JURNAL HUKUM CARAKA JUSTITIA | Vol. 4 No. 2 | November 2024 | p. 90 - 104

IMPLIKASI ETIKA DAN HUKUM DALAM PENGGUNAAN TEKNOLOGI PENGENALAN WAJAH: PERLINDUNGAN PRIVASI VERSUS KEAMANAN PUBLIK

Rahmat Rambe
Lukman Abdurrahman
Sistem Informasi, Fakultas Rekayasa Industri, Telkom University
gyurahmat@student.telkomuniversity.ac.id

Abstract

Facial recognition technology has been widely applied in everyday life and raises pros and cons, especially in the legal and ethical realms related to protecting privacy and public security. This research investigates the moral and legal implications of implementing this technology, with a focus on the conflict between individual privacy and public safety. Through a comprehensive literature review, this research analyzes various relevant views and findings. Researchers' conclusions often highlight the dilemma between ethics and law in the use of facial recognition technology, emphasizing the importance of striking a balance between protecting privacy and public safety. This research aims to make a significant contribution to understanding this debate and promoting responsive and fair policy.

Keywords*: Facial Recognition Technology; Ethics; Law; Privacy Protection; Public Security*.

Abstrak

Penggunaan teknologi pengenalan wajah telah banyak diterapkan dalam kehidupan sehari-hari dan menimbulkan pro dan kontra, terutama di ranah hukum dan etika terkait perlindungan privasi dan keamanan publik. Penelitian ini menyelidiki implikasi etika dan hukum dalam penerapan teknologi ini, dengan fokus pada pertentangan antara privasi individu dan keamanan publik. Melalui kajian literatur yang komprehensif, penelitian ini menganalisis berbagai pandangan dan temuan yang relevan. Temuan peneliti sering kali menyoroti dilema antara etika dan hukum dalam penggunaan teknologi pengenalan wajah, menekankan pentingnya keseimbangan antara perlindungan privasi dan keamanan publik. Penelitian ini bertujuan memberikan kontribusi signifikan dalam memahami perdebatan ini dan mendorong kebijakan yang responsif dan adil.

Kata kunci: Teknologi Pengenalan Wajah; Etika; Hukum; Perlindungan Privasi; Keamanan Publik.

A. Pendahuluan

Teknologi pengenalan wajah adalah suatu terobosan yang sangat penting dalam bidang teknologi informasi dan komunikasi. Penggunaan teknologi ini tidak hanya memberikan kemudahan dalam mengotentikasi pengguna, tetapi juga menjadi alat pengawasan yang lebih canggih dalam berbagai sektor, seperti keamanan perangkat elektronik, penegakan hukum, pengawasan publik dan banyak lainnya. Seiring dengan kemajuan teknologi pengenalan wajah ini, sering menjadi pro dan kontra di kalangan publik, sehingga menimbulkan beberapa pertanyaan publik terutama mengenai etika dan hukum yang terkait dalam ranah penggunaannya. Salah satu hal yang menjadi kontra di kalangan publik terkait etika dan hukum dalam penggunaan teknologi pengenalan wajah adalah mengenai lingkup perlindungan privasi individu atau pengguna dan keamanan publik.

Di tengah perkembangan teknologi yang sangat pesat, timbul kekhawatiran mengenai seberapa besar potensi terjadinya penyalahgunaan dan invasi terhadap privasi individu/pengguna dalam penggunaan teknologi pengenalan wajah dan perkembangan teknologi yang semakin meningkat. Meskipun teknologi pengenalan wajah memberikan manfaat yang sangat signifikan mengenai keamanan dan efisiensinya, tetapi tetap akan ada penggunaan teknologi tersebut menjadi masalah yang serius terutama mengenai hak-hak individu khususnya mengenai privasi dan kebebasan pribadi. Penggunaan teknologi pengenalan wajah yang merupakan bagian dari transformasi teknologi di era modern saat ini banyak sekali diterapkan dalam berbagai konsep, seperti keamanan, komunikasi perdagangan elektronik dan lain-lain. Perkembangan teknologi pengenalan wajah saat ini, dalam hal ini diperlukan penyelidikan mengenai implikasi hukum yang muncul.

Teknologi Pengenalan Wajah atau dalam bahasa inggris sering dikenal sebagai *Facial Recognition Technology* (FRT) adalah salah satu teknologi biometri yang tersedia dan bertujuan untuk mengidentifikasi suatu individu dengan mengukur dan menganalisis karakteristik fisiologis atau perilaku manusianya[1]. Proses FRT sendiri mengatakan bahwa gambar wajah seseorang yang dibandingkan dalam sampel gambar wajah orang lain dalam suatu *database*, memberikan skor atau bukti bahwa gambar yang dibandingkan merujuk pada orang yang sama. FRT selain untuk verifikasi identitas digunakan juga untuk pemrosesan data biometri dan membuat profil individu, dengan tujuan untuk menganalisis pola dan membuat kesimpulan tentang perilaku dan emosi.

