JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 5, No. 1, Januari 2026, pp. 26 - 35
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/169

Illegal Deepfake-Based Artificial Intelligence Content and Efforts to Combat It in Indonesia

Putri Aulia Lestari[*1], Zulfa Rizqi Saputri[2], Resti Jamilah[3], Febiyanti[4], Muhamad Fadli Fadilah[5], M Fadlan Firnanda[6], Tya Septiani Nurfauzia Koeswara[7]
[1,2,3,4,5,6,7] Program Studi Sistem Informasi Kampus Kota Sukabumi, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika
Jl. Raya Cemerlang No. 8, 43135, Sukakarya, Kec. Warudoyong, Sukabumi, Jawa Barat, Indonesia
e-mail: 19232272@bsi.ac.id*[1], 19231697@bsi.ac.id[2], 19232430@bsi.ac.id[3], 19230549@bsi.ac.id[4], 19232284@bsi.ac.id[5], 19232180@bsi.ac.id[6], tya.tsf@bsi.ac.id[7]

ARTICLE INFO

Article History:

Received: 30-10-2025
Revised: 20-11-2025
Accepted: 11-12-2025
Published: 21-01-2026

ABSTRACT

Technological advancements have made remarkable progress, particularly in Artificial Intelligence (AI), which has revolutionized sectors such as education, entertainment, business, and communication. However, alongside these benefits, AI has also introduced significant risks, particularly the misuse of deepfake technology to produce illegal or unethical digital content. This study aims to examine the misuse of AI, focusing on the motives, causes, preventive measures, and real cases in Indonesia. Employing a literature review method with descriptive qualitative analysis, this research utilizes secondary data sources from scientific journals, legal frameworks such as the ITE Law, Pornography Law, and Personal Data Protection (PDP) Law, as well as case reports from social media and online news. The findings reveal that the main motives behind deepfake misuse include financial profit, personal revenge, political propaganda, and sexual exploitation. The study also highlights several underlying causes, including rapid AI development, insufficient legal enforcement, and low public awareness of AI ethics and digital security. To mitigate these issues, it is crucial to promote ethical education on AI, strengthen legal policies, and enhance AI-based deepfake detection systems. This study emphasizes the importance of collaboration between the government, technology developers, and society to ensure responsible AI use and protect individuals from the growing threats of digital manipulation in this technological era.

Keywords: *Deepfake, Artificial Intelligence (AI), Illegal Content, Study Literature.*

Abstrak

Perkembangan teknologi telah mengalami kemajuan yang luar biasa, terutama dalam bidang Kecerdasan Buatan (*Artificial Intelligence*/AI) yang telah merevolusi berbagai sektor seperti pendidikan, hiburan, bisnis, dan komunikasi. Namun, di balik berbagai manfaat tersebut, muncul pula risiko serius, salah satunya adalah penyalahgunaan teknologi *deepfake* dalam pembuatan konten digital yang ilegal maupun tidak etis. Penelitian

DOI: https://doi.org/10.51903/r5xwq018

p-ISSN : 2803-1507 e-ISSN : 2803-1531

ini bertujuan untuk mengkaji penyalahgunaan AI dengan fokus pada motif, penyebab, langkah pencegahan, serta kasus-kasus yang terjadi di Indonesia. Metode yang digunakan adalah kajian pustaka dengan analisis kualitatif deskriptif, menggunakan data sekunder dari jurnal ilmiah, kerangka hukum seperti Undang-Undang ITE, Undang-Undang Pornografi, dan Undang-Undang Perlindungan Data Pribadi (PDP), serta laporan kasus yang beredar di media sosial dan berita daring. Hasil penelitian menunjukkan bahwa motif utama pelaku dalam penyalahgunaan *deepfake* meliputi keuntungan finansial, balas dendam pribadi, propaganda politik, dan eksploitasi seksual. Selain itu, penyebab utama yang teridentifikasi adalah pesatnya perkembangan AI, lemahnya penegakan hukum, serta rendahnya kesadaran masyarakat terhadap etika dan keamanan digital. Untuk mengatasi permasalahan ini, diperlukan pendidikan mengenai etika penggunaan teknologi AI, penguatan kebijakan hukum, serta pengembangan sistem deteksi *deepfake* berbasis AI. Penelitian ini menekankan pentingnya kolaborasi antara pemerintah, pengembang teknologi, dan masyarakat guna memastikan penggunaan AI yang bertanggung jawab serta melindungi individu dari ancaman manipulasi digital di era teknologi ini.

