metode penelitian yuridis normatif, yaitu pendekatan yang dilakukan dengan cara menelaah pendekatan teori-teori atau konsep-konsep, mengkaji peraturan perundang-undangan. Dalam penelitian ini, peraturan perundang-undangan yang akan dikaji adalah ketentuan-ketentuan yang ada dalam (*EU General Data Protection Regulation* dan (*EU Artificial Intelligence Act* yang berkaitan dengan *Face Recognition Technology* dalam lingkup kawasan Uni Eropa.³³

2. Pendekatan Penelitian

Dalam rangka menjawab rumusan masalah penelitian, penulis menggunakan tiga pendekatan permasalahan, yaitu Pendekatan Perundang-undangan, Pendekatan Konseptual dan Pendekatan Kasus. Ada pun penjelasan mengenai pendekatan tersebut, yaitu sebagai berikut:

³¹ Soerjono Soekanto dan Sri Mamudji, 2018, *Penelitian Ilmu Hukum Normatif Suatu Tinjauan Singkat*, PT. Raja Grafindo Persada: Jakarta, hlm.13.

³² Ikah Atikah, 2022, *Metode Penelitian Hukum*, Sukabumi: CV. Haura Utama, hlm. 6.

³³ Pujiati. "*Metode Penelitian Yuridis Normatif di Bidang Hukum*". *Metode Penelitian Yuridis Normatif di Bidang Hukum*, diakses pada tanggal 15 Oktober 2025 pukul 13.45.

a. Pendekatan Perundang-Undangan

Pendekatan ini merupakan pendekatan yang dilakukan dengan cara menelaah dan menganalisis peraturan perundang-undangan, dimana peraturan yang penulis gunakan dalam penelitian ini adalah (EU) *General Data Protection Regulation* dan (EU) *Artificial Intelligence Act* yang bersangkutan paut dengan isu hukum yang sedang ditangani.³⁴

b. Pendekatan Kasus

Pendekatan kasus adalah pendekatan yang dilakukan dengan cara melakukan telaah terhadap kasus-kasus yang berkaitan dengan masalah yang dihadapi. Pendekatan ini bertujuan untuk mempelajari penerapan norma-norma atau kaidah hukum yang digunakan dalam praktik.³⁵ Dalam penelitian ini penulis menggunakan Kasus Clearview AI Inc. sebagai bentuk pendekatan penelitian untuk menjawab rumusan masalah kedua.

c. Pendekatan Konseptual (*conceptual approach*)

Peter Mahmud Marzuki menjelaskan bahwa yang dimaksud dengan pendekatan konseptual adalah pendekatan yang dilakukan manakala peneliti tidak beranjak dari aturan hukum yang ada. Hal itu dikarenakan memang belum atau tidak ada aturan hukum untuk masalah yang dihadapi.³⁶

3. Sifat Penelitian

Sifat penelitian yang penulis gunakan dalam tulisan ini adalah deskriptif analitis, yaitu menjelaskan aturan-aturan perundang-undangan yang relevan dengan teori-teori hukum yang menjadi objek kajian.³⁷ Penelitian deskriptif bertujuan untuk menyusun uraian yang sistematis, objektif, dan akurat mengenai

³⁴ Nur Solikin, 2021, *Pengantar Metode Penelitian Hukum*, Pasuruan, Qiara Media, hlm.58

³⁵ *Ibid.*

³⁶ *Ibid.* hlm. 60.

³⁷ Zainuddin Ali, 2010, *Metode Penelitian Hukum*, Jakarta, Sinar Grafika, hlm. 105-106.

fakta-fakta yang ditemukan, sehingga dapat memberikan gambaran yang jelas serta jawaban yang terstruktur terhadap rumusan permasalahan penelitian.

4. Jenis Data

Adapun jenis data yang digunakan dalam penelitian ini adalah data sekunder. Data sekunder tersebut diperoleh melalui penelitian kepustakaan (*library research*) dengan membaca buku-buku, artikel, dan literatur terkait. Sumber data-data sekunder dalam penelitian ini terdiri sebagai berikut:

a. Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang terdiri atas peraturan perundang-undangan, risalah resmi, dokumen hukum, dan putusan pengadilan.³⁸ Bahan hukum primer merupakan bahan-bahan hukum yang bersifat mengikat maupun tidak mengikat, terdiri dari:

- 1) EU) *General Data Protection Regulation* sebagai peraturan tentang perlindungan data pribadi EU;
- 2) (EU) *Artificial Intelligence Act* sebagai peraturan yang mengatur secara komprehensif tentang pengembangan dan penggunaan kecerdasan buatan di EU.³⁹
- 3) *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 2.0* sebagai pedoman untuk menggunakan FRT dalam penegakan hukum di EU.
- 4) *Guidelines on facial recognition (Convention 108/ Consultative Committee of the Convention for the protection of individuals with regard*

³⁸ *Ibid.*, hlm. 47.

³⁹ EU AI Act “*The EU AI Act*,” *EU AI Act - EU Artificial Intelligence Act*, diakses pada tanggal 15 Oktober 2025 pukul 13.51.

to automatic processing of personal data) sebagai pedoman untuk menggunakan FRT dalam penegakan hukum di EU.

b. Bahan Hukum Sekunder

Menurut Peter Mahmud Marzuki, bahan hukum sekunder ialah semua publikasi tentang hukum yang bukan berupa dokumen resmi, seperti buku teks yang menjelaskan hukum, jurnal hukum, komentar atas putusan pengadilan dan hasil penelitian atau telaah ilmiah. Bahan hukum sekunder dalam tulisan ini adalah buku-buku hukum, skripsi dan disertasi, serta jurnal hukum yang berkaitan dengan *Face Recognition Technology*, GDPR, dan AI Act.