Literatur *review* atau kajian literatur adalah suatu ringkasan yang didapatkan dari suatu

[1] Fontes Catarina, & Christian Perrone. n.d. "Ethics of Surveillance: Harnessing the Use of Live Facial Recognition Technologies in Public Spaces for Law Enforcement" (Technical University of Munich, 2021).

sumber bacaan yang berkaitan dengan bahasan penelitian. Baik secara dari segi latar belakang yang membahas fungsi persiapan pengumpulan data aktual akan dituangkan dalam sebuah tinjauan literatur di dalam setiap survei dan penelitian eksperimental. Kajian literatur juga sering digunakan sebagai alat untuk menciptakan konteks masa lalu[2]. Kajian literatur mengenai aplikasi implikasi etika dan hukum dalam penggunaan teknologi pengenalan wajah pada saat ini menjadi sangat relevan digunakan dalam konteks ini, karena dengan menggunakan kajian literatur dapat menciptakan konteks masa lalu mengenai perkembangan teknologi pengenalan wajah dan kaitannya dengan etika dan hukum.

Dengan menganalisis berbagai pandangan, teori serta temuan yang dikaitkan dalam suatu literatur dapat dipahami secara mendalam mengenai tantangan dan konflik yang muncul antara perlindungan privasi individu/pengguna dan kebutuhan akan keamanan publik dalam konteks penggunaan teknologi tersebut. Alasan penggunaan kajian literatur sebagai metode pendekatan, karena dengan melakukan kajian literatur dapat menguraikan perspektif yang beragam dan berbeda mengenai isu dalam hal ini. Di mulai dari perspektif etika yang mempertimbangkan nilai moral, perspektif hukum yang mencakup regulasi dan kebijakan mengenai aturan penggunaan teknologi pengenalan wajah dan lainnya. Dengan pemahaman yang didapat dari kajian literatur mengenai isu tersebut secara kompleksitas, dapat diharapkan untuk mengidentifikasi solusi yang tepat dalam mencapai keseimbangan yang sesuai antara perlindungan privasi individu dan kebutuhan akan keamanan publik.

Dengan demikian, diharapkan membahas mengenai upaya-upaya dalam mengembangkan kerangka kerja regulasi yang sesuai dan etis untuk teknologi pengenalan wajah. Dapat juga mengidentifikasi kerangka kerja yang memadai untuk mengatur teknologi ini, serta memastikan bahwa hak individu seseorang tetap terlindungi menjaga keamanan dan ketertiban secara keseluruhan. Serta dilakukan pembahasan mengenai pentingnya menjaga penyebaran isu-isu tentang teknologi pengenalan wajah.

B. Kajian Teoretis

1. Teknologi Pengenalan Wajah (*Facial Recognition Technology*)

FRT adalah salah satu teknologi biometri yang tersedia yang bertujuan untuk mengidentifikasi individu dengan mengukur dan menganalisis karakteristik fisiologis atau

[2] Muannif Ridwan, Bahrul Ulum, & Fauzi Muhammad, "Pentingnya Penerapan Literature Review Pada Penelitian Ilmiah (The Importance Of Application Of Literature Review In Scientific Research)", *Jurnal Masohi* 2, no. 1 (2021): 42-51, http://journal.fdi.or.id/index.php/jmas/article/view/356.

perilaku manusia[3]. FRT adalah sebuah teknologi yang digunakan untuk mengenali dan mengidentifikasi wajah seseorang menggunakan komputer. Dalam pengenalan wajah, sistem menggunakan algoritme dan data tentang fitur-fitur wajah, seperti bentuk mata, hidung, dan bibir, untuk membedakan satu wajah dengan lainnya. Dalam artikel "*Face Recognition Technology: A Review*" yang diterbitkan pada tahun 2019 dalam jurnal IEEE Access[4], penulis menjelaskan bahwa pengenalan wajah menggunakan teknik-teknik seperti:

a. *Extraction of facial features*, yaitu sistem yang mengumpulkan data tentang fitur-fitur wajah, seperti bentuk mata, hidung, dan bibir.
b. *Feature normalization*, yaitu data fitur-fitur wajah diproses untuk menghilangkan varianbiabilitas dan membuatnya lebih mudah digunakan oleh sistem.
c. *Pattern recognition*: Sistem membandingkan data fitur-fitur wajah dengan *database* untuk mengidentifikasi wajah yang sesuai.

Menurut sumber lainnya, seperti artikel "*A Review on Face Recognition Techniques*" yang diterbitkan pada tahun 2020 dalam jurnal International *Journal of Advanced Research in Computer Science and Software Engineering*[5], pengenalan wajah juga menggunakan teknologi-teknologi lainnya, seperti:

a. *Deep learning*: Sistem menggunakan jaringan saraf tiruan untuk belajar dari data dan fitur wajah dan meningkatkan akurasi pengenalan.
b. *Biometric authentication*: Sistem menggunakan informasi biometri, seperti iris, *fingerprint*, atau *vena blood flow*, untuk meningkatkan keamanan pengenalan.

2. Hukum dan Etika

Hukum adalah sistem aturan atau norma yang dibuat dan diberlakukan oleh institusi atau otoritas yang berwenang, yang mengatur perilaku masyarakat, untuk menjaga ketertiban dan keadilan. Hukum bersifat wajib dan memiliki sanksi bagi yang melanggar. Etika adalah cabang filsafat yang berkaitan dengan prinsip moral dan nilai-nilai yang menentukan perilaku yang benar atau salah, baik atau buruk. Etika adalah panduan perilaku yang lebih bersifat pribadi dan sosial, yang tidak memiliki sanksi hukum, tetapi lebih kepada sanksi sosial atau moral[6].