Kata Kunci: *Deepfake, Kecerdasan Buatan (Artificial Intelligence/AI), Konten Ilegal, Studi Kepustakaan.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini berlangsung dengan sangat pesat, membawa perubahan besar dalam hampir seluruh aspek kehidupan manusia [1]. Transformasi digital tidak hanya mengubah cara manusia berkomunikasi, bekerja, dan memperoleh informasi, tetapi juga mendorong munculnya teknologi baru yang secara langsung memengaruhi keamanan digital masyarakat [2], [3], [4]. Di satu sisi, perkembangan ini memberikan banyak manfaat, namun di sisi lain juga menghadirkan tantangan yang semakin kompleks dan tidak dapat diabaikan [5]. Perubahan tersebut turut mempengaruhi cara masyarakat beradaptasi dengan sistem digital yang semakin terintegrasi dalam aktivitas sehari-hari.

Salah satu hasil nyata dari perkembangan tersebut adalah hadirnya kecerdasan buatan atau Artificial Intelligence (AI), yang kini tidak hanya digunakan untuk kebutuhan produktivitas tetapi juga memiliki potensi disalahgunakan dalam berbagai konteks digital [6]. Pemanfaatan AI telah merambah ke berbagai bidang, mulai dari kesehatan, transportasi, pendidikan, hingga hiburan, dan kemampuan AI mengolah data secara cepat serta akurat menunjukkan besarnya pengaruh teknologi ini terhadap kehidupan modern [7]. Kemampuan AI dalam mengolah data membuat teknologi ini digunakan secara luas untuk meningkatkan efisiensi berbagai layanan digital. Perkembangan ini menunjukkan besarnya ketergantungan masyarakat pada teknologi yang mampu beroperasi secara otomatis.

Namun, di balik manfaatnya, AI juga dapat menjadi ancaman ketika digunakan secara tidak etis. Pesatnya perkembangan teknologi digital turut memicu munculnya *cybercrime* [8]. yaitu kejahatan siber yang memanfaatkan teknologi untuk merugikan orang lain, termasuk dalam bentuk penyebaran konten manipulatif yang semakin sulit dikenali [9]. Salah satu wujud nyata penyalahgunaan AI dalam *cybercrime* yang kini menjadi perhatian besar adalah pembuatan konten ilegal berupa manipulasi gambar atau video seseorang tanpa izin, yang dikenal dengan istilah *deepfake* [10]. *Deepfake*, sebagai teknologi berbasis machine learning, memungkinkan penggantian wajah atau suara dengan sangat realistis, sehingga menimbulkan kesulitan dalam membedakan antara konten asli dan manipulasi, dan hal ini tentunya memberi ruang besar bagi pelaku kejahatan untuk melakukan tindakan kriminal seperti pornografi, pencemaran nama baik, penyebaran berita palsu, hingga pemerasan online [11].

Kasus manipulasi digital paling sering ditemukan pada pembuatan konten pornografi tanpa persetujuan, yang dapat menimbulkan trauma psikologis, kerusakan reputasi, dan stigma sosial bagi korban [12]. Selain itu, konten manipulatif juga digunakan dalam penyebaran informasi palsu, propaganda politik, hingga ancaman digital dengan memanfaatkan video hasil rekayasa untuk meminta sejumlah uang [13]. Hal ini menunjukkan bahwa teknologi ini bukan sekadar inovasi, tetapi ancaman nyata yang berdampak luas bagi individu maupun masyarakat dan memerlukan perhatian lebih serius dari sisi penelitian serta kebijakan [14]. Penyebaran konten semacam ini turut memperlihatkan bagaimana teknologi digital dapat dimanfaatkan untuk memanipulasi persepsi publik melalui materi visual yang tampak meyakinkan.

Salah satu contoh jelas di Indonesia adalah insiden iklan investasi ilegal pada 2023–2024, di mana wajah tokoh publik seperti Nagita Slavina, Raffi Ahmad, dan Ustaz Solmed dipalsukan untuk mempromosikan aplikasi fiktif seperti “Hydro Trade,” memperlihatkan betapa mudahnya masyarakat tertipu oleh konten digital yang tampak meyakinkan [15]. Kasus tersebut menunjukkan bahwa teknologi manipulasi digital dapat

p-ISSN : 2803-1507 e-ISSN : 2803-1531

dimanfaatkan dengan sangat mudah oleh pihak yang tidak bertanggung jawab. Konten palsu yang menyerupai tokoh publik membuat masyarakat sulit membedakan antara informasi yang valid dan konten rekayasa. Fenomena ini juga mengindikasikan adanya peningkatan risiko penipuan yang memanfaatkan citra digital untuk menarik perhatian calon korban. Rincian berbagai kasus yang pernah terjadi di Indonesia dapat dilihat pada Tabel 1.

