

## Analisis Etika dan Dampak Penggunaan Sistem Pengenalan Wajah untuk Manajemen Kehadiran di Lingkungan Sekolah

Dhi'fan Razaqa<sup>1</sup>, Muhammad Rezka Al Maghribi<sup>2</sup>, Nabilah Dwi Gunasti<sup>3</sup>, Theresia Wati<sup>4</sup>  
 Program Studi Informatika/Fakultas Ilmu Komputer  
 Universitas Pembangunan Nasional Veteran Jakarta  
 Pondok Labu, Kecamatan Cilandak, Kota Depok  
 2210511091@mahasiswa.upnvj.ac.id<sup>1</sup>, 2210511086@mahasiswa.upnvj.ac.id<sup>2</sup>,  
 2210511096@mahasiswa.upnvj.ac.id<sup>3</sup>, theresiawati@upnvj.ac.id<sup>4</sup>

**Abstrak.** Penggunaan sistem pengenalan wajah untuk manajemen kehadiran di sekolah menawarkan efisiensi dalam proses absensi dan peningkatan kedisiplinan siswa. Sistem ini memungkinkan absensi yang lebih cepat dan akurat serta membantu mengidentifikasi siswa yang sering terlambat atau bolos. Namun, teknologi ini menimbulkan kekhawatiran mengenai privasi, keamanan data, dampak psikologis, dan etika. Penelitian ini menggunakan metode tinjauan literatur sistematis untuk mengevaluasi dampak etis, psikologis, dan keamanan dari implementasi sistem pengenalan wajah di sekolah. Hasil menunjukkan bahwa meskipun teknologi ini meningkatkan efisiensi, terdapat risiko signifikan terhadap privasi siswa jika data tidak dikelola dengan baik. Oleh karena itu, sekolah harus menerapkan kebijakan privasi yang ketat dan standar keamanan tinggi untuk melindungi data biometrik siswa, serta memberikan edukasi kepada siswa dan orang tua mengenai penggunaannya. Penting untuk memiliki kebijakan yang transparan dan evaluasi berkala untuk memastikan penggunaan teknologi yang aman dan efektif, serta menghindari diskriminasi atau bias. Regulasi yang ketat diperlukan untuk memastikan penggunaan teknologi yang sesuai dengan hukum dan etika. Dengan langkah-langkah yang tepat, teknologi ini dapat meningkatkan proses belajar mengajar dan keamanan di sekolah tanpa mengorbankan privasi dan hak-hak individu.

Kata Kunci: Sistem Pengenalan Wajah, Absensi Siswa, Data Biometrik, Etika dan Dampak Teknologi

### 1 Pendahuluan

Berkembangnya teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam pendidikan, termasuk inovasi sistem pengenalan wajah (face recognition) untuk absensi di sekolah menengah. Sistem ini menggunakan Artificial Intelligence (AI) untuk mengidentifikasi siswa melalui data biometrik seperti gambar wajah, mengotomatiskan proses absensi, meningkatkan kedisiplinan siswa, dan menjaga keamanan sekolah. Selain mengurangi waktu pencatatan dan human error, sistem ini mempermudah identifikasi masalah ketidakhadiran atau keterlambatan siswa, yang berpotensi meningkatkan prestasi akademik [1].

Namun, penggunaan teknologi ini menimbulkan kekhawatiran terkait privasi dan keamanan data biometrik siswa. Data sensitif ini dapat disalahgunakan jika tidak dilindungi dengan baik, menimbulkan kekhawatiran di kalangan orang tua siswa. Selain itu, ada pertimbangan psikologis dan etis, seperti ketidaknyamanan siswa dan orang tua terhadap pemantauan ketat serta rasa privasi yang mungkin dilanggar. Oleh karena itu, penting bagi sekolah untuk mengelola data biometrik dengan standar keamanan tinggi dan pendekatan transparan.