[3] Fontes Catarina, & Christian Perrone. n.d., *Loc. Cit.*
[4] Cen, Feng, and Guanghui Wang, "Dictionary Representation of Deep Features for Occlusion-Robust Face Recognition", *IEEE Access* 7 (2019): 605-26595, https://doi.org/10.1109/ACCESS.2019.2901376.
[5] Kamini Solanki, & Prashant Pittalia. 2016, "Review of Face Recognition Techniques." *International Journal of Computer Applications* 133, no. 12 (January 2016): 0975 – 8887, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e1c48439ea50a7c59d3411b6c1b881bfa4b678f7
[6] Pujanarko Mung, Dan Victor, and Andreas Simanjuntak, "Problematika Etika Komunikasi Verbal dalam Penulisan

3. Hak Privasi Individu

Hak privasi adalah hak seorang individu untuk menentukan apakah data pribadi akan dikomunikasikan atau tidak kepada pihak lain[7]. Privasi individu adalah hak seseorang untuk mengendalikan informasi pribadi mereka dan melindungi diri dari pengawasan atau gangguan yang tidak diinginkan. Privasi mencakup berbagai aspek seperti[8] :

a. Privasi Informasi: Hak untuk mengendalikan informasi pribadi, seperti data medis, keuangan, dan komunikasi pribadi.
b. Privasi Fisik: Hak untuk bebas dari intervensi fisik atau gangguan, seperti pengawasan tanpa izin atau penyadapan.
c. Privasi Lokasi: Hak untuk bergerak dan berada di tempat tertentu tanpa pengawasan atau pelacakan yang tidak sah.
d. Privasi Komunikasi: Hak untuk menjaga kerahasiaan komunikasi, seperti surat, email, atau percakapan telepon.

4. Keamanan Publik

Keamanan publik adalah keadaan di mana masyarakat merasa aman dari ancaman terhadap keselamatan pribadi, harta benda, dan ketertiban umum. Keamanan Publik adalah suatu tindak pencegahan dan perlindungan dari kejadian-kejadian yang dapat membahayakan keselamatan dan keamanan masyarakat dari bahaya besar, cedera, atau kerusakan harta benda.

C. Metode Penelitian

Metode utama yang digunakan dalam pembahasan kali ini adalah metode kajian literatur. Di mana metode kajian literatur ini dapat digunakan mengeksplorasi implikasi etika dan hukum dalam pengelolaan teknologi pengenalan wajah, khususnya dalam konteks perlindungan privasi individu dan keamanan publik. Metode kajian literatur juga dapat digunakan untuk mengumpulkan informasi dan analisis informasi tersebut dari sumber-sumber yang relevan. Penelitian dengan menggunakan metode literatur digunakan dengan cermat untuk mendapatkan pemahaman mengenai data dan informasi yang komprehensif mengenai implikasi etika dan hukum dalam pengelolaan teknologi pengenalan wajah. Dari

Berita di Media Online". *Jurnal Citra* 9, no. 1 (2021).

[7] Willa Wahyuni, "Perbedaan Pelindungan Data Pribadi Dan Hak Privasi", https://www.hukumonline.com/berita/a/perbedaan-pelindungan-data-pribadi-dan-hak-privasi-lt634028ec159e2/ (diakses 29 Juli 2024).

[8] Sekaring Ayumeida Kusnadi, & Andy Usmina Wijaya, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi", *Al Wasath Jurnal Ilmu Hukum* 2, no. 1 (2021): 9-16, https://doi.org/10.47776/alwasath.v2i1.127.

penerapan metode kajian literatur ini diharapkan peneliti dapat memperoleh pemahaman yang komprehensif tentang isu-isu yang kompleks mengenai etika, hukum, teknologi pengenalan wajah dari berbagai perspektif[9].

Dalam menggunakan metode kajian literatur, ada beberapa langkah dan tahapan dalam penggunaan metode tersebut. Penjelasan langkah-langkahnya adalah sebagai berikut:

1. Identifikasi sumber informasi, yaitu mengidentifikasi sumber informasi yang relevan terkait topik penelitian dan pembahasan seperti jurnal, buku dan lainnya.
2. Seleksi sumber informasi, yaitu menganalisis sumber-sumber yang telah di identifikasi agar menemukan relevansinya dengan topik penelitian. Hanya sumber yang memiliki hubungan dengan implikasi etika dan hukum dalam pengelolaan atau penggunaan teknologi pengenalan wajah yang dapat digunakan.
3. Analisis dan sintesis informasi, yaitu informasi yang diperoleh dari sumber yang relevan akan dianalisis kembali secara kritis untuk mengidentifikasi teman, tren, dan temuan-temuan penting tentang implikasi etika dan hukum dalam pengelolaan atau penggunaan teknologi pengenalan wajah.
4. Sintesis temuan, yaitu maksudnya adalah temuan yang telah berhasil di identifikasi dari proses analisis sebelumnya akan disintesis menjadi sebuah narasi yang koheren dan komprehensif. Dalam hal ini akan melibatkan secara langsung pengorganisasian informasi yang relevan menjadi beberapa tema atau sub tema yang memudahkan pembaca dalam memahami mengenai implikasi etika dan hukum dalam penggunaan teknologi pengenalan wajah.
5. Evaluasi dan interpretasi, yaitu mengenai temuan yang telah disintesis kemudian dievaluasi dan diinterpretasikan dalam konteks pertanyaan penelitian. Dalam hal ini melibatkan penafsiran terhadap implikasi etika dan hukum dari penggunaan teknologi pengenalan wajah, serta menarik suatu kesimpulan yang relevan untuk mendukung argumen penelitian.