5. Teknik Pengumpulan Data

Teknik yang digunakan dalam pengumpulan data untuk menyelesaikan skripsi ini adalah melalui studi kepustakaan (*bibliography study*). Teknik ini merupakan pengkajian informasi tertulis mengenai hukum yang berasal dari sumber dan dipublikasikan secara luas serta dibutuhkan dalam penelitian hukum normatif.⁴⁰ Bahan penelitian kepustakaan ini diperoleh dari:

- a. Perpustakaan Fakultas Hukum Universitas Andalas
- b. Buku-buku serta bahan bacaan lainnya yang penulis miliki dan artikel-artikel yang relevan dengan penelitian
- c. *Web sourcing*

6. Teknik Pengolahan dan Analisis Data

a. Pengolahan Data

Pada penelitian ini, penulis menggunakan beberapa metode pengolahan data sebagai berikut:

⁴⁰ Muhaimin, 2010, *Metode Penelitian Hukum*, Mataram, Mataram University Press, hlm.65.

1) Pemeriksaan data (*editing*)

Penulis memeriksa kembali apakah data yang terkumpul melalui studi pustaka, dokumen, dan seluruh bahan-bahan hukum yang sudah dikumpulkan sudah dianggap relevan, jelas, tidak berlebihan dan tanpa kesalahan.⁴¹

2) Sistematisasi data (*Sistematizing*)

Penulis melakukan seleksi terhadap bahan hukum, kemudian melakukan klasifikasi menurut penggolongan seperti golongan peraturan perundang-undangan, artikel, dan bahan hukum lainnya.⁴²

3) Deskripsi

Penulis menggambarkan hasil penelitian berdasarkan bahan hukum yang diperoleh kemudian menganalisisnya

b. Analisis Data

Menurut Sri Mamudji dkk., analisis data berarti kegiatan mengurai sesuatu sampai ke komponen-komponen dan kemudian menelaah hubungan masing-masing komponen dengan keseluruhan konteks dari berbagai sudut pandang. Penelaahan dilakukan sesuai dengan tujuan penelitian yang telah ditetapkan.⁴³

Metode analisis data yang digunakan dalam penelitian ini adalah analisis deskriptif kualitatif, yaitu suatu metode yang dilakukan dengan mengkaji dan menginterpretasikan data yang relevan terhadap isu hukum yang menjadi objek penelitian. Data yang dianalisis berupa data nonkuantitatif yang bersumber dari berbagai bahan hukum, baik bahan

⁴¹Nur Solikin, 2021, *Op.Cit.*, hlm.123

⁴²*Ibid.*

⁴³*Ibid*, hlm.105-106.

hukum primer, sekunder, maupun tersier, seperti peraturan perundang-undangan, dokumen hukum, literatur, serta sumber tertulis lainnya yang berkaitan dengan permasalahan penelitian.⁴⁴

Seluruh data tersebut dianalisis secara sistematis untuk memperoleh pemahaman yang komprehensif mengenai permasalahan yang dikaji. Hasil analisis selanjutnya disajikan secara deskriptif dengan memberikan interpretasi yang tepat terhadap ketentuan hukum, konsep, maupun doktrin yang relevan, sehingga dapat ditarik suatu kesimpulan yang menjawab rumusan masalah dalam penelitian ini.

F. Sistematika Penelitian

Sistematika penulisan bertujuan untuk memberikan gambaran dan arahan yang lebih jelas mengenai hal yang ditulis oleh penulis dimana penulisan ini dibagi menjadi 4 (empat) bab sebagai berikut:

BAB I: PENDAHULUAN

Pada bab ini, berisikan tentang pemaparan mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II: TINJAUAN KEPUSTAKAAN

Pada bab ini, menyajikan tentang tinjauan umum yang memuat substansi utama penelitian. Tinjauan kepustakaan dalam penelitian ini diawali dengan tinjauan umum FRT yang di dalamnya terdapat pengertian; tujuan dan mekanisme; manfaat FRT. Selanjutnya, bab ini membahas mengenai tinjauan umum data pribadi, yang mencakup pengertian, jenis-jenis, dan perlindungan

⁴⁴ Suteki dan Galang Taufani, 2018, Metodologi Penelitian Hukum: Filsafat, Teori, dan Praktik, Rajawali Pers, Depok, hlm. 213.

data pribadi. Tidak berhenti di situ, pengertian dan jenis-jenis data pribadi turut dibahas pada bab ini. Terakhir, bab ini juga membahas mengenai tinjauan umum GDPR dan AI Act.

BAB III: HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini, penulis menguraikan hasil penelitian mengenai analisis penggunaan FRT yang ditinjau berdasarkan GDPR dan AI Act. Hasil penelitian ini terdiri dari pengaturan hukum dan bentuk perlindungan hukum yang diberikan oleh EU GDPR dan AI Act dalam risiko penggunaan FRT terhadap data pribadi.

BAB IV: PENUTUP

Pada bab ini, penulis menguraikan tentang kesimpulan dari seluruh pembahasan dan memuat saran dari penulis yang berkaitan dengan materi penelitian.