Tujuan makalah ini adalah menganalisis dampak etis, psikologis, dan keamanan dari implementasi sistem pengenalan wajah di sekolah serta memberikan rekomendasi solusi yang mempertimbangkan prinsip-prinsip etika untuk meningkatkan perlindungan privasi dan keamanan data, serta mendukung penerimaan semua pihak terkait. Makalah ini membahas teknologi pengenalan wajah, implementasinya di sekolah, serta analisis manfaat dan tantangannya. Selain itu, makalah ini memberikan rekomendasi solusi untuk memastikan penggunaan sistem ini tidak mengancam privasi siswa, serta panduan praktis bagi sekolah dalam mengimplementasikan teknologi ini secara bertanggung jawab dan etis.

### 2 Tinjauan Pustaka

#### 2.1 Sistem Pengenalan Wajah (Face Recognition)

Sistem pengenalan wajah adalah teknologi biometrik yang menggunakan wajah manusia untuk identifikasi dan verifikasi. Karena wajah manusia memiliki keunikan dan karakteristik yang khas, teknologi ini dapat digunakan untuk kehadiran, pembuatan Kartu Tanda Penduduk, serta sistem keamanan [2].

### 2.2 Data Biometrik

Data biometrik adalah karakteristik fisik atau perilaku yang dapat mengidentifikasi seseorang secara unik, seperti DNA, sidik jari, wajah, dan pola suara [3].

### 2.3 Etika dalam Penggunaan Teknologi Informasi

Etika dalam penggunaan teknologi informasi adalah kumpulan prinsip moral dan nilai-nilai yang memberikan arahan kepada individu dalam mengembangkan, menggunakan, dan mengelola teknologi informasi. Tujuan etika adalah memastikan bahwa teknologi tersebut dimanfaatkan secara bertanggung jawab dan sesuai dengan prinsip-prinsip moral yang berlaku. Prinsip etika ini meliputi pertimbangan terhadap aspek-aspek seperti privasi, keadilan, keamanan, dan distribusi kekuasaan dalam penggunaan teknologi informasi [4].

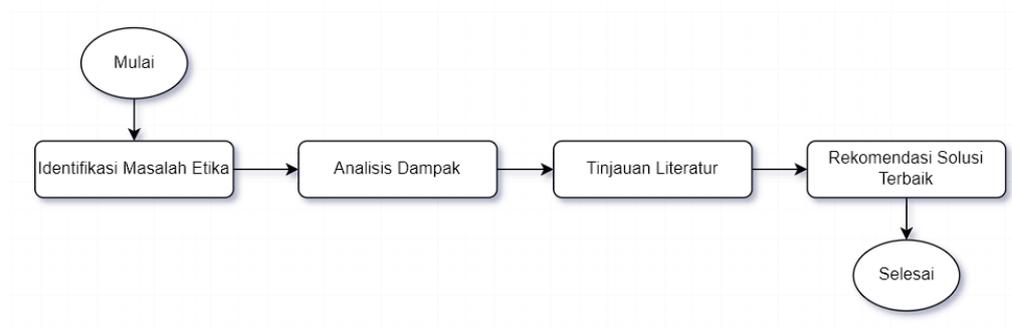
### 2.4 Implikasi Etika Sistem Pengenalan Wajah

Menyeimbangkan hak privasi individu dengan kebutuhan keamanan publik dalam penerapan sistem pengenalan wajah sangatlah penting. Teknologi ini menimbulkan berbagai kekhawatiran etis, termasuk privasi, transparansi, kesetaraan, keragaman, dan hak asasi manusia. Oleh karena itu, regulasi dan penilaian seperti Penilaian Dampak Hak Asasi Manusia harus diterapkan dalam pengembangan dan implementasi sistem pengenalan wajah [4].

### 2.5 Tinjauan Literatur Sistematis (Systematic Literature Review)

Tinjauan literatur sistematis merupakan metode yang efektif untuk mengidentifikasi, mengevaluasi, dan menginterpretasi semua penelitian yang relevan dengan pertanyaan penelitian atau topik tertentu dengan cara yang sistematis dan terorganisir [5].

## 3 Metodologi



**Gambar 2.** Tahapan Penelitian

### 3.1 Identifikasi Masalah Etika

Identifikasi dan penjelasan masalah etika yang muncul dari penggunaan sistem pengenalan wajah dalam studi kasus ini, termasuk pelanggaran privasi, potensi penyalahgunaan data, dan dampak psikologis pada siswa.

