Jurnal Antologi Hukum
Vol. 5, No. 1, July 2025

E-ISSN : 2809-0748
P-ISSN : 2809-1078

PERLINDUNGAN HUKUM BAGI KORBAN PENGGUNAAN TEKNOLOGI PENGENALAN WAJAH

Fauzul Hilmi[1], Zaid Alfauza Marpaung[2]
[1,2]Universitas Islam Negeri Sumatera Utara
[1]*Email*: fauzul_hilmi@ymail.com
[2]*Email*: zaidallfauza@yahoo.co.id

DOI: https://doi.org/10.21154/antologihukum.v5i1.5128

Received: July 8, 2025	Revised: July 19, 2025	Approved: July 20, 2025

Abstract: *Facial recognition technology, although beneficial for security, poses legal challenges, especially in cases of misidentification, which risk violating privacy and causing injustice. This study explores the criminal law implications and personal data protection issues in Indonesia, focusing on the misidentification of Abdul Manaf in the 2022 incident involving Ade Armando. Using a normative legal research method, the study analyzes Law No. 27/2022 on Personal Data Protection (PDP), Law No. 11/2008 on Electronic Information and Transactions (ITE), and cybersecurity principles. The findings show that misidentification can lead to defamation, discrimination, and abuse of the legal system due to algorithmic bias and weak data verification. Biometric data protection requires clear consent, transparency, and strong cybersecurity measures. It is recommended that regulations be strengthened, technical standards improved, and collaboration among stakeholders enhanced to balance technological innovation with human rights protection.*

Keywords: *Criminal Law, Cybersecurity, Facial Recognition Technology*

Abstrak: Teknologi pengenalan wajah, meskipun bermanfaat bagi keamanan, menimbulkan tantangan hukum terutama dalam kasus kesalahan identifikasi yang berisiko melanggar privasi dan menyebabkan ketidakadilan. Penelitian ini mengkaji implikasi hukum pidana dan perlindungan data pribadi di Indonesia, dengan fokus pada kasus salah identifikasi Abdul Manaf dalam insiden Ade Armando tahun 2022. Menggunakan metode normatif, penelitian ini menganalisis UU PDP No. 27/2022, UU ITE No. 11/2008, serta prinsip keamanan siber. Hasil menunjukkan bahwa kesalahan identifikasi dapat memicu pencemaran nama baik, diskriminasi, dan penyalahgunaan sistem hukum akibat bias algoritma dan verifikasi data yang lemah. Perlindungan data biometrik memerlukan persetujuan jelas, transparansi, dan keamanan siber yang kuat. Disarankan agar penguatan regulasi, standar teknis, dan kerja sama semua pihak dilakukan untuk menyeimbangkan inovasi teknologi dengan perlindungan hak asasi manusia.

Kata Kunci : Hukum Pidana, Keamanan Siber, Teknologi Pengenalan Wajah

PENDAHULUAN

Teknologi pengenalan wajah telah diadopsi secara luas dalam berbagai sektor, mulai dari sistem keamanan di bandara dan pusat perbelanjaan. Di balik potensi manfaat tersebut, penerapan teknologi ini juga menimbulkan berbagai

tantangan, terutama jika terjadi kesalahan identifikasi yang bisa berdampak serius pada individu.[1] Salah satu contoh nyata terjadi dalam kasus pengeroyokan Ade Armando pada 11 April 2022, di mana teknologi pengenalan wajah digunakan oleh pihak kepolisian untuk mengidentifikasi para terduga pelaku dari rekaman CCTV. Dalam proses tersebut, Abdul Manaf sempat ditetapkan sebagai tersangka. Namun, setelah dilakukan penyelidikan lebih lanjut, ditemukan bahwa Abdul Manaf sebenarnya berada di Karawang, Jawa Barat, saat kejadian berlangsung. Alibi yang kuat, didukung oleh saksi dan bukti lain, kemudian menuntut klarifikasi dan koreksi atas penetapan status tersangka melalui hasil identifikasi berbasis teknologi tersebut.[2] Kejadian ini menimbulkan kontroversi di masyarakat dan menjadi sorotan kritis atas keakuratan serta validitas penggunaan teknologi pengenalan wajah dalam penegakan hukum. Kombinasi antara faktor eksternal seperti penggunaan aksesori (misalnya, topi) yang dapat mengganggu proses identifikasi dan keterbatasan algoritma yang belum sempurna, memperlihatkan bahwa teknologi ini seharusnya dijadikan alat bantu, bukan sebagai satu-satunya dasar penetapan status tersangka.

Pentingnya penggunaan bukti tambahan sesuai standar hukum, misalnya minimal dua alat bukti sebagaimana diamanatkan dalam KUHAP, menjadi semakin relevan untuk menghindari potensi kriminalisasi terhadap individu yang tidak bersalah. Studi kasus seperti yang dialami Abdul Manaf menjadi landasan yang kuat untuk mengkaji lebih mendalam efektivitas, batasan, dan penerapan etis dari teknologi pengenalan wajah di Indonesia. Lebih jauh, kasus ini membuka diskursus mengenai perlindungan hak privasi dan data pribadi dalam era digital, di mana teknologi biometrik semacam ini mengumpulkan data sensitif. Di tengah keberadaan regulasi yang mendukung perlindungan data, seperti Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pelindungan Data Pribadi, perlu dilakukan evaluasi kritis terhadap mekanisme penggunaan dan pengamanan data guna meminimalisir risiko penyalahgunaan dan kesalahan identifikasi.

---

[1] Fredi Syahlulus Tarigan, "Implikasi Hukum Terhadap Penggunaan Teknologi Pengenalan Wajah Kajian Literatur," *Judge : Jurnal Hukum* 4, no. 01 (2023): 01, https://doi.org/10.54209/judge.v4i01.375.

[2] CNN Indonesia, "IPW Sentil Polisi Salah Tetapkan Tersangka Pengeroyok Ade Armando," CNN Indonesia, diakses 9 April 2025, https://www.cnnindonesia.com/nasional/20220414141540-12-784875/ipw-sentil-polisi-salah-tetapkan-tersangka-pengeroyok-ade-armando.