Tabel 1. Kasus Deepfake di Indonesia

No	Kasus	Contoh Deepfake	Tahun	Provinsi	Sumber
1	Video deepfake Luhut Pandjaitan berpidato palsu tentang vaksin COVID-19 dan investasi asing.	Video	2021	DKI Jakarta	Kompas.com
2	Deepfake video porno non-konsensual menargetkan presenter TV nasional di Telegram.	Video	2021	DKI Jakarta	Detik.com
3	Gambar deepfake manipulasi wajah tokoh adat Papua untuk hoaks konflik tanah.	Gambar	2023	Papua	Kominfo
4	Deepfake video pidato palsu Presiden Jokowi untuk kampanye politik.	Video	2021	DKI Jakarta	Detik.com
5	Gambar deepfake wajah korban bencana untuk penggalangan dana palsu di Samarinda.	Gambar	2023	Kalimantan Timur	Borneo Tribune
6	Gambar deepfake foto selebriti untuk promosi produk ilegal di Kupang.	Gambar	2024	Nusa Tenggara Timur	RRI.co.id
7	Video deepfake ceramah agama palsu untuk provokasi di Banda Aceh.	Video	2024	Aceh	Serambinews.com
8	Audio deepfake dokter untuk penipuan obat palsu di Malang.	Audio	2022	Jawa Timur	Jatim Times
9	Gambar deepfake foto artis untuk konten dewasa ilegal di media sosial.	Gambar	2023	DKI Jakarta	Jakarta Globe
10	Kasus manipulatif video deepfake (“Tiga Gubernur”).	Video	2025	Jawa Timur	Mili.id
11	Kasus “AMA” modus penipuan dengan video deepfake atas nama pejabat negara.	Video	2025	Bandar Lampung	Kompas.com
12	Deepfake pornografi artis Raline Shah.	Video	2021	DKI Jakarta	Detik.com

Berdasarkan Tabel 1. Kasus *Deepfake* di Indonesia, dapat disimpulkan kasus deepfake terbanyak berada di provinsi DKI Jakarta dengan bentuk video yang dimanipulasi dengan berbagai motif, salah satunya propaganda politik. Keberadaan *deepfake* juga memperbesar persoalan pelanggaran privasi di era digital. Identitas dan wajah seseorang yang diunggah ke internet dapat dengan mudah diambil lalu dimanipulasi untuk tujuan yang tidak sah. Hal ini memperlihatkan adanya kesenjangan antara pesatnya perkembangan teknologi dengan kesiapan masyarakat maupun instrumen hukum dalam menghadapinya [16]. Di Indonesia, meskipun telah tersedia beberapa instrumen hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi, dan Undang-Undang Perlindungan Data Pribadi, penerapannya masih menghadapi sejumlah kendala, khususnya dalam menjerat pelaku *deepfake* yang kerap sulit dilacak [17]. Oleh karena itu, isu penyalahgunaan AI melalui *deepfake* dalam produksi konten ilegal perlu dikaji secara lebih mendalam, baik dari aspek sosial maupun hukum, agar dapat memberikan perlindungan yang lebih efektif bagi masyarakat.

2. TINJAUAN PUSTAKA

Penelitian mengenai perkembangan teknologi pada era industri 4.0 dan *society 5.0* menunjukkan bahwa *artificial intelligence (AI)* menjadi salah satu inovasi utama yang mendorong percepatan otomatisasi dan pengambilan keputusan cerdas. Menurut [18], perkembangan ini memperlihatkan bagaimana *AI* terus memperluas perannya dalam kehidupan modern. Studi terdahulu juga menyoroti bahwa *AI* digunakan pada berbagai aplikasi seperti peramalan cuaca, sistem penerjemahan, hingga sistem rekomendasi di berbagai sektor; peneliti [19] menambahkan bahwa pemanfaatan tersebut semakin meluas dari tahun ke tahun. Selain itu, menurut penelitian [20], *AI* semakin banyak dimanfaatkan dalam pembuatan konten digital, termasuk gambar, audio, dan video, karena kemampuannya menghasilkan *output* secara cepat dan efisien. Temuan-temuan ini menegaskan peran signifikan *AI* dalam mendukung transformasi digital di berbagai bidang.

Sejumlah penelitian membahas teknologi *deepfake* sebagai salah satu produk perkembangan *AI* yang memanfaatkan model *deep learning* untuk mempelajari ekspresi wajah, gerakan, maupun suara manusia. Menurut [21], teknologi ini mampu memanipulasi gambar, audio, dan video secara sangat realistis sehingga memunculkan berbagai risiko, termasuk penyalahgunaan untuk pencemaran nama baik dan pelanggaran privasi. Penelitian lain menemukan bahwa *deepfake* dapat digunakan untuk melakukan tindakan kriminal

p-ISSN : 2803-1507 e-ISSN : 2803-1531

seperti penipuan dan pembuatan konten palsu yang menyerupai seseorang; studi [22] menyebutkan bahwa hal ini menjadi ancaman serius dalam ruang digital modern. Berbagai penelitian tersebut menekankan perlunya kewaspadaan karena teknologi *deepfake* dapat menghasilkan konten digital yang tampak nyata tetapi tidak pernah terjadi.