### 3.2 Analisis Dampak

Analisis dampak dari penggunaan sistem pengenalan wajah terhadap privasi siswa, kepercayaan orang tua terhadap sekolah, dan keamanan data pribadi

### 3.3 Tinjauan Literatur Sistematis (Systematic Literature Review)

Proses peninjauan literatur terkait etika penggunaan teknologi biometrik di lingkungan pendidikan, serta kode etik yang relevan bagi profesional TI.

### 3.4 Identifikasi Masalah Etika

Mengusulkan solusi-solusi yang mempertimbangkan prinsip-prinsip etika, seperti pembatasan penggunaan data biometrik, konsultasi dengan siswa dan orang tua, dan transparansi dalam penggunaan teknologi.

## 4 Hasil Dan Pembahasan

### 4.1 Identifikasi Masalah Etika

Dalam penggunaan sistem pengenalan wajah untuk mengelola kehadiran siswa di sekolah menengah, terdapat beberapa masalah etika signifikan yang perlu diidentifikasi dan dijelaskan. Berikut adalah masalah-masalah tersebut.

#### 1. Pelanggaran Privasi

Pengumpulan dan penyimpanan data biometrik, seperti gambar wajah, tanpa persetujuan yang eksplisit dan informasi yang jelas mengenai penggunaannya dapat dianggap sebagai pelanggaran privasi siswa. Data biometrik merupakan informasi pribadi yang sangat sensitif, dan pengelolaannya harus dilakukan dengan sangat hati-hati. Penting bagi sekolah untuk mendapatkan persetujuan yang jelas dan sukarela dari siswa dan orang tua sebelum mengimplementasikan sistem pengenalan wajah. Persetujuan ini harus mencakup penjelasan rinci mengenai bagaimana gambar wajah siswa akan dikumpulkan, disimpan, digunakan, dan dilindungi. Tanpa persetujuan yang benar-benar sukarela dan berdasarkan informasi lengkap, penggunaan teknologi ini dapat dianggap melanggar hak privasi individu.

#### 2. Potensi Penyalahgunaan Data

Data biometrik yang dikumpulkan untuk keperluan manajemen kehadiran memiliki risiko besar untuk disalahgunakan. Kekhawatiran utama adalah bahwa data ini dapat digunakan untuk tujuan lain di luar pencatatan kehadiran, seperti pemantauan perilaku siswa atau bahkan dibagikan dengan pihak ketiga tanpa izin. Hal ini dapat menimbulkan ketidakpercayaan dan rasa tidak aman di kalangan siswa dan orang tua. Selain itu, data biometrik yang bocor dapat menimbulkan risiko keamanan yang serius dan permanen bagi individu yang terdampak, mengingat data seperti wajah tidak dapat diubah seperti kata sandi. Oleh karena itu, sekolah harus menerapkan kebijakan privasi yang ketat dan transparan yang membatasi penggunaan data hanya untuk tujuan yang telah disetujui serta memastikan bahwa data tersebut disimpan dengan keamanan yang tinggi, termasuk enkripsi dan akses terbatas.

#### 3. Dampak Psikologis pada Siswa

Implementasi teknologi pengenalan wajah di sekolah dapat menimbulkan perasaan tidak aman dan terawasi di kalangan siswa. Mengetahui bahwa setiap pergerakan mereka diawasi dan dicatat bisa menyebabkan stres dan kecemasan, serta perasaan kehilangan privasi dan kebebasan. Rasa tidak aman ini juga dapat mengganggu proses belajar-mengajar, karena siswa mungkin merasa kurang nyaman dan terganggu dengan pemantauan yang terus-menerus. Selain itu, jika siswa merasa bahwa data mereka tidak aman atau bahwa privasi mereka tidak dihargai, ini dapat menurunkan tingkat kepercayaan mereka terhadap institusi sekolah. Hal ini dapat berdampak negatif pada kerjasama antara siswa, orang tua, dan sekolah serta menghambat perkembangan sosial dan emosional siswa. Penggunaan teknologi ini juga bisa menyebabkan pengucilan terhadap siswa tertentu, terutama jika data digunakan untuk menandai siswa yang sering absen atau terlambat, yang pada gilirannya dapat berdampak negatif pada perkembangan sosial dan emosional siswa serta proses belajar mereka.