D. Hasil Penelitian dan Pembahasan

Orang pertama yang mengemukakan gagasan tentang privasi adalah Warren dan Brandheis, di mana mereka berdua menerbitkan sebuah artikel berjudul "Hak atas Privasi" di sebuah majalah akademik *Harvard University Law School*. Menurut Warren dan Brandheis, dengan adanya perkembangan teknologi yang semakin pesat, kesadaran bahwa individu

[9] Rifka Agustianti, Lissiana Nussifera, *et. al.*, *Metode Penelitian Kuantitatif dan Kualitatif* (Makasar: CV Tohar Media, 2022).

memiliki hak untuk menikmati kehidupan mereka tanpa gangguan, serta hak untuk tidak melanggar privasi mereka oleh pemerintah atau pihak lain mulai muncul. Oleh karena itu, hak atas privasi sebagai kebutuhan untuk mengakui bahwa individu, kelompok, atau institusi memiliki hak untuk membuat keputusan independen tentang pengungkapan informasi diri mereka[10]. Ketika orang lain mendapatkan informasi pribadi seseorang, mengamati mereka, atau mendapatkan akses terhadap mereka, hak privasi orang tersebut telah dilanggar. Penting bagi kita untuk di ingat bahwa hak atas privasi itu harus selalu dihormati dan tidak dapat diabaikan.

Setiap manusia yang berada di dunia dan hidup di atas dunia ini memiliki hak-hak terhadap hidupnya, termasuk salah satunya yaitu hak dalam mendapatkan keamanan terhadap data pribadi. Indonesia sendiri merupakan negara hukum yang sangat menegaskan atas hak perlindungan informasi data pribadi pada beberapa peraturan perundang-undang seperti Pasal 28 G ayat (1) UUD 1945 yang menyatakan bahwa setiap orang berhak atas perlindungan data diri pribadi, keluarga, kehormatan, martabat, dan harta benda. UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta UU Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Pasal 26 ayat (1) yang mengatur bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.

Perlindungan terhadap data pribadi menurut Pasal 1 ayat (2) UU PDP adalah segala upaya yang dilakukan dalam melindungi data pribadi individu dalam rangkaian pemrosesan atau pengelolaan data pribadi untuk menjamin suatu hak konstitusional subjek data pribadi. Data pribadi sendiri terdiri atas 2 kategori, yaitu data spesifik yang mana didalamnya mencakup rincian mengenai kesehatan, biometri, genetika, catatan kriminal, data tentang anak, rincian keuangan, dan data lainnya sebagaimana yang ditentukan oleh kerangka hukum dan data umum yang mencakup mengenai informasi pribadi (alamat, nama lengkap, jenis kelamin, kebangsaan, agama, status perkawinan, atau data pribadi lainnya yang terlibat secara kolektif dalam hal membedakan suatu individu)[11]. Berdasarkan jenis data pribadi yang telah dipaparkan sebelumnya, maka beberapa hal yang termasuk dalam hal seperti biometri dan genetika adalah salah satu jenis data pribadi yang spesifik yang sering ditemui pada kebanyakan jenis penggunaan teknologi perlindungan data informasi pribadi termasuk

[10] Denda Ginanjar, & Arief Fahmi Lubis, "Urgensi Perlindungan Data Pribadi Dalam Menjamin Keamanan Data", *Jurnal Hukum Dan HAM Wara Sains* 1, no. 01 (2022): 22, https://doi.org/10.58812/jhhws.v1i01.7.
[11] Tim Hukum Online, "Dasar Hukum Perlindungan Data Pribadi", https://www.hukumonline.com/berita/a/dasar-hukum-perlindungan-data-pribadi-lt638d55f57a6d0/ (diakses 1 Agustus 2024).

teknologi pengenalan wajah.

Perkembangan teknologi dan informasi pada zaman sekarang ini dapat menunjukkan peningkatan yang spesifik dalam hal memudahkan manusia dalam segala hal. Namun, kondisi ini tidak hanya menunjukkan peningkatan terhadap hal-hal yang positif saja, tetapi terjadi juga peningkatan pada hal-hal yang negatif, seperti yang bersifat kriminalitas. Tindakan kriminalitas yang terjadi biasanya di mana orang-orang dapat belajar dan mempelajari dengan mudah serta mencoba melakukan untuk memanfaatkan penggunaan teknologi dalam mencuri informasi data pribadi seseorang yang akan digunakan dalam hal kepentingan pribadi nantinya oleh Si pencuri. Oleh karena hal ini, di saat ini dibutuhkannya pengamanan yang lebih ketat dan yang spesifik untuk melindungi privasi data pribadi. Saat ini telah banyak berbagai hal dalam upaya yang dilakukan untuk menciptakan sistem keamanan terhadap data pribadi, seperti dimulai dari fitur *password* pola atau Pin dan hasilnya menunjukkan kurang efektif terhadap solusi dan rencana penggunaan fitur *password* dalam hal pengamanan data pribadi karena fitur *password* menggunakan pola atau Pin mudah ditebak oleh orang lain.