Penelitian terdahulu juga mengungkapkan bahwa teknologi *deepfake* banyak digunakan dalam pembuatan konten ilegal yang dapat merusak norma sosial dan menimbulkan ancaman keamanan digital. Menurut [23], konten semacam ini berpotensi disalahgunakan dengan dampak sosial yang luas. Studi sebelumnya menunjukkan bahwa manipulasi gambar, suara, dan video dengan tingkat akurasi tinggi dapat menipu publik dan memunculkan risiko sosial yang signifikan; peneliti [24] menegaskan bahwa efeknya dapat mengganggu kepercayaan masyarakat terhadap informasi digital. Selain itu, beberapa penelitian mengidentifikasi penggunaan *deepfake* dalam eksploitasi seksual, di mana wajah korban disisipkan ke dalam konten gambar atau video sehingga menimbulkan kerugian besar bagi korban, baik secara psikologis maupun sosial; studi [25] menunjukkan bahwa praktik ini menjadi isu yang sangat berbahaya dalam perkembangan teknologi digital modern.

Penelitian terkait regulasi menunjukkan bahwa Indonesia memiliki beberapa dasar hukum dalam menangani kejahatan siber, seperti UU Pornografi dan UU ITE, yang dapat digunakan untuk memproses pelanggaran yang melibatkan *deepfake* meskipun belum ada aturan khusus yang mengatur teknologi ini secara spesifik. Menurut [26], kerangka hukum tersebut masih bersifat umum. Studi lain menekankan bahwa Undang-Undang Perlindungan Data Pribadi berperan penting dalam memberikan landasan hukum terhadap penyebaran konten ilegal yang berkaitan dengan pencurian atau penyalahgunaan identitas digital; peneliti [27] menambahkan bahwa penguatan regulasi menjadi kebutuhan mendesak. Penelitian-penelitian tersebut menegaskan bahwa kerangka hukum yang ada masih membutuhkan penguatan agar mampu merespons perkembangan teknologi *deepfake* secara komprehensif.

Sejumlah penelitian membahas pentingnya tata kelola *AI* sebagai upaya untuk memastikan pemanfaatan teknologi kecerdasan buatan berjalan selaras dengan tujuan organisasi dan prinsip etika yang berlaku. Menurut [28], tata kelola *AI* diperlukan untuk mengidentifikasi berbagai potensi risiko dan dampak negatif dari penggunaan *AI*. Studi-studi tersebut menunjukkan bahwa risiko-risiko tersebut dapat diminimalkan melalui kebijakan dan mekanisme pengawasan yang tepat; peneliti [29] menambahkan bahwa tata kelola yang kuat juga penting dalam membangun kepercayaan publik. Selain itu, menurut penelitian [30], tata kelola *AI* yang baik mampu memastikan bahwa penerapannya dilakukan secara bertanggung jawab dan berkelanjutan. Hal ini menegaskan bahwa *AI governance* menjadi komponen penting dalam pemanfaatan *AI* modern.

3. METODOLOGI PENELITIAN

3.1. *Jenis Penelitian*

Penelitian ini menggunakan pendekatan studi kepustakaan (*library research*) dengan mengumpulkan informasi-informasi mengenai konten illegal. Pendekatan ini bermaksud untuk meninjau atau menelaah mengenai dampak dari penyalahgunaan teknologi *Artificial Intelligence* (AI) yaitu *deepfake*. Untuk memahami isu mengenai konten illegal berbasis *deepfake,* analisis yang dilakukan yaitu menggunakan metode kualitatif deskriptif dengan menggunakan data sekunder yang bersumber dari jurnal, buku atau riset-riset terdahulu [31]. Pendekatan ini digunakan untuk memperoleh gambaran yang komprehensif mengenai perkembangan teknologi serta implikasinya terhadap penyebaran konten manipulatif di lingkungan digital.

Informasi penelitian bersumber dari data sekunder yang diambil dari jurnal ilmiah nasional, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi dan Undang-Undang Perlindungan Data Pribadi. Agar hasil penelitian relevan, maka literatur yang diambil atau dipilih dibatasi pada rentang waktu tahun 2020 sampai 2025. Dalam penelusuran jurnal ilmiah menggunakan kata kunci "*deepfake* Indonesia", "konten ilegal", "*cybercrime* AI", "penyalahgunaan *deepfake*", dan "dampak AI". Batasan tersebut diterapkan untuk memastikan bahwa data yang dikaji mencerminkan perkembangan terkini mengenai pemanfaatan teknologi digital dalam konteks pelanggaran siber.