Penggunaan sistem pengenalan wajah di sekolah menengah menimbulkan sejumlah masalah etika yang signifikan, termasuk pelanggaran privasi, potensi penyalahgunaan data, dan dampak psikologis pada siswa. Untuk mengatasi masalah ini, penting bagi sekolah untuk mendapatkan persetujuan yang jelas dan sukarela dari siswa dan orang tua, menerapkan kebijakan privasi yang ketat dan transparan, serta memastikan bahwa teknologi digunakan secara adil dan tidak diskriminatif. Dengan demikian, sekolah

dapat mengurangi risiko dan memastikan bahwa penggunaan teknologi pengenalan wajah memberikan manfaat yang maksimal tanpa mengorbankan hak dan kesejahteraan siswa

#### **4.2 Analisis Dampak**

Penggunaan sistem pengenalan wajah untuk mengelola kehadiran siswa di sekolah menengah membawa dampak yang signifikan terhadap berbagai aspek, termasuk privasi siswa, kepercayaan orang tua terhadap sekolah, dan keamanan data pribadi.

##### **1. Dampak Terhadap Privasi Siswa**

Pengumpulan data biometrik, seperti gambar wajah dan sidik jari, merupakan tindakan yang sensitif karena data ini unik dan tidak dapat diubah. Tanpa persetujuan yang jelas dan terinformasi dari siswa dan orang tua, pengumpulan data ini dapat menyebabkan siswa merasa bahwa privasi mereka dilanggar. Rasa diawasi secara terus-menerus dapat mengurangi rasa kebebasan dan privasi dalam lingkungan sekolah. Penggunaan sistem pengenalan wajah juga untuk memantau masuk dan keluarnya siswa dari kelas atau area tertentu dapat menciptakan lingkungan yang terasa menekan. Pengawasan yang intensif ini bisa menyebabkan siswa merasa tidak nyaman atau tertekan, yang berdampak negatif pada konsentrasi dan kenyamanan mereka dalam belajar.

##### **2. Dampak Terhadap Interaksi Sosial dan Perkembangan Emosional**

Sistem pengenalan wajah yang digunakan untuk menandai siswa tertentu, misalnya yang sering terlambat atau absen, dapat menyebabkan siswa merasa dipermalukan atau dijauhi oleh teman-teman mereka. Hal ini dapat mempengaruhi interaksi sosial dan perkembangan emosional siswa secara negatif. Dalam jangka panjang, hal ini bisa menurunkan motivasi belajar dan keterlibatan mereka di sekolah. Peraturan yang terlalu ketat juga dapat memotivasi siswa untuk mencari celah untuk mengelabui sistem dan terlibat dalam kenakalan serta pelanggaran.

##### **3. Dampak Terhadap Kepercayaan Orang Tua**

Orang tua menginginkan jaminan bahwa data pribadi anak-anak mereka akan dijaga dengan aman. Jika mereka merasa bahwa privasi anak mereka terancam atau bahwa data dapat disalahgunakan, tingkat kepercayaan mereka terhadap sekolah bisa menurun. Ketidakpercayaan ini dapat mempengaruhi hubungan antara orang tua dan pihak sekolah, membuat komunikasi dan kerjasama menjadi lebih sulit. Orang tua mungkin juga khawatir tentang bagaimana data biometrik siswa akan disimpan dan dilindungi, dengan ancaman kebocoran data atau penyalahgunaan informasi pribadi menjadi sumber kekhawatiran yang serius.

##### **4. Dampak Terhadap Keamanan Data Pribadi**

Keamanan data pribadi merupakan aspek kritis dalam penggunaan teknologi pengenalan wajah. Data biometrik yang bocor atau disalahgunakan dapat menciptakan risiko besar, termasuk penipuan, penculikan, dan perdagangan anak. Sekolah harus transparan mengenai langkah-langkah keamanan yang diterapkan dan memastikan bahwa data siswa dilindungi dengan teknologi enkripsi dan protokol keamanan yang kuat. Jika terjadi insiden keamanan seperti kebocoran atau akses yang tidak sah terhadap data biometrik siswa, hal ini bisa memperburuk kepercayaan orang tua terhadap sekolah. Kegagalan dalam menanggapi insiden dengan baik bisa berdampak jangka panjang pada reputasi sekolah dan kepercayaan masyarakat.