Pengenalan wajah, sebagai bagian dari teknologi biometrik, merupakan suatu metode identifikasi yang semakin luas digunakan dalam sistem keamanan.[3] Teknologi ini memanfaatkan karakteristik unik dari wajah seseorang untuk memverifikasi atau mengenali identitas mereka.[4] Selain pengenalan wajah, teknologi biometrik lainnya seperti pengenalan retina mata, sidik jari, dan iris mata juga digunakan untuk meningkatkan keamanan.[5] Dengan memanfaatkan fitur-fitur unik pada wajah, sistem pengenalan wajah dapat memberikan tingkat keakuratan yang tinggi, memungkinkan penggunaannya dalam berbagai aplikasi, mulai dari pengamanan perangkat hingga pengawasan akses fisik.[6] Kesalahan identifikasi merupakan salah satu tantangan utama yang dihadapi dalam implementasi teknologi pengenalan wajah.[7] Meskipun teknologi ini terus mengalami perkembangan, namun belum sepenuhnya bebas dari kemungkinan kesalahan yang dapat memiliki konsekuensi hukum yang serius.[8] Dalam ranah hukum pidana, kesalahan identifikasi memiliki potensi untuk mengakibatkan penyalahgunaan proses hukum yang dapat berdampak pada ketidakadilan sistematis. Ketidakcocokan identifikasi dapat memberikan pemahaman yang salah terhadap identitas individu, bahkan memunculkan risiko penangkapan atau penuntutan yang tidak adil.[9]

Teknologi pengenalan wajah seringkali memiliki kecenderungan untuk rentan terhadap diskriminasi, terutama ketika dihadapkan pada kelompok-kelompok tertentu seperti minoritas etnis atau individu dengan warna kulit yang berbeda, dan kasus pengeroyokan Ade Armando memperlihatkan hal ini secara

---

[3] Jawahitha Sarabdeen, "Protection of the rights of the individual when using facial recognition technology," *Heliyon* 8, no. 3 (2022): e09086, https://doi.org/10.1016/j.heliyon.2022.e09086.

[4] Vera Lúcia Raposo, "The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal," *European Journal on Criminal Policy and Research* 29, no. 4 (2023): 515–33, https://doi.org/10.1007/s10610-022-09512-y.

[5] D. Utegen dan B. Zh Rakhmetov, "Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models," ARTICLES, *Journal of Digital Technologies and Law* 1, no. 3 (2023): 3, https://doi.org/10.21202/jdtl.2023.36.

[6] Serign Modou Bah dan Fang Ming, *An Improved Face Recognition Algorithm and its Application in Attendance Management System*, 5, no. 20 (2020), https://www.sciencedirect.com/science/article/pii/S2590005619300141.

[7] Maša Galič dan Lonneke Stevens, "Regulating Police Use of Facial Recognition Technology in The Netherlands: The Complex Interplay Between Criminal Procedural Law and Data Protection Law," *New Journal of European Criminal Law* 14, no. 4 (2023): 459–78, https://doi.org/10.1177/20322844231212834.

[8] Rahmat Rambe dan Lukman Abdurrahman, "Implikasi Etika Dan Hukum Dalam Penggunaan Teknologi Pengenalan Wajah: Perlindungan Privasi Versus Keamanan Publik," *Jurnal Hukum Caraka Justitia* 4, no. 2 (2024): 90–104, https://doi.org/10.30588/jhcj.v4i2.1828.

[9] Anfa'un Nisa' Fidinir Rahman dkk., "Perlindungan Hukum Terhadap Korban Penyalahgunaan Teknik Deepfake," *Perspektif Administrasi Publik Dan Hukum* 2, no. 1 (2025): 247–55, https://doi.org/10.62383/perspektif.v2i1.202.

nyata. Dalam kasus tersebut, kesalahan identifikasi yang menimpa Abdul Manaf, yang sempat ditetapkan sebagai tersangka meskipun memiliki alibi kuat bahwa ia berada di Karawang, menunjukkan bagaimana penggunaan teknologi tersebut tanpa verifikasi data yang memadai dapat menimbulkan potensi bias dan diskriminasi dalam penegakan hukum. Dinamika ini tidak hanya menciptakan ketidaksetaraan dalam pengenalan dan pemrosesan wajah, tetapi juga meningkatkan risiko penyalahgunaan data dan pelanggaran hak asasi, terutama jika data pribadi yang sensitif bocor atau disalahgunakan oleh pihak yang tidak berwenang. Kejadian ini menegaskan perlunya penerapan langkah perlindungan data yang ketat dan verifikasi berlapis, agar teknologi pengenalan wajah dapat digunakan secara etis dan tidak menghambat keadilan dalam proses hukum serta tidak merusak integritas sistem pengawasan.

Pada penerapannya, penggunaan teknologi pengenalan wajah harus memperhatikan prinsip-prinsip perlindungan data pribadi yang diamanatkan oleh kedua undang-undang ini.[10] Hal ini tidak hanya untuk mencegah potensi penyalahgunaan, seperti kesalahan identifikasi yang bisa berakibat pada tindakan hukum yang merugikan, tetapi juga untuk menjaga kepercayaan dan hak asasi manusia. Misalnya, kesalahan identifikasi yang pernah terjadi dalam kasus pengeroyokan Ade Armando menggarisbawahi pentingnya verifikasi data tambahan dan bukti yang memadai sebelum menetapkan seseorang sebagai tersangka. Fenomena diskriminasi menjadi perhatian dalam penerapan teknologi pengenalan wajah. Teknologi ini, meskipun canggih, masih rentan terhadap bias dan kesalahan, terutama terhadap kelompok minoritas atau individu dengan karakteristik fisik tertentu. Ketidakakuratan dalam identifikasi dapat memicu ketidakadilan dalam sistem hukum pidana, yang pada gilirannya dapat mengakibatkan ketidaksetaraan sistematis. Selain itu, peningkatan penggunaan teknologi ini menimbulkan risiko signifikan terkait keamanan data dan potensi penyalahgunaan oleh pihak yang tidak berwenang.

Berdasarkan latar belakang masalah yang telah diuraikan, tujuan penelitian ini adalah untuk mengkaji tantangan hukum pidana yang muncul akibat kesalahan identifikasi dalam penggunaan teknologi pengenalan wajah serta mengevaluasi upaya perlindungan data dan keamanan siber yang dapat diterapkan demi

[10] Bondan Ayu Maharani dkk., "Perlindungan Hukum Masyarakat Dari Dampak Negatif Penggunaan AI," *Media Hukum Indonesia (MHI)* 3, no. 2 (2025): 2, https://doi.org/10.5281/zenodo.15783168.

mengatasi risiko ancaman hukum yang timbul dari penggunaan teknologi tersebut. Ruang lingkup penelitian ini mencakup analisis terhadap tantangan hukum pidana yang muncul akibat penyalahgunaan teknologi pengenalan wajah, khususnya yang dipicu oleh kesalahan identifikasi. Selain itu, penelitian ini juga mengeksplorasi aspek perlindungan data dan keamanan siber sebagai bagian dari strategi mitigasi risiko hukum yang diakibatkan oleh ketidaktepatan sistem teknologi tersebut. Kasus kesalahan identifikasi yang menimpa Abdul Manaf dalam peristiwa pengeroyokan Ade Armando pada 2022 dijadikan sebagai studi kasus utama untuk memperjelas analisis. Metode penelitian yang digunakan adalah pendekatan normatif dengan mengkaji sejumlah regulasi, seperti UU Perlindungan Data Pribadi (PDP) No. 27 Tahun 2022 dan UU Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008, serta mempertimbangkan berbagai teori hukum yang relevan, termasuk hukum pidana, hukum privasi, hak asasi manusia, dan hukum teknologi informasi.