Perkembangan teknologi saat ini dikembangkan untuk mengatasi permasalahan terhadap perlindungan data pribadi, pengamanan dan pengembangan fitur baru pengganti *password* yaitu fitur sidik jari. Fitur sidik jari di sini akan mengumpulkan data pribadi seperti biometri yang mana cukup mampu dalam hal mengamankan informasi pribadi, tetapi dikemudian hari menimbulkan permasalahan di mana dalam hal kasus ketika tangan yang digunakan sedang dalam kondisi kotor atau luka, sehingga sensor terhadap pengenalan sidik jari tidak merespons dan dapat dikenali sehingga proses terhambat. Untuk mengatasi masalah tersebut, dikembangkanlah fitur teknologi pengenalan wajah dalam hal upaya perlindungan data informasi pribadi yang lebih optimal. Dalam penggunaannya, teknologi pengenalan wajah ini cukup membantu dan memudahkan pengamanan informasi pribadi di dalam perangkat, seperti *handphone*.

Salah satu contoh penggunaan teknologi pengenalan wajah di berbagai sektor seperti di bandara dan daerah perbatasan digunakan untuk pemeriksaan identitas penumpang, mempercepat proses imigrasi, dan mengidentifikasi individu yang dicari oleh otoritas. Dalam sistem CCTV penggunaan teknologi pengenalan wajah digunakan untuk memantau kerumunan, mendeteksi perilaku mencurigakan, dan meningkatkan respons darurat jika terjadi sesuatu hal. Pada saat ini banyak perangkat modern yang telah menggunakan fitur teknologi pengenalan wajah untuk membuka kunci perangkat, memberikan lapisan keamanan tambahan di samping Pin atau kata sandi dan lainnya.

Pada perusahaan dan sekolah, fitur teknologi pengenalan wajah juga digunakan untuk mencatat kehadiran karyawan atau siswa secara otomatis, hal ini menggantikan metode tradisional seperti absensi manual atau kartu identitas. Pada toko ritel juga teknologi pengenalan wajah digunakan menggunakan kamera untuk menganalisis demografi pelanggan dan menampilkan iklan yang relevan dilayar digital. Di beberapa restoran dan hotel juga menggunakan teknologi pengenalan wajah untuk mengenali pelanggan tetap dan memberikan layanan yang dipersonalisasi. Pada bank dan institusi keuangan juga menggunakan pengenalan teknologi wajah untuk memverifikasi identitas nasabah saat membuka akun, *login* ke aplikasi *mobile banking*, atau melakukan transaksi *online*. Platform media sosial yang umum digunakan pada zaman sekarang seperti *Facebook* maupun yang lainnya menggunakan teknologi wajah untuk menandai (*Tag*) orang lain dalam foto secara otomatis.

Aplikasi seperti *Snapchat* dan *Instagram* juga menggunakan pengenalan wajah untuk menerapkan filter AR yang mengikuti gerakan mimik wajah pengguna. Rumah sakit dan klinik juga banyak menggunakan teknologi pengenalan wajah untuk memverifikasi identitas pasien, memastikan catatan medis yang akurat, dan meningkatkan keamanan terhadap akses ke data kesehatan pasien. Penelitian dan beberapa aplikasi kesehatan mental juga menggunakan fitur teknologi pengenalan wajah dalam hal untuk mendeteksi dan menganalisis emosi pengguna, membantu dalam diagnosis dan perawatan pengguna.

Beberapa sistem transportasi umum saat ini menggunakan fitur pengenalan wajah untuk mengidentifikasi penumpang dan mengintegrasikan dengan sistem tiket elektronik, upaya peningkatan efisiensi dan keamanan. Kepolisian juga menggunakan pengenalan wajah untuk mengidentifikasi dan melacak pelaku kejahatan melalui rekaman CCTV atau gambar dari tempat kejadian suatu perkara. Dengan digunakannya teknologi fitur pengenalan wajah untuk mengenali individu dalam kerumunan selama demonstrasi atau acara publik besar sangat bermanfaat dan banyak digunakan. Teknologi pengenalan wajah semakin terus berkembang dan aplikasinya semakin luas dan memberikan banyak manfaat, namun juga memunculkan tantangan terkait privasi dan etika yang harus dikelola dengan lebih bijak.

Pada zaman sekarang ini yang mana perkembangan teknologi semakin canggih dan berkembang, pelayanan jasa maupun barang juga ikut berubah menjadi modern dengan digunakannya teknologi, salah satunya teknologi pengenalan wajah untuk perlindungan data pribadi dalam sistem elektronik. Teknologi pengenalan wajah yang awalnya bermanfaat dan memudahkan dalam mengenali seseorang dapat berdampak negatif, di mana teknologi pengenalan wajah memungkinkan pengawasan massal tanpa persetujuan individu, yang

dianggap sebagai pelanggaran hak privasi. Dalam banyak kasus yang terjadi, seorang individu mungkin tidak menyadari bahwa mereka sedang diawasi, dan data wajah mereka disimpan bahkan dianalisis seseorang. Mereka juga mungkin tidak mengetahui jika misalnya teknologi yang merekam wajah mereka dan kemudian digunakan untuk membuat video *deepfake*, yang mana akan merusak reputasi individu atau digunakan untuk menipu publik.