##### **5. Dampak Terhadap Kepatuhan Hukum dan Reputasi Sekolah**

Sekolah harus mematuhi regulasi privasi data yang berlaku, seperti undang-undang perlindungan data pribadi. Kegagalan untuk mematuhi regulasi ini bisa mengakibatkan konsekuensi hukum yang serius, termasuk denda dan sanksi, serta merusak reputasi sekolah di mata masyarakat. Oleh karena itu, penting bagi sekolah untuk bekerja sama dengan ahli hukum dan keamanan data untuk memastikan bahwa semua praktik yang dilakukan sesuai dengan regulasi yang berlaku.

Penggunaan sistem pengenalan wajah di sekolah menengah menimbulkan berbagai dampak etis dan praktis yang signifikan, terutama terkait dengan privasi siswa, kepercayaan orang tua, keamanan data pribadi, dan kepatuhan hukum. Untuk mengatasi tantangan ini, sekolah harus menerapkan kebijakan

privasi yang ketat, memastikan persetujuan yang terinformasi, serta mengambil langkah-langkah keamanan yang kuat untuk melindungi data biometrik siswa. Dengan demikian, sekolah dapat meminimalkan risiko dan memastikan bahwa teknologi pengenalan wajah digunakan secara etis dan bertanggung jawab.

### **4.3 Tinjauan Literatur Sistematis (Systematic Literature Review)**

Penggunaan teknologi biometrik, seperti sistem pengenalan wajah, di lingkungan pendidikan telah menimbulkan berbagai isu etis yang memerlukan perhatian serius. Teknologi ini diterapkan untuk berbagai tujuan, termasuk keamanan, manajemen kehadiran, dan pengawasan, namun penerapannya menimbulkan sejumlah masalah etika.

#### **A. Etika Penggunaan Teknologi Biometrik di lingkungan Pendidikan**

##### **1. Privasi dan Keamanan Data**

Data biometrik, seperti gambar wajah dan sidik jari, merupakan informasi yang sangat sensitif. Kekhawatiran utama yang sering muncul adalah terkait privasi dan keamanan data. Sifat sensitif dari data biometrik membuatnya rentan terhadap penyalahgunaan dan pelanggaran keamanan. Kebocoran data biometrik dapat mengakibatkan risiko besar jika data tersebut jatuh ke tangan yang salah [6]. Selain itu, penyimpanan data biometrik harus dilakukan dengan protokol keamanan yang ketat untuk mencegah akses tidak sah dan penyalahgunaan.

##### **2. Persetujuan dan Kesadaran**

Persetujuan yang jelas dan terinformasi dari siswa dan orang tua sangat penting sebelum data biometrik dikumpulkan dan digunakan. Siswa dan orang tua harus diberi informasi yang memadai tentang bagaimana data mereka akan digunakan, disimpan, dan dilindungi [7]. Tanpa persetujuan yang benar-benar sukarela dan berdasarkan informasi yang lengkap, penggunaan teknologi ini dapat dianggap melanggar hak privasi individu [8].

##### **3. Dampak Psikologis dan Sosial**

Penggunaan teknologi pengenalan wajah dapat menyebabkan perasaan tidak nyaman dan stres di kalangan siswa. Penelitian menunjukkan bahwa pengawasan yang ketat dapat menimbulkan dampak negatif pada kesehatan mental siswa dan menciptakan lingkungan belajar yang kurang kondusif [9]. Selain itu, ada kekhawatiran bahwa penerapan teknologi ini dapat mempengaruhi dinamika sosial di sekolah, menciptakan rasa ketidakpercayaan antara siswa dan pihak sekolah [10].

#### **B. Kode Etik bagi Profesional TI**

Profesional teknologi informasi memiliki tanggung jawab besar untuk memastikan bahwa teknologi yang mereka kembangkan dan kelola digunakan secara etis. Beberapa kode etik yang relevan bagi profesional TI mencakup prinsip-prinsip berikut:

##### **1. Privasi dan Kerahasiaan**

Kode etik dari ACM (Association for Computing Machinery) menekankan pentingnya menjaga privasi dan kerahasiaan informasi pengguna. Profesional TI harus memastikan bahwa data yang mereka tangani dilindungi dengan baik dan tidak digunakan tanpa izin yang jelas [11].