KERANGKA TEORI

Teori hukum pidana berperan penting dalam mengatur tindakan kriminal, termasuk dalam pemanfaatan teknologi pengenalan wajah yang berpotensi melanggar hak privasi.[11] Teori hukum pidana adalah kerangka konseptual yang menjelaskan prinsip-prinsip dasar dalam menentukan apa yang dikategorikan sebagai tindak pidana, bagaimana suatu perbuatan dinilai sebagai pelanggaran hukum, serta bentuk sanksi yang layak diberikan.[12] Teori hukum pidana adalah kerangka konseptual yang terdiri dari prinsip, konsep, dan aturan yang menjadi dasar dalam menentukan apa yang disebut tindak pidana, bagaimana kesalahan pelaku dinilai, serta sanksi yang layak diberikan sebagai respons atas pelanggaran hukum. Selain itu, teori ini juga berfungsi untuk mengelompokkan jenis-jenis kejahatan, menilai pertanggungjawaban pelaku, dan menentukan hukuman yang proporsional demi terciptanya keadilan serta ketertiban sosial. Sebagai fondasi hukum, teori ini membantu membentuk kebijakan, menjalankan sistem peradilan, serta merancang strategi pencegahan agar angka kejahatan dapat ditekan secara efektif.[13]

[11] Soerjono Soekanto, *Penelitian Hukum Normatif Suatu Tinjauan Singkat* (PT. Raja Grafindo Persada, 2020).

[12] Jimly Asshiddiqie, *Hukum Pidana: Suatu Pengantar* (Sinar Grafika, 2021).

[13] Saldi Isra, *Hukum Pidana: Suatu Pengantar* (PT RajaGrafindo Persada, 2017).

Pemahaman terhadap hukum pidana tidak terlepas dari kerangka teori yang menjadi dasar dalam menilai suatu perbuatan sebagai tindak pidana, menentukan kesalahan pelaku, dan memberikan sanksi yang sesuai. Teori ini menjadi fondasi dalam penyusunan kebijakan hukum, pelaksanaan sistem peradilan, serta upaya pencegahan kejahatan. Dalam penerapan teknologi pengenalan wajah, aspek hukum pidana sangat penting untuk mengatur potensi pelanggaran hukum, terutama yang terkait dengan hak privasi dan identitas seseorang. Salah satu contohnya adalah kasus pengeroyokan Ade Armando pada tahun 2022, di mana teknologi tersebut digunakan untuk mengidentifikasi pelaku dari rekaman kamera pengawas. Sayangnya, hal ini berujung pada salah tangkap terhadap Abdul Manaf, yang sebenarnya sedang berada di Karawang saat kejadian. Kasus ini menegaskan bahwa penggunaan teknologi pengenalan wajah tanpa verifikasi yang memadai dapat memicu kesalahan hukum, merusak reputasi seseorang, hingga menyalahgunakan proses peradilan. Oleh karena itu, pengaturan yang jelas dan mekanisme kontrol yang ketat diperlukan untuk menghindari risiko tersebut.

Teori hukum privasi berfokus pada perlindungan hak individu atas privasi dan data pribadi, terutama dalam pemanfaatan teknologi pengenalan wajah. Dalam konteks penelitian ini, teori tersebut memberikan kerangka hukum untuk menentukan batasan dalam pengumpulan, penggunaan, dan penyimpanan data biometrik wajah, sehingga hak kebebasan dan privasi masyarakat tetap terjaga.[14] Teori hukum privasi membahas perlindungan hak individu atas informasi pribadi dalam menghadapi perkembangan teknologi informasi yang memungkinkan pengumpulan dan penyebaran data secara luas. Dengan pesatnya inovasi digital, penting bagi hukum untuk terus berkembang guna menjaga keseimbangan antara kemajuan teknologi dan penghormatan terhadap privasi.[15] Teori hukum privasi membahas tantangan perlindungan data pribadi di tengah perkembangan teknologi dan arus pertukaran informasi global yang semakin tidak terbatas. Dengan meningkatnya kemampuan sistem untuk memantau dan memproses data individu secara luas, risiko pelanggaran privasi semakin nyata. Untuk itu, diperlukan kerangka hukum yang kuat guna menegaskan hak setiap orang atas kontrol terhadap data dirinya, menerapkan standar perlindungan yang ketat, serta

[14] Harkristuti Harkrisnowo, *Hukum Privasi di Indonesia: Tinjauan Terhadap Perlindungan Data Pribadi* (PT Citra Aditya Bakti, 2018).

[15] Bambang Sutrisno, *Privasi dalam Hukum: Perlindungan Privasi dalam Era Digital* (PT Elex Media Komputindo, 2019).

memperkuat mekanisme pengawasan baik di tingkat nasional maupun internasional agar hak privasi sebagai bagian dari hak asasi manusia tetap terjaga.[16]

Pemahaman tentang hukum privasi semakin penting di tengah perkembangan teknologi yang mampu mengakses dan mengolah data pribadi secara luas, terutama dalam penerapan sistem pengenalan wajah. Teori hukum privasi hadir sebagai panduan untuk menetapkan batasan dalam pengelolaan data biometrik, sehingga hak masyarakat atas kebebasan dan kerahasiaan informasi tetap terjaga. Di tengah pesatnya inovasi digital, hukum perlu terus diperbarui agar mampu melindungi hak individu tanpa menghambat kemajuan teknologi. Salah satu contohnya adalah kasus salah identifikasi yang dialami Abdul Manaf, di mana penggunaan teknologi pengenalan wajah tanpa proses verifikasi yang ketat berujung pada kesalahan penegakan hukum. Kejadian ini membuka mata bahwa sistem yang digunakan sering kali rentan terhadap bias dan berpotensi menimbulkan diskriminasi. Perlunya pengaturan yang lebih ketat dalam pengelolaan data serta transparansi dalam penerapan teknologi menjadi semakin mendesak untuk mencegah pelanggaran hak dan menjaga kepercayaan masyarakat terhadap sistem hukum.

Teori hukum hak asasi manusia menekankan pentingnya perlindungan hak-hak dasar setiap individu, termasuk hak atas privasi dan kebebasan pribadi, terutama dalam penerapan teknologi pengenalan wajah. Dalam konteks ini, negara memiliki kewajiban untuk memastikan bahwa penggunaan teknologi tidak melanggar prinsip kesetaraan, keadilan, dan penghormatan terhadap martabat manusia. Perlindungan terhadap data biometrik dan pencegahan penyalahgunaan teknologi harus dilihat sebagai bagian dari upaya menjaga hak asasi yang tidak dapat dikurangi, serta mendorong kesejahteraan masyarakat secara adil dan inklusif.[17] Kerangka hukum harus dirancang untuk menyeimbangkan inovasi teknologi dengan tanggung jawab negara dalam melindungi hak-hak konstitusional warganya.[18] Teori hukum hak asasi manusia menempatkan perlindungan dan penguatan hak-hak dasar individu sebagai fondasi dalam membangun masyarakat yang adil dan beradab. Hak-hak seperti kebebasan politik, ekonomi, akses

[16] Enny Nurbaningsih, *Hak Privasi dalam Hukum: Perlindungan Hak Privasi di Era Globalisasi* (Pustaka Yustisia, 2017).