3.2. *Lokasi dan Waktu Penelitian*

Penelitian ini dilaksanakan secara daring (*online*) melalui kegiatan pengumpulan data sekunder yang diperoleh dari berbagai sumber terpercaya, seperti jurnal ilmiah, buku, situs web resmi, serta laporan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

penelitian akademik yang relevan dengan topik kajian. Proses penelitian berlangsung selama satu tahun, yaitu mulai dari Januari hingga Desember 2025, yang mencakup tahap pengumpulan data, analisis literatur, serta penyusunan hasil penelitian. Pemilihan metode daring dilakukan karena memungkinkan peneliti mengakses literatur yang lebih luas tanpa batasan geografis. Rentang waktu tersebut dipilih untuk memberikan ruang yang cukup dalam menelaah perkembangan kasus dan literatur yang berkaitan dengan isu penyalahgunaan teknologi *deepfake*.

3.3. *Sumber dan Teknik Pengumpulan Data*

Sumber data dalam penelitian ini berupa data sekunder yang dikumpulkan dari berbagai literatur, seperti jurnal ilmiah, artikel penelitian, buku referensi, peraturan perundang-undangan, serta dokumen hukum yang membahas pelanggaran digital dan pemalsuan data. Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dengan cara menelusuri serta menganalisis berbagai sumber tertulis yang relevan. Sumber-sumber tersebut dipilih berdasarkan kredibilitas dan relevansinya dengan fokus penelitian. Pendekatan ini memberikan kesempatan bagi peneliti untuk menelaah secara mendalam berbagai informasi yang berkaitan dengan penyebaran konten ilegal berbasis *deepfake*.

3.4. *Teknik Analisis Data*

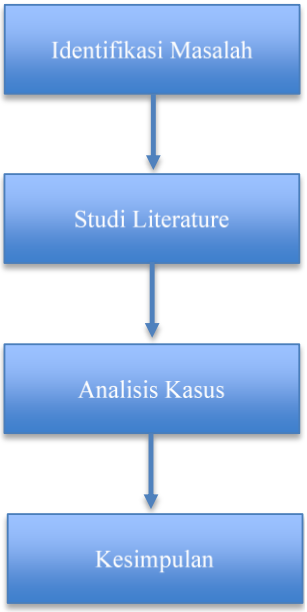
Teknik analisis data yang digunakan dalam penelitian ini adalah metode analisis isi (*content analysis*) dengan pendekatan kualitatif deskriptif. Teknik ini dipilih untuk menelaah berbagai dokumen, literatur, dan laporan kasus terkait penyalahgunaan teknologi *Artificial Intelligence* (AI), khususnya *deepfake*, dalam konteks kejahatan siber di Indonesia. Metode ini memungkinkan peneliti mengidentifikasi pola representasi dan kecenderungan pemanfaatan teknologi manipulasi digital. Pendekatan analisis isi juga digunakan untuk mengevaluasi sejauh mana perkembangan teknologi memengaruhi karakteristik kejahatan digital yang muncul.

Analisis dilakukan dengan menelusuri isi sumber data sekunder seperti jurnal ilmiah, peraturan perundang-undangan, laporan berita, serta hasil riset terdahulu. Setiap dokumen dikaji untuk menemukan pola, bentuk pelanggaran, jenis konten ilegal, serta dampaknya terhadap individu dan masyarakat. Peneliti juga mengidentifikasi keterkaitan antara kemajuan teknologi AI dengan meningkatnya tindak kejahatan digital, terutama pada ranah pelanggaran privasi dan penyebaran konten manipulatif berbasis *deepfake*. Proses analisis dilakukan secara sistematis untuk memastikan bahwa temuan penelitian mencerminkan kondisi aktual penyalahgunaan teknologi digital.

3.5. *Tahapan Penelitian*

Tahapan penelitian disusun secara sistematis untuk menggambarkan alur proses yang digunakan dalam mencapai tujuan penelitian. Setiap tahap dirancang agar peneliti dapat mengikuti proses analisis secara terstruktur berdasarkan data sekunder yang dikumpulkan. Penyusunan tahapan ini juga bertujuan untuk memastikan bahwa seluruh langkah penelitian memiliki keterkaitan logis antara satu tahap dengan tahap lainnya. Penjelasan mengenai tahapan tersebut memberikan gambaran yang jelas mengenai proses kerja penelitian yang dilakukan. Alur lengkap tahapan penelitian dapat dilihat pada Gambar 1.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 1. Flowchart