##### **2. Transparansi dan Akuntabilitas**

Profesional TI harus beroperasi dengan transparansi, menjelaskan dengan jelas kepada pengguna bagaimana data mereka akan digunakan dan memberikan informasi yang diperlukan untuk membuat keputusan yang diinformasikan [12]. Mereka juga harus bertanggung jawab atas dampak dari teknologi yang mereka kembangkan dan implementasikan.

##### **3. Keadilan dan Non-Diskriminasi**

Kode etik juga menggarisbawahi pentingnya keadilan dan non-diskriminasi dalam penggunaan teknologi. Profesional TI harus memastikan bahwa teknologi yang mereka ciptakan tidak mendiskriminasi kelompok tertentu dan digunakan untuk kebaikan bersama .

#### 4. Keamanan dan Kesejahteraan Publik

Kode etik IEEE menekankan pentingnya memastikan keamanan dan kesejahteraan publik dalam setiap pengembangan teknologi. Profesional TI harus mengembangkan teknologi yang aman dan melindungi kepentingan publik [12].

Penggunaan teknologi biometrik di lingkungan pendidikan membawa manfaat signifikan dalam hal efisiensi dan keamanan. Namun, penting untuk mempertimbangkan aspek etis seperti privasi, persetujuan, dampak psikologis, dan dinamika sosial. Kode etik bagi profesional TI menyediakan panduan penting untuk memastikan bahwa teknologi ini digunakan secara etis dan bertanggung jawab. Dengan mengikuti prinsip-prinsip etika ini, sekolah dan profesional TI dapat mengurangi risiko dan memastikan bahwa penggunaan teknologi biometrik memberikan manfaat yang maksimal tanpa mengorbankan hak dan kesejahteraan siswa.

#### **4.4 Rekomendasi Solusi Terbaik**

Sistem pengenalan wajah di sekolah harus diterapkan dengan pertimbangan etika yang mendalam untuk memastikan bahwa data biometrik digunakan secara aman dan bertanggung jawab. Berikut adalah rekomendasi solusi terbaik yang mencakup prinsip-prinsip etika utama.

##### 1. Penggunaan Terbatas dan Spesifik

Sistem pengenalan wajah hanya boleh digunakan untuk tujuan spesifik seperti manajemen kehadiran siswa. Penggunaan data biometrik untuk tujuan lain harus dilarang kecuali ada persetujuan eksplisit dan tertulis dari siswa dan orang tua. Kebijakan ini harus dinyatakan secara jelas dalam kebijakan privasi sekolah.

##### 2. Pembatasan Lama Penyimpanan Data

Data biometrik harus disimpan hanya selama diperlukan untuk tujuan absensi. Setelah periode tersebut berakhir, data harus segera dihapus. Penyimpanan data yang berlebihan meningkatkan risiko penyalahgunaan dan kebocoran data.

##### 3. Keamanan Data yang Tinggi

Data biometrik harus dilindungi dengan standar keamanan tinggi, termasuk enkripsi dan akses terbatas. Hanya karyawan yang berwenang dan terlatih yang dapat mengakses data tersebut. Sekolah harus secara rutin mengaudit sistem keamanan untuk memastikan perlindungan data dari ancaman kebocoran atau akses tidak sah.

##### 4. Sosialisasi dan Edukasi

Sebelum mengimplementasikan sistem pengenalan wajah, sekolah harus mengadakan sesi sosialisasi dan edukasi dengan siswa dan orang tua. Mereka harus diberi penjelasan yang transparan tentang tujuan, manfaat, risiko, dan langkah-langkah keamanan teknologi ini. Edukasi ini penting agar semua pihak memahami cara kerja teknologi dan dampaknya terhadap privasi.

##### 5. Persetujuan Terinformasi

Sekolah harus mendapatkan persetujuan yang jelas dan terinformasi dari siswa dan orang tua sebelum mengumpulkan data biometrik. Persetujuan ini harus bersifat sukarela dan diberikan berdasarkan pemahaman yang lengkap tentang penggunaan dan perlindungan data. Formulir persetujuan harus mudah dipahami.