[17] Bagas Wahyu Priambodo dan Dipo Wahjoeono, "Perlindungan Hukum Terhadap Penggunaan Teknologi Biometrik Dalam Transaksi Perbankan Untuk Meningkatkan Keamanan," *Madani: Jurnal Ilmiah Multidisiplin* 1, no. 11 (2023): 11, https://doi.org/10.5281/zenodo.10276789.

[18] Ronald Myles Dworkin, 2017, *Taking Rights Seriously*, Harvard University Press, Cambridge.

pendidikan, pelayanan kesehatan, serta kebebasan berpikir dan berpendapat menjadi bagian tak terpisahkan dari upaya mewujudkan kesejahteraan dan martabat manusia. Dengan menegakkan hak-hak tersebut, setiap individu memiliki peluang yang setara untuk berkembang secara utuh dan hidup bermakna dalam tatanan sosial yang inklusif.[19]

Hak asasi manusia menjadi prinsip dasar dalam pengaturan pemanfaatan teknologi, khususnya yang berkaitan dengan data pribadi seperti pengenalan wajah. Teori hukum HAM menempatkan negara sebagai pihak yang bertanggung jawab untuk memastikan bahwa teknologi digunakan tanpa melanggar hak privasi, kebebasan, dan martabat setiap orang. Dalam praktiknya, penggunaan sistem biometrik harus diimbangi dengan perlindungan hukum yang kuat agar tidak menimbulkan bias, kesalahan identifikasi, atau diskriminasi. Kasus salah tangkap Abdul Manaf menjadi contoh bagaimana kelemahan pada sistem verifikasi data dan algoritma dapat berujung pada pelanggaran hukum yang merugikan individu. Ini menjadi pengingat bahwa pengaturan teknologi harus lebih ketat, dengan penerapan mekanisme perlindungan data yang menyeluruh dan verifikasi berlapis, sehingga inovasi teknologi bisa berjalan beriringan dengan prinsip keadilan serta perlindungan hak konstitusional warga negara.

Teori hukum teknologi informasi membahas pengaturan hukum yang relevan dalam pemanfaatan teknologi digital, termasuk kewajiban para pihak seperti penyedia layanan, pengelola aplikasi, dan pengguna dalam menjaga keamanan dan perlindungan data. Fokus utamanya adalah mengkaji dampak hukum dari penggunaan teknologi dalam berbagai aspek kehidupan, seperti privasi, hak kekayaan intelektual, dan keamanan informasi. Dengan perkembangan teknologi yang begitu cepat, teori ini terus beradaptasi untuk memberikan kerangka hukum yang memadai dalam menghadapi tantangan baru di era digital.[20] Teori hukum teknologi informasi merupakan bidang hukum yang mengkaji pengaturan dan perlindungan dalam pemanfaatan teknologi di tengah kehidupan modern, terutama menyangkut isu privasi, keamanan data, serta hak kekayaan intelektual di ruang digital.[21] Teori hukum teknologi informasi mempelajari pengaturan dan pemanfaatan teknologi dalam berbagai aspek kehidupan, termasuk perlindungan

[19] Martha Craven Nussbaum, *Creating Capabilities: The Human Development Approach* (Harvard University Press, 2021).

[20] Bambang Sutedja, *Teori Hukum Teknologi Informasi* (Rajawali Pers, 2020).

[21] Rahmi Jened, *Hukum Teknologi Informasi dan Komunikasi* (Sinar Grafika, 2015).

data pribadi, kebebasan berekspresi di dunia maya, serta tanggung jawab hukum yang muncul dari penggunaan teknologi. Selain menyoroti kerangka hukum yang mengatur individu dan organisasi, teori ini juga mengkaji dampak sosial dan politik dari perkembangan teknologi informasi, sehingga mampu memberikan perspektif yang lebih luas dalam menyusun regulasi yang sesuai dengan dinamika digital saat ini.[22]

Pemanfaatan teknologi digital membutuhkan kerangka hukum yang jelas untuk mengatur kewajiban para pelaku teknologi, termasuk penyedia layanan dan pengelola aplikasi dalam menjaga keamanan dan perlindungan data pengguna. Teori hukum teknologi informasi hadir sebagai acuan untuk mengevaluasi dampak hukum dari penggunaan sistem digital dalam berbagai aspek kehidupan, seperti perlindungan privasi, hak atas kekayaan intelektual, dan pengelolaan keamanan informasi. Tidak hanya itu, teori ini juga mengkaji perubahan sosial dan politik yang muncul sebagai akibat perkembangan teknologi, sehingga dapat memberikan panduan dalam penyusunan regulasi yang responsif terhadap perkembangan zaman. Kasus salah identifikasi Abdul Manaf menjadi contoh nyata perlunya evaluasi menyeluruh terhadap penerapan teknologi pengenalan wajah di Indonesia, baik dari sisi efektivitas maupun etika. Kejadian ini membuktikan bahwa tanpa dukungan alat bukti yang kuat dan sesuai prosedur hukum, seperti minimal dua alat bukti sebagaimana diatur dalam KUHAP, risiko salah tangkap sangat tinggi. Untuk itu, hukum harus terus diperbarui agar mampu menjawab tantangan baru di tengah pesatnya perkembangan teknologi digital.

ANALISIS PERATURAN HUKUM TERHADAP PENGGUNAAN TEKNOLOGI PENGENALAN WAJAH

Hukum pidana adalah cabang hukum yang mengatur tindakan yang dianggap melanggar norma-norma yang ditetapkan oleh negara dan memberikan sanksi atau hukuman kepada pelaku kejahatan. Hukum pidana berfokus pada perlindungan masyarakat, menjaga ketertiban, dan melaksanakan keadilan.[23] Hukum pidana meliputi berbagai aspek, mulai dari definisi kejahatan, proses penyelidikan, persidangan, hingga pelaksanaan hukuman. Tujuannya adalah untuk menegakkan keadilan dan memastikan bahwa pelanggar hukum diberikan sanksi yang sesuai

[22] Hikmahanto Juwana, *Hukum dan Teknologi Informasi* (Prenada Media, 2018).
[23] Asshiddiqie, *Hukum Pidana: Suatu Pengantar*.

dengan tingkat kejahatan yang dilakukan.[24] Tantangan hukum pidana dalam kesalahan identifikasi teknologi pengenalan wajah di Indonesia mencakup berbagai aspek hukum yang perlu diperhatikan. Teknologi pengenalan wajah, yang menggunakan algoritma dan perangkat lunak untuk mengidentifikasi individu berdasarkan fitur wajah, tidak selalu sempurna dan dapat menghadapi kesulitan dalam memberikan identifikasi yang akurat. Beberapa tantangan yang mungkin muncul melibatkan kesalahan identifikasi, bias, dan ketidakakuratan dalam kondisi pencahayaan yang buruk atau variasi pose wajah.