Pada Gambar 1 Flowchart Tahapan Penelitian menunjukkan alur tahapan penelitian yang dimulai dari identifikasi masalah sebagai langkah awal untuk mengidentifikasi isu utama yang berkaitan dengan penyebaran konten illegal berbasis teknologi deepfake di Indonesia. Selanjutnya dilakukan Studi Literatur untuk mengumpulkan berbagai referensi ilmiah, peraturan, serta memperkuat landasan teori dan memahami konteks penelitian. Tahap selanjutnya peneliti melakukan Analisis Kasus dengan berbagai contoh penyalahgunaan deepfake di Indonesia seperti pelanggaran, dampak, serta keterkaitan antara kemajuan teknologi AI dan kejahatan siber. Tahap akhir menyusun kesimpulan yang memuat ringkasan temuan penelitian Utama mengenai motif, faktor penyebab, serta upaya penanganan konten ilegal berbasis deepfake berdasarkan hasil analisis.

3.5.1. *Identifikasi Masalah*

Tahap pertama yang dilakukan yaitu mengidentifikasi masalah yang menjadi fokus penelitian, yaitu penyebaran konten ilegal berbasis teknologi *deepfake* di Indonesia. Di tahap ini peneliti mencari dan mengamati fenomena yang terjadi tujuannya untuk menemukan masalah yang aktual dan signifikan yang berhubungan dengan dampak teknologi *deepfake* di Indonesia. Langkah ini diperlukan agar batasan penelitian dapat ditetapkan secara jelas sesuai konteks perkembangan kejahatan digital. Proses identifikasi juga membantu peneliti memahami karakteristik permasalahan yang muncul akibat penyalahgunaan teknologi manipulasi visual.

3.5.2. *Studi Literatur*

Pada tahap ini, peneliti mengumpulkan dan mengamati dari berbagai referensi ilmiah yang relevan untuk memperkuat teori penelitian. Sumber data yang digunakan adalah jurnal ilmiah, artikel akademik, juga peraturan perundang-undangan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Tujuannya untuk memahami konsep dasar *deepfake*, dampak sosial dan hukum yang ditimbulkan. Tahap ini juga membantu peneliti meninjau bagaimana perkembangan teknologi AI memengaruhi munculnya bentuk-bentuk kejahatan digital baru.

3.5.3. *Analisis Kasus*

Tahap ini peneliti memperdalam pengetahuan berdasarkan beberapa kasus nyata penyebaran konten *deepfake* yang terjadi di Indonesia. Data dianalisis secara deskriptif dengan menjelaskan bentuk, penyebab, dan dampak dari kasus yang terjadi. Analisis ini bertujuan untuk menemukan pola perilaku penyebaran, tantangan hukum, dan upaya pencegahan dan penegakan hukum yang telah dilakukan. Pendekatan ini memungkinkan peneliti memahami dinamika pemanfaatan teknologi manipulatif dalam berbagai konteks pelanggaran digital.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

3.5.4. *Kesimpulan*

Pada tahap akhir ini berisi ringkasan hasil dari penelitian yang mencakup pola penyebaran konten ilegal berbasis *deepfake*, dampak sosial yang ditimbulkan, serta langkah-langkah yang bisa dilakukan untuk menanggulanginya. Tahap ini disusun untuk memberikan gambaran umum mengenai hasil pemetaan permasalahan yang diperoleh dari analisis sebelumnya. Proses ini juga menjelaskan keterkaitan antara temuan penelitian dengan fenomena penyalahgunaan teknologi manipulatif di ruang digital. Penjelasan pada tahap ini membantu merangkum arah pemahaman yang diperoleh setelah seluruh rangkaian tahapan penelitian dilaksanakan.

3.6. *Hasil yang Diharapkan*

Penelitian ini diharapkan dapat memberikan pemahaman tentang penyebab dan dampak sosial dari dari penyebaran konten ilegal berbasis *deepfake* di Indonesia, juga analisis terhadap UU ITE dan UU PDP dalam menangani kasus *deepfake* dan memperkuat upaya pemerintah dan Lembaga dalam mencegah penyalahgunaan teknologi kecerdasan buatan. Hasil tersebut juga diharapkan mampu menjadi rujukan bagi penelitian selanjutnya yang membahas perkembangan kejahatan digital. Pemahaman yang diperoleh dapat memberikan gambaran mengenai kebutuhan penguatan regulasi pada ranah perlindungan data pribadi dan keamanan digital. Temuan penelitian ini juga diharapkan dapat meningkatkan kesadaran publik mengenai risiko penyalahgunaan teknologi manipulasi visual.