Data wajah atau data pribadi yang dicuri dapat digunakan oleh pihak ketiga untuk melakukan penipuan atau pencurian identitas. Misalnya, seseorang dapat menggunakan data wajah orang lain atau informasi pribadi data orang lain untuk mengakses akun bank atau informasi pribadi lainnya. Teknologi ini memungkinkan identifikasi dan verifikasi identitas individu secara otomatis berdasarkan fitur wajar mereka. Meskipun memiliki potensi besar dalam pencegahan kejahatan dan peningkatan keamanan, penggunaan teknologi pengenalan wajah menimbulkan berbagai dilema etis yang perlu diperhatikan dengan sangat serius.

Teknologi pengenalan wajah juga memiliki potensi untuk memperburuk ketidakadilan dan diskriminasi yang sudah ada. Jika tidak diawasi dengan baik, teknologi ini dapat digunakan secara tidak proporsional terhadap kelompok minoritas, meningkatkan risiko diskriminasi dan pelanggaran hak-hak mereka. Penggunaan teknologi pengenalan wajah harus diatur untuk memastikan bahwa penerapannya adil dan tidak diskriminatif. Hal ini termasuk ke dalam pengembangan kebijakan yang menjamin bahwa teknologi ini tidak digunakan untuk menargetkan atau memprofilkan kelompok tertentu secara tidak adil. Pengawasan yang terus- menerus melalui teknologi pengenalan wajah yang dapat menimbulkan dampak sosial dan psikologis yang signifikan. Seorang individu mungkin bisa merasa tidak nyaman atau tertekan oleh pengawasan yang konstan, di mana dapat mempengaruhi perilaku dan kebebasan mereka dalam kehidupan sehari-hari. Selain itu, rasa takut akan diawasi juga dapat mempengaruhi partisipasi dalam kegiatan publik, seperti demonstrasi atau protes yang mana merupakan bagian penting dari hak demokratis.

Penggunaan teknologi pengenalan wajah harus sesuai dengan prinsip-prinsip hak asasi manusia, termasuk didalamnya hak privasi. Oleh karena itu, penting bagi pemerintah dan lembaga yang menggunakan fitur teknologi pengenalan wajah untuk bersikap transparan tentang bagaimana data dikumpulkan, digunakan, dan disimpan. Selain itu, individu harus memiliki hak untuk mengetahui kapan dan di mana teknologi ini digunakan, serta tujuan penggunaannya. Akurasi suatu teknologi pengenalan wajah sangat penting, terutama dalam konteks penegakan hukum. Kesalahan dalam identifikasi dapat menyebabkan konsekuensi serius, termasuk penahanan yang salah dan pelanggaran terhadap hak-hak individu. Bias dalam teknologi pengenalan wajah sering kali berasal dari data pelatihan yang tidak

seimbang. Upaya dalam mengurangi bias ini, diperlukannya upaya untuk memastikan bahwa *data set* yang digunakan untuk melatih algoritme pengenalan wajah yang mencerminkan keragaman suatu populasi. Selain itu, pengujian dan validasi yang ketat juga harus dilakukan untuk memastikan bahwa sistem tersebut berfungsi dengan baik untuk semua kelompok demografi[12].

Keamanan publik adalah konsep yang mencakup perlindungan masyarakat dari suatu ancaman, bahaya, dan risiko yang dapat membahayakan keselamatan seseorang. Hal ini melibatkan berbagai aspek, seperti termasuk pencegahan kejahatan, respons terhadap bencana, pengelolaan lalu lintas, dan tindakan untuk menjaga ketertiban umum. Strategi pencegahan kejahatan melibatkan penegakan hukum yang efektif, penggunaan teknologi pengawasan, patroli polisi, dan program-program komunitas. Pencegahan ini bertujuan untuk mengurangi kesempatan terhadap tindakan kriminal dan meningkatkan rasa aman di masyarakat. Penegakan hukum adalah salah satu pilar utama keamanan publik. Polisi, jaksa, dan lembaga penegak hukum lainnya bertugas untuk menegakkan undang-undang, menangkap pelaku kejahatan, dan memastikan bahwa pelanggaran hukum harus mendapatkan sanksi yang sesuai.

Penyalahgunaan teknologi pengenalan wajah dapat mengurangi kepercayaan publik terhadap pemerintah dan perusahaan yang menggunakannya. Kurangnya akan transparansi dan akuntabilitas dapat membuat individu merasa tidak aman dan kurang percaya terhadap teknologi yang ada. Di Indonesia sendiri, berbagai peraturan perundang-undangan telah diadopsi untuk melindungi data pribadi dan publik. Pada Oktober 2022, Indonesia telah mengesahkan UU PDP untuk melindungi data pribadi individu yang diproses oleh entitas publik dan swasta. Undang-undang ini akan mencakup hak individu tersebut atas data pribadi mereka sendiri dan kewajiban pengendali data dalam pengumpulan, penyimpanan, penggunaan, dan pemusnahan data pribadi. UU PDP juga memberikan hak kepada individu untuk mengakses, mengoreksi, menghapus, dan membatasi pemrosesan data pribadi. Seorang individu berhak memiliki hak untuk menarik persetujuan pemrosesan data kapan saja.