Implikasi hukum pidana dari kesalahan identifikasi teknologi pengenalan wajah dapat mencakup serangkaian dampak yang meliputi kehilangan privasi, penyalahgunaan sistem hukum, dan bahkan tindakan pelecehan hukum. Ketika seseorang salah diidentifikasi sebagai pelaku kejahatan, terjadilah kehilangan privasi yang mengakibatkan pencemaran nama baik dan konsekuensi hukum yang tidak adil. Selain itu, penyalahgunaan sistem hukum dapat terjadi ketika teknologi pengenalan wajah digunakan secara tidak cermat atau tanpa memperhatikan hak asasi manusia, menyebabkan keraguan terhadap integritas sistem hukum. Bahkan lebih serius, kesalahan identifikasi semacam itu dapat memicu tindakan pelecehan hukum terhadap individu yang tidak bersalah, menggugah perdebatan tentang perlindungan hak asasi manusia dalam penerapan teknologi keamanan dan penegakan hukum.

Dalam menghadapi tantangan identifikasi teknologi pengenalan wajah, beberapa pertimbangan hukum pidana yang relevan perlu ditekankan. Pertama, membedakan antara kesalahan identifikasi sebagai kesalahan sistem dan kesalahan yang dilakukan dengan sengaja menjadi esensial. Perlindungan privasi individu juga menjadi fokus utama, dengan diperlukannya perluasan hak individu untuk melawan tindakan merugikan yang mungkin timbul dari kesalahan identifikasi teknologi. Pengaturan sanksi yang ketat bagi pelanggaran privasi di lingkungan teknologi pengenalan wajah juga diperlukan guna menegaskan batasan dan konsekuensi hukum yang jelas. Dengan demikian, langkah-langkah hukum ini diharapkan dapat memberikan landasan yang kuat dalam menangani dampak negatif dari kesalahan identifikasi teknologi pengenalan wajah, melindungi hak-hak individu, dan menjaga integritas sistem hukum.

[24] Saldi Isra, *Perlindungan Hukum dalam Sistem Peradilan Pidana di Indonesia* (Sinar Grafika, 2019).

Membedakan antara kesalahan identifikasi sebagai kesalahan sistem dan kesalahan yang dilakukan dengan sengaja menjadi hal yang krusial. Penting untuk membedakan antara kesalahan yang terjadi karena kegagalan teknologi pengenalan wajah dan kesalahan yang disengaja. Relevansi hal ini sangat penting dalam menilai tanggung jawab hukum individu dalam kasus-kasus kesalahan identifikasi dan menentukan mekanisme yang dapat digunakan untuk mengatasi kesalahan tersebut. Perlindungan privasi individu dalam konteks teknologi pengenalan wajah juga menjadi suatu keharusan. Ini melibatkan pembatasan pengumpulan, penggunaan, dan penyimpanan data wajah individu, serta memastikan bahwa individu memiliki hak untuk melawan tindakan merugikan yang mungkin timbul dari kesalahan identifikasi teknologi. Pengaturan hukum yang ketat diperlukan untuk menanggulangi pelanggaran privasi di lingkungan teknologi pengenalan wajah. Langkah ini bertujuan untuk menegaskan batasan dan konsekuensi hukum yang jelas bagi mereka yang melanggar privasi individu melalui penggunaan teknologi ini.[25]

Pentingnya memiliki pengaturan dan standar teknis yang jelas terkait dengan penggunaan teknologi pengenalan wajah sangat ditekankan dalam rangka mengamankan penerapannya. Hal ini mencakup penetapan persyaratan dan protokol yang ketat untuk meminimalkan kesalahan identifikasi dan memastikan penggunaan teknologi tersebut secara akurat dan adil. Pengaturan semacam itu perlu merinci pedoman teknis yang bersifat spesifik, mencakup kriteria identifikasi yang tinggi dan pengujian reguler untuk menilai kehandalan sistem. Selain itu, untuk menegakkan kepatuhan dan menjamin keadilan, sanksi hukum yang memadai bagi pelanggaran hukum yang melibatkan kesalahan identifikasi teknologi pengenalan wajah perlu dipertimbangkan secara serius. Ini mencakup penerapan sanksi terhadap individu atau entitas yang dengan sengaja memanfaatkan teknologi ini untuk tujuan jahat atau yang mengabaikan tanggung jawab mereka dalam memastikan akurasi dan keadilan dalam proses identifikasi tersebut. Dengan adanya pengaturan dan sanksi yang tegas, diharapkan dapat menciptakan lingkungan penggunaan teknologi pengenalan wajah yang lebih aman, andal, dan etis.

[25] Ryan Calo, "The Case for a Federal Robotics Commission: Lessons from Privacy Law," *ale Journal of Law and Technology* 1, no. 1 (2020).

Saat ini, Indonesia belum memiliki satu undang-undang yang secara khusus mengatur teknologi pengenalan wajah. Namun, implementasinya tidak bebas dari aturan hukum. Penggunaan teknologi ini diatur dalam kerangka peraturan perundang-undangan yang lebih luas, terutama yang berkaitan dengan pelindungan data pribadi dan penyelenggaraan sistem elektronik. Regulasi utama yang menjadi acuan adalah Undang-Undang Pelindungan Data Pribadi (UU PDP) yang baru disahkan. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memegang peranan sentral. Dalam UU ini, data biometrik, yang mencakup data wajah untuk identifikasi, dikategorikan sebagai data pribadi yang bersifat spesifik. Klasifikasi ini membawa konsekuensi penting: pemrosesan data wajah memerlukan dasar hukum yang lebih ketat dibandingkan data pribadi umum. Persetujuan eksplisit dari individu pemilik data menjadi syarat utama, kecuali jika ada dasar hukum lain yang relevan dan memenuhi syarat ketat dalam UU PDP. Prinsip-prinsip seperti transparansi, pembatasan tujuan, dan keamanan data juga wajib dipatuhi. Selain UU PDP, kerangka hukum pendukung lainnya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, dan Peraturan Pemerintah 1 Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Regulasi ini menggarisbawahi pentingnya persetujuan dalam penggunaan data pribadi melalui media elektronik dan menetapkan kewajiban bagi Penyelenggara Sistem Elektronik (PSE) untuk melindungi data yang mereka kelola, termasuk data biometrik. Permenkominfo No. 20 Tahun 2016 juga sempat menjadi acuan sebelum UU PDP berlaku penuh.

Secara praktis, kombinasi dari peraturan-peraturan ini mewajibkan setiap pihak yang menggunakan teknologi pengenalan wajah di Indonesia untuk memenuhi beberapa syarat kunci. Mereka harus mendapatkan persetujuan yang jelas dan terinformasi (eksplisit) dari individu, transparan mengenai tujuan penggunaan data wajah, membatasi penggunaan data hanya untuk tujuan tersebut, menerapkan langkah-langkah keamanan yang memadai untuk melindungi data dari akses tidak sah atau penyalahgunaan, serta menghormati hak-hak individu terkait data pribadi mereka (seperti hak akses, perbaikan, atau penghapusan). Meskipun belum ada legislasi spesifik untuk pengenalan wajah, UU Pelindungan Data Pribadi menjadi payung hukum utama yang mengatur penggunaannya di Indonesia dengan menekankan pada status data wajah sebagai data spesifik yang memerlukan

perlakuan khusus. Kepatuhan terhadap UU PDP, serta UU ITE dan peraturan turunannya, adalah esensial bagi implementasi teknologi ini secara legal dan etis. Perkembangan regulasi turunan dari UU PDP di masa mendatang mungkin akan memberikan panduan yang lebih detail mengenai penerapan teknologi ini.