##### 6. Konsultasi Berkelanjutan

Sekolah harus mengadakan konsultasi berkelanjutan dengan siswa dan orang tua untuk mengevaluasi dampak penggunaan teknologi ini. Masukan dari mereka harus digunakan untuk menyesuaikan kebijakan guna mengatasi kekhawatiran yang mungkin muncul.

#### 7. Kebijakan Privasi yang Transparan:

Sekolah harus memiliki kebijakan privasi yang jelas dan transparan terkait penggunaan data biometrik. Kebijakan ini harus mencakup jenis data yang dikumpulkan, tujuan pengumpulan, cara data disimpan dan dilindungi, serta akses data. Kebijakan ini harus mudah diakses oleh semua pihak terkait.

#### 8. Laporan Berkala

Sekolah harus menerbitkan laporan berkala tentang penggunaan sistem pengenalan wajah, termasuk bagaimana data digunakan dan dilindungi serta insiden keamanan yang mungkin terjadi. Ini akan membantu membangun kepercayaan dengan menunjukkan komitmen terhadap transparansi dan keamanan.

#### 9. Mekanisme Pengaduan

Sekolah harus menyediakan mekanisme pengaduan yang mudah diakses bagi siswa dan orang tua yang memiliki kekhawatiran atau masalah terkait penggunaan sistem pengenalan wajah. Pengaduan harus ditangani dengan serius dan direspon dengan tindakan yang tepat dan cepat.

#### 10. Teknologi Anonimisasi

Sekolah dapat mempertimbangkan penggunaan teknologi anonimisasi untuk mengurangi risiko privasi. Data biometrik dapat diproses sehingga identitas individu tidak langsung terlihat dan hanya digunakan untuk verifikasi kehadiran tanpa menyimpan informasi pribadi.

#### 11. Kepatuhan terhadap Undang-Undang Perlindungan Data

Sekolah harus memastikan bahwa semua praktik pengumpulan dan penyimpanan data sesuai dengan undang-undang perlindungan data yang berlaku, seperti UU Perlindungan Data Pribadi di Indonesia. Kepatuhan ini meliputi persetujuan yang sah, perlindungan data dengan standar keamanan tinggi, dan hak akses serta penghapusan data bagi siswa dan orang tua.

#### 12. Audit dan Pemantauan Rutin

Sekolah harus mengadakan audit dan pemantauan rutin untuk memastikan bahwa semua kebijakan dan praktik terkait penggunaan data biometrik dipatuhi dengan ketat. Audit ini sebaiknya dilakukan oleh pihak ketiga yang independen untuk memastikan objektivitas dan transparansi.

Dengan mengimplementasikan rekomendasi di atas, sekolah dapat memastikan bahwa penggunaan sistem pengenalan wajah dilakukan secara etis, transparan, dan bertanggung jawab, serta melindungi privasi dan keamanan data siswa.

## **5 Kesimpulan dan Saran**

### **5.1 Kesimpulan**

Penggunaan teknologi pengenalan wajah di sekolah memiliki dampak yang signifikan terhadap berbagai aspek kehidupan siswa dan manajemen sekolah. Analisis etika dan dampak dari teknologi ini menunjukkan beberapa poin penting yang harus dipertimbangkan dengan cermat.

1. Pelanggaran Privasi Pengumpulan dan penyimpanan data biometrik tanpa persetujuan yang jelas dan informasi yang memadai dapat dianggap sebagai pelanggaran privasi siswa.
2. Potensi Penyalahgunaan Data Data biometrik yang dikumpulkan berpotensi disalahgunakan untuk tujuan lain selain pencatatan kehadiran, seperti pemantauan perilaku siswa atau dibagikan kepada pihak ketiga tanpa izin.
3. Dampak Psikologis Implementasi teknologi pengenalan wajah di sekolah dapat menimbulkan perasaan tidak aman dan terawasi di kalangan siswa, yang dapat menyebabkan stres, kecemasan, dan gangguan dalam proses belajar-mengajar.

4. Kepatuhan terhadap Hukum Sekolah harus memastikan bahwa semua praktik pengumpulan dan penyimpanan data sesuai dengan undang-undang perlindungan data yang berlaku, termasuk persetujuan yang sah dan perlindungan data dengan standar keamanan tinggi.