Selain UU PDP, ada juga terdapat undang-undang lain seperti UU ITE. UU ITE mengatur penggunaan teknologi informasi dan transaksi elektronik, termasuk perlindungan data dalam ruang digital. UU ITE juga memberikan dasar hukum untuk penegakan hukum terhadap pelanggaran keamanan data. Selain itu juga terdapat PP Nomor 71 Tahun 2019

[12] Denda Ginanjar, & Arief Fahmi Lubis, *Op. cit*., 25.

tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) yang mengatur penyelenggaraan sistem dan transaksi elektronik di mana didalamnya terdapat kewajiban pengelola sistem elektronik untuk melindungi data pribadi pengguna. PP PSTE juga mewajibkan penyelenggara sistem elektronik untuk menerapkan standar keamanan informasi yang sangat memadai. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 mengenai perlindungan data pribadi dalam sistem elektronik, peraturan ini memberikan pedoman teknis untuk perlindungan data pribadi di dalam sistem elektronik, termasuk kewajiban pengendali data untuk melindungi data dari akses yang tidak sah dan penyalahgunaan.

Salah satu tantangan yang paling utama adalah bagaimana memastikan kepatuhan terhadap UU PDP dan regulasinya. Hal ini memerlukan edukasi yang luas dan pemahaman yang mendalam oleh pemangku kepentingan. Seiring dengan perkembangan teknologi yang semakin pesat, tantangan dalam melindungi data pribadi dan publik menjadi sorotan dan permasalahan yang sangat kompleks. Teknologi baru seperti pengenalan wajah dan kecerdasan buatan membutuhkan regulasi yang adaptif dan responsif. Hal ini karena memerlukan peningkatan kesadaran publik akan hak-hak mereka atas data pribadi dan bagaimana langkah-langkah perlindungan yang tersedia merupakan hal penting untuk meminimalkan risiko penyalahgunaan dan pencurian data.

Untuk mengatasi tantangan etis yang terkait dengan teknologi pengenalan wajah dalam keamanan publik, berikut beberapa kebijakan yang dapat dipertimbangkan:

1. Transparansi dan Akuntabilitas, yaitu lembaga yang menggunakan teknologi pengenalan wajah harus transparan tentang penggunaan teknologi dan bertanggung jawab akan dampak dari penggunaannya. Audit dan penilaian independen harus juga dilakukan secara berkala guna memastikan kepatuhan terhadap standar etika dan hukum.
2. Persetujuan dan Informasi, yaitu setiap individu harus diberi informasi yang jelas dan rinci tentang penggunaan teknologi pengenalan wajah dan diberikan pilihan untuk menyetujui atau menolak penggunaannya dalam situasi tertentu.
3. Regulasi yang kuat, yaitu pemerintah harus dapat mengembangkan dan menerapkan regulasi yang ketat untuk mengatur penggunaan teknologi pengenalan wajah. Regulasi ini juga harus mencakup perlindungan privasi, pengurangan bias, dan jaminan keadilan serta non-diskriminasi.
4. Pengembangan dan Pengujian yang Etis, yaitu pengembangan teknologi pengenalan wajah harus memastikan bahwa produk harus diuji dan divalidasi secara etis dan ilmiah.

Disisi lain juga harus bekerja untuk mengurangi bias dan meningkatkan akurasi sistem, serta mempertimbangkan dampak sosial dari teknologi yang sedang dikembangkan.

5. Pendidikan dan Pelatihan, yaitu suatu pengguna teknologi pengenalan wajah, termasuk diantaranya aparat penegak hukum, harus menerima pendidikan dan pelatihan yang memadai tentang implikasi etis dan cara menggunakan teknologi secara bertanggung jawab.

Untuk melindungi suatu data pribadi dan data publik dalam penggunaan teknologi pengenalan wajah harus merekomendasikan beberapa hal yang bisa diambil dan meliputi langkah-langkah teknis, kebijakan, dan praktik yang memastikan privasi dan keamanan data. Salah satu contohnya, yaitu sebagai berikut:

1. Pastikan data wajah yang dikirim melalui jaringan dienkripsi untuk mencegah intersepsi oleh pihak yang tidak berwenang dan bertanggung jawab, dan juga mengenai data yang disimpan di server atau perangkat harus dienkripsi untuk memastikan privasi dan keamanan data;
2. Gunakan teknik anonimitasi untuk menghapus atau mengaburkan informasi yang dapat di identifikasi individu dari *data set* sebelum digunakan dalam analisis atau pelatihan model.
3. Selalu mengumpulkan data yang benar-benar diperlukan untuk tujuan spesifik dan menghindari pengumpulan data yang berlebih;
4. Membatasi selalu periode penyimpanan data pribadi sesuai dengan kebutuhan operasional dan kebijakan hukum yang berlaku. Serta menghapus data yang tidak lagi diperlukan secara aman;
5. Menerapkan kontrol akses yang berbasis peran untuk membatasi siapa yang dapat mengakses dan memproses data wajah serta selalu menggunakan *autentikasi multi-faktor* (MFA) sebagai tambahan keamanan;
6. Melakukan audit secara rutin dan pemantauan terhadap sistem pengenalan wajah untuk mendeteksi dan merespons insiden keamanan secara cepat dan tanggap;
7. Memberikan informasi yang jelas kepada individu tentang pengumpulan, penggunaan, dan penyimpanan data wajah mereka. Serta mendapatkan persetujuan eksplisit dari individu sebelum mengumpulkan data wajah mereka;
8. Melakukan penilaian akan dampak privasi sebelum mengimplementasikan teknologi wajah untuk mengidentifikasi dan mengurangi risiko terhadap privasi individu;
9. Memberikan pelatihan kepada karyawan tentang praktik perlindungan data dan kebijakan privasi dalam memastikan pentingnya akan cara melindungi data pribadi;

10. Menggunakan algoritme dan data pelatihan yang dirancang untuk meminimalkan bias rasial, gender, dan bias lainnya. Serta melakukan pengujian secara berkala dalam memastikan akurasi dan keadilan sistem;
11. Menyediakan mekanisme bagi setiap individu untuk mengajukan pengaduan terkait penggunaan data wajah mereka dan menyediakan jalan untuk pemulihan jika hak privasi mereka dilanggar.

E. Penutup

Penggunaan teknologi pengenalan wajah telah membawa dampak signifikan dalam berbagai aspek kehidupan sehari-hari, terutama dalam keamanan dan efisiensi. Namun, teknologi ini juga menimbulkan perdebatan mengenai implikasi etika dan hukum, terutama terkait dengan perlindungan privasi individu dan kebutuhan akan keamanan publik. Melalui kajian literatur yang komprehensif, temuan penelitian menunjukkan bahwa, meskipun teknologi pengenalan wajah dapat meningkatkan keamanan, ada risiko penyalahgunaan yang dapat mengancam privasi individu. Oleh karena itu, sangat penting untuk menemukan keseimbangan yang tepat seperti menciptakan regulasi penggunaan teknologi ini dan meningkatkan keamanan teknologi pengenalan wajah.

Daftar Pustaka

Artikel Jurnal

Feng, Cen, & Guanghui Wang. "Dictionary Representation of Deep Features for Occlusion-Robust Face Recognition". *IEEE Access* 7 (2019): 605-26595. https://doi.org/10.1109/ACCESS.2019.2901376.

Ginanjar, Denda, & Arief Fahmi Lubis. "Urgensi Perlindungan Data Pribadi Dalam Menjamin Keamanan Data". *Jurnal Hukum Dan HAM Wara Sains* 1, no. 01 (2022): 21-26. https://doi.org/10.58812/jhhws.v1i01.7.

Kusnadi, Sekaring Ayumeida, & Andy Usmina Wijaya. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi". *Al Wasath Jurnal Ilmu Hukum* 2, no. 1 (2021): 9-16. https://doi.org/10.47776/alwasath.v2i1.127.

Mung, Pujanarko, Victor, & Andreas Simanjuntak. n.d. "Problematika Etika Komunikasi Verbal Dalam Penulisan Berita di Media Online". *Jurnal Citra* 9, no. 1 (2021).

Ridwan, Muannif, Bahrul Ulum, & Fauzi Muhammad. "Pentingnya Penerapan Literature Review Pada Penelitian Ilmiah (The Importance Of Application Of Literature Review In Scientific Research)." *Jurnal Masohi* 2, no. 1 (2021): 42-51. http://journal.fdi.or.id/index.php/jmas/article/view/356.

Solanki, Kamini, & Prashant Pittalia. "Review of Face Recognition Techniques." *International*

Journal of Computer Applications 133, no. 12 (January 2016): 0975 – 8887. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e1c48439ea50a7c59d3411b6c1b881bfa4b678f7.

Buku

Agustianti, Rifka, Lissiana Nussifera, *et. al. Metode Penelitian Kuantitatif dan Kualitatif*. Makasar: CV Tohar Media, 2022.

Ringkasan Penelitian

Catarina, Fontes, & Christian Perrone. "Ethics of Surveillance: Harnessing the Use of Live Facial Recognition Technologies in Public Spaces for Law Enforcement." Technical University of Munich, 2021.

Internet

Platin, Rachel. n.d. "Big Brother Back Again: Facial Recognition Technology And The Need For Further Legal Protections." https://www.eff.org/pages/face-recognition (diakses 1 Juli 2024).

Tim Hukum Online. "Dasar Hukum Perlindungan Data Pribadi." https://www.hukumonline.com/berita/a/dasar-hukum-perlindungan-data-pribadi-lt638d55f57a6d0/ (diakses 1 Agustus 2024).

Wahyuni, Willa. "Perbedaan Pelindungan Data Pribadi Dan Hak Privasi." https://www.hukumonline.com/berita/a/perbedaan-pelindungan-data-pribadi-dan-hak-privasi-lt634028ec159e2/ (diakses 29 Juli 2024).