Tantangan hukum pidana dalam kesalahan identifikasi teknologi pengenalan wajah melibatkan beberapa aspek yang perlu dipertimbangkan. Pertama, perlindungan hak privasi menjadi fokus utama, di mana pengaturan hukum pidana harus memastikan penggunaan teknologi ini tidak merugikan individu atau mengabaikan hak privasi mereka. Kedua, kebijakan privasi menjadi hal penting dalam melindungi individu dari intervensi pihak ketiga, dan hukum pidana perlu memastikan kebebasan individu dalam penggunaan teknologi pengenalan wajah.[26] Selanjutnya, kendali dan pengawasan juga menjadi aspek krusial, di mana regulasi harus memastikan penggunaan teknologi ini tidak melanggar hak privasi dengan pengawasan yang berlebihan atau invasif. Aspek teknis juga harus diperhatikan dalam hukum pidana untuk menghindari kendala teknis yang dapat merugikan individu. Selain itu, aspek sosial dan etis juga perlu diperhitungkan, karena penggunaan teknologi ini dapat memiliki dampak sosial, psikologis, dan etis yang perlu diatur secara cermat. Terakhir, kendala keteknologi menjadi perhatian penting, dan hukum pidana harus mempertimbangkan regulasi yang menghindari gangguan dalam penggunaan teknologi pengenalan wajah.[27]

Penting bagi pemerintah, regulator, dan lembaga hukum di Indonesia untuk memperhatikan tantangan hukum pidana yang muncul seiring dengan perkembangan teknologi pengenalan wajah. Dalam konteks kesalahan identifikasi, pertimbangan hukum pidana yang relevan harus mencakup aspek penggunaan yang sah, kesalahan identifikasi, pemalsuan identitas, privasi, dan perlindungan data. Pentingnya memperhitungkan upaya untuk mencegah ketidakadilan dan diskriminasi dalam penggunaan teknologi pengenalan wajah di Indonesia tidak boleh diabaikan. Oleh karena itu, perlu dibentuk kerangka hukum yang jelas dan komprehensif, melibatkan regulator yang kompeten dalam mengawasi implementasi teknologi ini. Langkah ini bertujuan untuk memastikan perlindungan

[26] Akmal Zulham Nurkamal dan Laras Astuti, "Perlindungan Hukum Korban Terhadap Pelanggaran Hak Privasi Dalam Pembuatan Konten Menggunakan Drone," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 3 (2024): 3, https://doi.org/10.18196/ijclc.v5i3.23254.

[27] Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi, "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital," Pusat Penelitian dan Pengkajian Perkara, dan Pengelolaan Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi, 2019.

hak-hak individu, mendukung keadilan, dan menyeimbangkan perkembangan teknologi dengan nilai-nilai keadilan dan hak asasi manusia di dalam masyarakat. Dengan adanya kerangka hukum yang kokoh, diharapkan dapat menciptakan lingkungan hukum yang kondusif untuk pengembangan dan penerapan teknologi pengenalan wajah di Indonesia.

Pemanfaatan teknologi pengenalan wajah di Indonesia masih dihadapkan pada sejumlah tantangan hukum, terutama dalam ranah pidana, di mana risiko kesalahan identifikasi bisa menyebabkan pelanggaran privasi hingga munculnya ketidakadilan hukum. Kasus salah identifikasi yang menimpa Abdul Manaf dalam peristiwa pengeroyokan Ade Armando menjadi salah satu contoh konkret, di mana sistem salah menetapkan dirinya sebagai tersangka meskipun ia memiliki alibi kuat. Kejadian ini menunjukkan perlunya perbaikan mendasar baik dari sisi regulasi maupun teknis agar teknologi ini digunakan secara akurat dan bertanggung jawab. Di sejumlah negara seperti Eropa, regulasi ketat seperti GDPR (*General Data Protection Regulation*) telah memberikan perlindungan lebih tinggi dengan mengategorikan data biometrik sebagai data sensitif yang memerlukan persetujuan eksplisit serta memberikan kontrol penuh kepada individu atas data mereka. Di Indonesia, meskipun UU Perlindungan Data Pribadi (PDP) No. 27 Tahun 2022 telah mengakui status khusus data biometrik, implementasinya masih perlu diperkuat melalui standar teknis yang lebih jelas dan sanksi yang tegas. Solusi yang dapat diterapkan antara lain adalah penyusunan pedoman teknis yang detail, pengujian berkala terhadap sistem, serta penerapan mekanisme verifikasi berlapis oleh aparat penegak hukum. Dalam konteks hukum acara, paling tidak harus ada dua alat bukti yang saling menguatkan sebelum menetapkan seseorang sebagai tersangka, sebagaimana diatur dalam KUHAP. Dengan demikian, pemanfaatan teknologi ini harus diiringi dengan kerangka hukum yang solid, standar operasional yang ketat, serta koordinasi yang baik antar instansi agar inovasi teknologi tidak melanggar hak asasi manusia dan tetap menjunjung tinggi rasa keadilan masyarakat.

ANALISIS PERLINDUNGAN DATA DAN KEAMANAN CYBER DALAM UPAYA UNTUK MENGATASI ANCAMAN HUKUM AKIBAT KESALAHAN IDENTIFIKASI TEKNOLOGI PENGENALAN WAJAH

Penerapan hukum pidana di ranah teknologi, khususnya pada penggunaan sistem pengenalan wajah, menjadi semakin kompleks ketika menghadapi tantangan

kesalahan identifikasi. Hal ini tampak jelas pada kasus pengeroyokan Ade Armando, di mana Abdul Manaf sempat diidentifikasi sebagai tersangka melalui analisis teknologi pengenalan wajah, walaupun pada kenyataannya alibi yang kuat membuktikan bahwa ia berada di Karawang saat kejadian berlangsung. Kesalahan identifikasi semacam ini tidak hanya mencemarkan nama baik individu, tetapi juga menimbulkan potensi penyalahgunaan sistem hukum dan mengaburkan batas antara kesalahan teknis dan tindakan yang disengaja. Penelitian ini menyoroti pentingnya perlindungan data dan keamanan siber sebagai upaya strategis untuk menanggulangi berbagai ancaman hukum yang muncul akibat kesalahan identifikasi berbasis teknologi pengenalan wajah. Fenomena kesalahan identifikasi tidak hanya mengikis kepercayaan publik terhadap sistem hukum, tetapi juga membuka celah bagi penyalahgunaan data pribadi yang sangat sensitif. Implementasi proteksi data dan sistem keamanan *cyber* menjadi langkah fundamental dalam menghadapi tantangan tersebut.