## 5.2 Saran

Untuk peneliti yang ingin mengambil topik yang sejenis, beberapa saran penting yang dapat membantu dalam pelaksanaan penelitian adalah sebagai berikut.

1. Melakukan Kajian Literatur yang Mendalam: Peneliti harus melakukan kajian literatur yang mendalam tentang teknologi pengenalan wajah, implikasi etis, dan regulasi terkait untuk memahami konteks penelitian yang lebih luas dan mengidentifikasi celah penelitian.
2. Memperhatikan Aspek Hukum dan Etika: Peneliti harus memastikan bahwa penelitian mereka mematuhi semua hukum dan regulasi terkait perlindungan data dan privasi. Mendapatkan persetujuan dari komite etika penelitian juga penting untuk melindungi hak dan kesejahteraan subjek penelitian.
3. Menjalani Kolaborasi dengan Ahli: Bekerja sama dengan ahli di bidang teknologi pengenalan wajah, etika, dan hukum dapat memberikan wawasan yang lebih mendalam dan memperkuat validitas penelitian.

## Referensi

- [1] S. M. Bah and F. Ming, "An improved face recognition algorithm and its application in attendance management system," *Array*, vol. 5, pp. 1–2, 2020, doi: <https://doi.org/10.1016/j.array.2019.100014>.
- [2] Sunardi, A. Fadlil, and D. Prayogi, "Sistem Pengenalan Wajah pada Keamanan Ruang Berbasis Convolutional Neural Network," *J. Sains Komput. Inform. J-SAKTI*, vol. 6, pp. 636–647, 2022, doi: <http://dx.doi.org/10.30645/j-sakti.v6i2.480>.
- [3] A. N. Samardzic, "Biometric Technology and Ethics: Beyond Security Applications," *J. Bus. Ethics*, vol. 167, no. 3, pp. 433–450, 2020, doi: <https://doi.org/10.1007/s10551-019-04143-6>.
- [4] D. Almeida, K. Shmarko, and E. Lomas, "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 Ethics*, vol. 2, no. 3, pp. 377–387, 2022, doi: <https://doi.org/10.1007/s43681-021-00077-w>.
- [5] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, 2019, doi: <https://doi.org/10.1016/j.jbusres.2019.07.039>.
- [6] A. Cavoukian and F. Carter, "Privacy by Design The 7 Foundational Principles," *Glob. Priv. Secur. Des.*, 2023, [Online]. Available: <https://gpsbydesign.org/the-7-foundational-principles-implementation-and-mapping-of-fair-information-practices/>
- [7] Mordini, E and Tzovaras, D, *Second Generation Biometrics: The Ethical, Legal and Social Context*, 1st ed. Springer Dordrecht, 2012. [Online]. Available: <https://doi.org/10.1007/978-94-007-3892-8>
- [8] Introna, L. D. and Nissenbaum, H., "Facial Recognition Technology: A Survey of Policy and Implementation Issues," *Cent. Catastr. Prep. Response N. Y. Univ.*, 2009, [Online]. Available: <https://ssrn.com/abstract=1437730>
- [9] A. J. Lu, G. Marcu, M. S. Ackerman, and T. R. Dillahunt, "Coding Bias in the Use of Behavior Management Technologies: Uncovering Socio-technical Consequences of Data-driven Surveillance in Classrooms," *ACM*, pp. 508–522, 2021, doi: <https://doi.org/10.1145/3461778.3462084>.
- [10] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015, doi: 10.1126/science.aaa1465.
- [11] Association for Computing Machinery, "ACM Code of Ethics and Professional Conduct," Association for Computing Machinery, 2018. [Online]. Available: <https://www.acm.org/code-of-ethics>
- [12] G. Adamson and J. Herkert, "Addressing Intelligent Systems and Ethical Design in the IEEE Code of Ethics," in *Codes of Ethics and Ethical Guidelines: Emerging Technologies, Changing Fields*, K. Laas, M. Davis, and E. Hildt, Eds., Cham: Springer International Publishing, 2022, pp. 145–159. doi: 10.1007/978-3-030-86201-5\_8.