4. HASIL DAN PEMBAHASAN

Berdasarkan analisis data yang diperoleh dari beberapa jurnal ilmiah, peraturan perundang-undangan, kasus yang terjadi di Indonesia yang melibatkan beberapa aspek seperti teknologi, sosial dan hukum. *Deepfake*, sebagai bentuk penyalahgunaan teknologi yang sangat berbahaya bagi masyarakat yang dilakukan oleh individu maupun kelompok. Fenomena tersebut menunjukkan bahwa pemanfaatan teknologi manipulatif semakin meningkat di tengah kemudahan akses perangkat digital yang tersedia bagi masyarakat. Motifnya bisa didasari oleh berbagai aspek, yaitu:

1. Keuntungan Finansial, pelaku yang melakukan kejahatan ini bertujuan untuk mencari keuntungan dari korban dengan memanfaatkan teknologi *deepfake*. Contohnya, memalsukan wajah seseorang untuk video promosi, mengedit foto atau video korban untuk dijadikan bahan pemerasan oleh pelaku kepada korban.
2. Balas dendam pribadi, dilakukan karena pelaku mempunyai dendam dan emosi pribadi terhadap korban dan melakukan kejahatan seperti menyebarkan berita hoax dan fitnah mengenai korban.
3. Propaganda politik, biasanya ini terjadi ketika akan melakukan pemilu dengan menyebarkan ideologi yang menyimpang maupun menyebarkan berita dapat memperkeruh suasana dan menyebabkan kegaduhan dalam dunia politik.
4. Eksploitasi seksual dan hiburan, motif ini dilakukan oleh pelaku untuk kesenangan pribadi dengan memanipulasi foto atau video korban dengan menjerumus kearah seksual dan menyebarkannya di media sosial yang bisa menimbulkan fitnah dan membuat korban mendapatkan sanksi sosial, walaupun foto atau video yang tersebar adalah hasil dari manipulasi menggunakan teknologi *deepfake*.

Dari berbagai motif tersebut, banyak penyebab dari munculnya kejahatan tersebut terjadi seperti, kemajuan dari teknologi AI yang mudah dan gratis yang bisa diakses oleh semua masyarakat, ini meningkatkan resiko penyalahgunaannya. Adapun, kesenjangan antara teknologi dengan hukum di Indonesia yang masih belum sepenuhnya mengantisipasi bahayanya penyalahgunaan *deepfake* dan kurangnya edukasi dan kesadaran mengenai bahayanya teknologi AI dalam penggunaan sosial media. Kondisi ini memperlihatkan bahwa perkembangan teknologi tidak sejalan dengan kemampuan masyarakat dalam mengenali ancaman digital yang ada. Fenomena tersebut juga menunjukkan perlunya pemahaman yang lebih mendalam mengenai penggunaan teknologi manipulatif dan dampaknya terhadap ruang digital yang semakin kompleks.

Pemahaman mengenai risiko penyalahgunaan teknologi deepfake menjadi sangat penting untuk mengantisipasi dampak negatif terhadap masyarakat. Langkah-langkah penanggulangan perlu dirancang berdasarkan bukti nyata dari motif dan penyebab penyalahgunaan teknologi ini. Selain itu, strategi yang tepat juga harus mempertimbangkan aspek sosial, hukum, dan edukasi publik agar implementasinya efektif.Berdasarkan motif dan penyebab tersebut, terdapat beberapa cara untuk menanggulangi penyalahgunaan teknologi *deepfake*, diantaranya:

p-ISSN : 2803-1507 e-ISSN : 2803-1531

1. Menerapkan etika dalam penggunaan teknologi *deepfake* dengan menyadari dampak dalam penyalahgunaan AI.
2. Mengedukasi masyarakat melalui kegiatan sosialiasi mengenai bahaya teknologi AI dan *deepfake*.
3. Memperkuat aturan dan hukum yang berlaku mengenai *deepfake*.
4. Mengembangkan teknologi untuk mendeteksi yang bisa membedakan konten manipulasi.

Kasus penyebaran konten pornografi yang ditangani Polda Metro Jaya pada tahun 2024 di DKI Jakarta menunjukkan semakin maraknya penyalahgunaan teknologi dan kejahatan digital berbasis siber. Berdasarkan laporan pusiknas.polri.go.id, salah satu contoh kasus yang menonjol adalah peristiwa yang menimpa AD, anak dari seorang musisi ternama Indonesia. Tidak terima diputus cinta, pelaku berinisial AP menyebarkan rekaman kegiatan seksualnya bersama AD ke ruang digital. Setelah dilaporkan, AP ditangkap dan ditetapkan sebagai tersangka. Menurut keterangan Direskrimsus Polda Metro Jaya, tindakan tersebut merupakan bentuk balas dendam, dan berdasarkan informasi Pusiknas Polri, pelaku dapat terancam hukuman hingga 15 tahun penjara sesuai ketentuan UU ITE dan UU Pornografi. Kasus tersebut memperlihatkan bagaimana motif personal dapat memicu penggunaan teknologi manipulatif untuk merugikan korban secara sosial maupun psikologis.