Regulasi pelindungan data, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, memberikan landasan hukum yang sangat penting dalam pengelolaan data biometrik, khususnya data wajah yang digunakan dalam teknologi pengenalan. Pengaturan yang ketat mengenai persetujuan eksplisit dari individu dan prinsip-prinsip transparansi serta pembatasan tujuan, memastikan bahwa data pribadi tidak diproses secara sewenang-wenang tanpa pengawasan yang memadai. Tingginya risiko kesalahan identifikasi, sebagaimana dialami dalam kasus pengeroyokan Ade Armando, menunjukkan bahwa setiap pelanggaran dalam pengolahan data dapat mengakibatkan dampak serius terhadap nama baik dan hak privasi seseorang. Kasus tersebut menimbulkan kekhawatiran akan potensi diskriminasi dan penyalahgunaan sistem hukum yang dapat merugikan individu yang tidak terlibat, sehingga perlindungan data harus diintegrasikan dengan sistem keamanan *cyber* yang handal.

Langkah-langkah keamanan siber yang komprehensif menjadi elemen kunci dalam menjaga integritas data pribadi dari ancaman peretasan, pencurian identitas, dan kebocoran data. Penyelenggara sistem elektronik diwajibkan untuk menerapkan protokol keamanan tinggi dan mekanisme enkripsi guna mencegah akses ilegal terhadap data biometrik. Pengawasan yang terus-menerus dan audit berkala juga diperlukan untuk mendeteksi kerentanan dan memperbaiki celah keamanan. Dalam kasus Abdul Manaf yang tersandung kesalahan identifikasi, aspek

keamanan *cyber* menjadi lebih krusial. Sistem pengenalan wajah yang tidak akurat, apabila dikombinasikan dengan kelemahan dalam pengamanan data, dapat mengakibatkan proses hukum yang tidak adil. Penguatan keamanan teknologi informasi harus menjadi prioritas agar kesalahan identifikasi tidak berujung pada pencemaran nama baik dan implikasi hukum yang merugikan.

Upaya peningkatan keamanan juga mencakup pembaruan sistem secara berkala, pelatihan bagi para operator, dan penyesuaian standar teknis agar sesuai dengan perkembangan teknologi. Langkah-langkah ini tidak hanya berfokus pada pengamanan data, tetapi juga memastikan bahwa setiap proses verifikasi identitas dilakukan dengan akurasi tinggi dan dijaga dari potensi manipulasi. Perbaikan terus-menerus pada algoritma pengenalan wajah sangat diperlukan untuk mengurangi bias yang terjadi akibat kondisi lingkungan atau penggunaan aksesori oleh subjek. Keterlibatan berbagai pihak, mulai dari lembaga pemerintah hingga sektor swasta, sangat penting dalam membangun ekosistem keamanan data yang kokoh. Sinergi antara regulator, penyedia teknologi, dan aparat penegak hukum harus terjalin dengan baik sehingga standar perlindungan data dapat diterapkan secara konsisten di semua lini. Kolaborasi ini juga membuka peluang untuk berbagi *best practices* dan mengoptimalkan sistem deteksi dini terhadap ancaman *cyber*. Selain itu, perlindungan data yang efektif harus selalu mempertimbangkan hak asasi manusia sebagai fondasi utamanya. Penggunaan teknologi pengenalan wajah yang didukung sistem keamanan siber yang handal, harus mampu menjaga kepercayaan publik dengan meminimalisir risiko diskriminasi dan pelanggaran privasi. Kebijakan yang mendukung keterbukaan informasi dan akuntabilitas penyelenggara sistem merupakan indikator penting dalam menciptakan lingkungan hukum yang adil dan transparan.

Sebagai bagian dari evaluasi berkelanjutan, standar teknis dan prosedur operasional perlu diperbarui sejalan dengan dinamika ancaman siber yang terus berkembang. Penerapan audit teknis dan verifikasi mandiri yang rutin dapat membantu memastikan bahwa setiap inovasi dalam teknologi pengenalan wajah sejalan dengan prinsip perlindungan data yang telah ditetapkan oleh regulasi nasional. Pendekatan ini juga memberikan ruang bagi perbaikan sistem yang responsif terhadap perubahan situasi. Hasil penelitian ini menekankan bahwa perlindungan data dan keamanan *cyber* merupakan dua pilar utama yang harus diintegrasikan untuk mengatasi ancaman hukum akibat kesalahan identifikasi

teknologi pengenalan wajah. Dengan adanya kerangka hukum yang jelas dan standar keamanan yang tinggi, diharapkan teknologi biometrik dapat memberikan manfaat optimal dalam penegakan hukum dan pengawasan, tanpa mengorbankan hak privasi serta keadilan bagi individu. Kolaborasi lintas sektor dan komitmen bersama dalam pembaruan sistem teknologi menjadi kunci untuk menciptakan ekosistem digital yang aman dan terpercaya.

Pengelolaan data dan keamanan siber memegang peran krusial dalam mencegah risiko hukum yang muncul akibat kesalahan identifikasi, terutama dalam penerapan teknologi pengenalan wajah. Selain perlunya regulasi yang jelas, penting juga untuk menerapkan langkah-langkah teknis yang memadai dan memastikan standar keamanan minimum yang konsisten. Salah satunya adalah penerapan sistem enkripsi yang kuat dan protokol keamanan tinggi untuk melindungi data biometrik dari akses tidak sah. Selain itu, sistem harus terus dipantau dan diaudit secara berkala guna mengidentifikasi potensi kelemahan serta memperbaikinya sebelum dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Tidak hanya itu, pihak pengelola teknologi juga wajib menjalani pelatihan agar mampu mengoperasikan sistem dengan cara yang benar dan etis. Perbaikan algoritma secara berkala juga diperlukan untuk meminimalkan risiko bias, misalnya akibat pengaruh lingkungan atau penggunaan atribut tertentu seperti kacamata atau penutup wajah. Sebagai contoh, di Tiongkok, pemerintah telah menetapkan standar nasional untuk teknologi pengenalan wajah yang mengutamakan akurasi tinggi dan menghindari potensi diskriminasi. Untuk mencapai hasil yang optimal, dibutuhkan kolaborasi antar berbagai pihak, termasuk regulator, penyedia teknologi, hingga aparat penegak hukum. Dengan adanya audit teknis secara rutin, verifikasi independen, serta komitmen kuat terhadap prinsip transparansi dan keadilan, penggunaan teknologi pengenalan wajah dapat berjalan secara efektif tanpa mengorbankan hak privasi dan keadilan individu.

KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, penerapan teknologi pengenalan wajah di Indonesia, seperti yang terlihat dalam kasus salah identifikasi Abdul Manaf, menimbulkan sejumlah tantangan hukum yang tidak sederhana, terutama dalam ranah pidana. Kesalahan sistem berpotensi menyebabkan pelanggaran privasi hingga munculnya ketidakadilan hukum bagi individu yang

tidak bersalah. Untuk mengatasi masalah ini, dibutuhkan langkah-langkah konkret yang dapat diimplementasikan oleh pembuat kebijakan. Langkah pertama yang perlu dipertimbangkan adalah penyempurnaan kerangka regulasi yang ada. Pemerintah sebaiknya segera menerbitkan aturan turunan dari UU Perlindungan Data Pribadi (PDP) No. 27 Tahun 2022 yang secara khusus mengatur penggunaan teknologi pengenalan wajah. Aturan ini harus mencakup standar teknis yang jelas, batasan penggunaan data, serta sanksi tegas bagi pelanggaran, agar pemanfaatannya tidak semata-mata bergantung pada interpretasi subjektif instansi terkait.

Kemudian, penting juga untuk mendirikan lembaga pengawas yang independen dan memiliki kapasitas teknis untuk melakukan audit serta evaluasi berkala terhadap sistem pengenalan wajah yang digunakan oleh instansi pemerintah maupun swasta. Lembaga ini diharapkan mampu mendeteksi potensi bias algoritma, memastikan transparansi, serta mencegah penggunaan teknologi yang berpotensi diskriminatif atau merugikan Masyarakat dan tidak kalah penting adalah memperkuat sinergi antar berbagai pihak terkait. Pemerintah, penyedia teknologi, akademisi, hingga organisasi masyarakat perlu duduk bersama untuk menyusun pedoman penggunaan teknologi yang etis, transparan, dan bertanggung jawab. Selain itu, edukasi kepada masyarakat tentang hak privasi dan risiko penggunaan teknologi biometrik perlu digalakkan guna meningkatkan kesadaran publik dan memberikan kontrol lebih besar atas data pribadi mereka.

DAFTAR PUSTAKA

Asshiddiqie, Jimly. *Hukum Pidana: Suatu Pengantar*. Sinar Grafika, 2021.

Bah, Serign Modou, dan Fang Ming. *An Improved Face Recognition Algorithm and its Application in Attendance Management System*. 5, no. 20 (2020). https://www.sciencedirect.com/science/article/pii/S2590005619300141.

Calo, Ryan. "The Case for a Federal Robotics Commission: Lessons from Privacy Law." *ale Journal of Law and Technology* 1, no. 1 (2020).

CNN Indonesia. "IPW Sentil Polisi Salah Tetapkan Tersangka Pengeroyok Ade Armando." CNN Indonesia. Diakses 9 April 2025. https://www.cnnindonesia.com/nasional/20220414141540-12-784875/ipw-sentil-polisi-salah-tetapkan-tersangka-pengeroyok-ade-armando.

Galič, Maša, dan Lonneke Stevens. "Regulating Police Use of Facial Recognition Technology in The Netherlands: The Complex Interplay Between Criminal Procedural Law and Data Protection Law." *New Journal of European Criminal Law* 14, no. 4 (2023): 459–78. https://doi.org/10.1177/20322844231212834.

Harkrisnowo, Harkristuti. *Hukum Privasi di Indonesia: Tinjauan Terhadap Perlindungan Data Pribadi*. PT Citra Aditya Bakti, 2018.

Isra, Saldi. *Hukum Pidana: Suatu Pengantar*. PT RajaGrafindo Persada, 2017.

Isra, Saldi. *Perlindungan Hukum dalam Sistem Peradilan Pidana di Indonesia*. Sinar Grafika, 2019.

Jened, Rahmi. *Hukum Teknologi Informasi dan Komunikasi*. Sinar Grafika, 2015.

Juwana, Hikmahanto. *Hukum dan Teknologi Informasi*. Prenada Media, 2018.

Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi. "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital." Pusat Penelitian dan Pengkajian Perkara, dan Pengelolaan Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi, 2019.

Maharani, Bondan Ayu, Hasnaa Amelia Rahajeng, Triana T, dan Zahra Dwi Arianti. "Perlindungan Hukum Masyarakat Dari Dampak Negatif Penggunaan AI." *Media Hukum Indonesia (MHI)* 3, no. 2 (2025): 2. https://doi.org/10.5281/zenodo.15783168.

Nurbaningsih, Enny. *Hak Privasi dalam Hukum: Perlindungan Hak Privasi di Era Globalisasi*. Pustaka Yustisia, 2017.

Nurkamal, Akmal Zulham, dan Laras Astuti. "Perlindungan Hukum Korban Terhadap Pelanggaran Hak Privasi Dalam Pembuatan Konten Menggunakan Drone." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 3 (2024): 3. https://doi.org/10.18196/ijclc.v5i3.23254.

Nussbaum, Martha Craven. *Creating Capabilities: The Human Development Approach*. Harvard University Press, 2021.

Priambodo, Bagas Wahyu, dan Dipo Wahjoeono. "Perlindungan Hukum Terhadap Penggunaan Teknologi Biometrik Dalam Transaksi Perbankan Untuk Meningkatkan Keamanan." *Madani: Jurnal Ilmiah Multidisiplin* 1, no. 11 (2023): 11. https://doi.org/10.5281/zenodo.10276789.

Rahman, Anfa'un Nisa' Fidinir, Syariffudin Syariffudin, dan Fathol Bari. "Perlindungan Hukum Terhadap Korban Penyalahgunaan Teknik Deepfake." *Perspektif Administrasi Publik Dan Hukum* 2, no. 1 (2025): 247–55. https://doi.org/10.62383/perspektif.v2i1.202.

Rambe, Rahmat, dan Lukman Abdurrahman. "Implikasi Etika Dan Hukum Dalam Penggunaan Teknologi Pengenalan Wajah: Perlindungan Privasi Versus Keamanan Publik." *Jurnal Hukum Caraka Justitia* 4, no. 2 (2024): 90–104. https://doi.org/10.30588/jhcj.v4i2.1828.

Raposo, Vera Lúcia. "The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal." *European Journal on Criminal Policy and Research* 29, no. 4 (2023): 515–33. https://doi.org/10.1007/s10610-022-09512-y.

Sarabdeen, Jawahitha. "Protection of the rights of the individual when using facial recognition technology." *Heliyon* 8, no. 3 (2022): e09086. https://doi.org/10.1016/j.heliyon.2022.e09086.

Soekanto, Soerjono. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. PT. Raja Grafindo Persada, 2020.

Sutedja, Bambang. *Teori Hukum Teknologi Informasi*. Rajawali Pers, 2020.

Sutrisno, Bambang. *Privasi dalam Hukum: Perlindungan Privasi dalam Era Digital*. PT Elex Media Komputindo, 2019.

Tarigan, Fredi Syahlulus. "Implikasi Hukum Terhadap Penggunaan Teknologi Pengenalan Wajah Kajian Literatur." *Judge : Jurnal Hukum* 4, no. 01 (2023): 01. https://doi.org/10.54209/judge.v4i01.375.

Utegen, D., dan B. Zh Rakhmetov. “Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models.” ARTICLES. *Journal of Digital Technologies and Law* 1, no. 3 (2023): 3. https://doi.org/10.21202/jdtl.2023.36.