Hasil analisis menunjukkan bahwa kasus deepfake terbanyak berada di provinsi DKI Jakarta dalam bentuk penyebarannya yaitu berbentuk video yang dimanipulasi dengan motif propaganda politik. Kasus ini menunjukkan perkembangan teknologi deepfake tidak hanya memberikan dampak positif bagi kemajuan digital, tetapi juga membuka peluang besar terhadap kejahatan penipuan, propaganda, pelanggaran privasi, dan kejahatan seksual. Selain itu, teknologi deepfake bisa diakses oleh seluruh pengguna internet yang artinya semua orang yang bisa mengakses internet dapat menggunakan teknologi deepfake, sehingga masyarakat menjadi lebih rentan dalam misinformasi dan disinformasi. Dalam konteks politik, dengan adanya penyebaran konten ilegal berbasis deepfake ini memungkinkan masyarakat terpropaganda dan memicu ketidakstabilan sosial. Fenomena ini semakin menegaskan bahwa kemampuan manipulasi visual yang kian realistis mampu memengaruhi persepsi publik secara signifikan.

5. DISKUSI

Hasil penelitian ini menunjukkan bahwa penggunaan media *busy book* berbasis aktivitas mampu meningkatkan kemandirian anak, sebuah temuan yang sejalan dengan penjelasan dalam [2] mengenai peran stimulasi taktil dalam pembelajaran anak usia dini. Peningkatan skor observasi pada setiap pertemuan memperlihatkan bahwa media berstruktur memberikan dukungan perkembangan yang stabil. Respons anak yang semakin konsisten memperlihatkan bahwa aktivitas berbasis eksplorasi fisik memberikan pengalaman belajar yang sesuai tahap perkembangan. Temuan ini mendukung pemahaman sebelumnya yang menekankan bahwa aktivitas manipulatif berkontribusi pada pembentukan *self-help skills* sebagaimana dijelaskan dalam [5].

Perbandingan dengan penelitian terdahulu menunjukkan bahwa temuan penelitian ini memperkuat laporan dalam [7] yang menjelaskan bahwa aktivitas *hands-on* meningkatkan fokus dan ketekunan anak. Tingkat keterlibatan anak yang terlihat dalam setiap sesi juga mengikuti pola yang dijelaskan oleh [10] terkait efektivitas media taktil dalam memfasilitasi pemahaman instruksional. Namun, adanya beberapa anak yang memerlukan waktu adaptasi lebih lama berbeda dengan laporan dalam [9] yang menunjukkan adaptasi lebih cepat, sehingga memberikan indikasi bahwa faktor karakter individual dapat memengaruhi kecepatan respons. Perbedaan ini memberi wawasan bahwa dinamika kelas dan kesiapan anak turut menentukan efektivitas media.

Fenomena fluktuasi perilaku pada awal pertemuan sejalan dengan catatan dalam [3] yang menyebutkan bahwa interaksi awal dengan media baru sering memunculkan variasi respons sebelum mencapai stabilitas. Ketertarikan anak pada warna dan bentuk tertentu juga mendukung penjelasan dalam [4] bahwa stimulus visual memiliki pengaruh besar terhadap perhatian anak usia dini. Pola respons tersebut memperlihatkan bahwa media *busy book* berfungsi tidak hanya sebagai alat instruksional, tetapi juga sebagai sarana regulasi sensorik. Temuan ini memberi pemahaman bahwa pembelajaran berbasis aktivitas memerlukan adaptasi lingkungan yang sesuai kebutuhan sensorik anak.

Secara teoritis, penelitian ini memperluas dukungan empiris terhadap kerangka kerja yang dijelaskan dalam [6] mengenai media aktif sebagai pemicu perkembangan kemandirian anak. Dari sisi praktis, media *busy book* memberikan alternatif pembelajaran yang mudah digunakan dan dapat diintegrasikan dalam rutinitas kelas maupun rumah. Observasi perilaku anak selama penggunaan media juga menunjukkan potensinya

p-ISSN : 2803-1507 e-ISSN : 2803-1531

sebagai alat asesmen informal, selaras dengan pandangan pada [11] mengenai asesmen berbasis aktivitas. Meskipun demikian, penelitian ini memiliki keterbatasan pada jumlah subjek dan variasi aktivitas, sehingga hasil yang diperoleh perlu dipahami dalam konteks ruang lingkup implementasi yang terbatas.

6. KESIMPULAN DAN SARAN

6.1 *Kesimpulan*

Berdasarkan penelitian yang telah dijelaskan, maka dapat disimpulkan bahwa teknologi AI berkembang pesat. Namun, terdapat banyak oknum yang menyalahgunakannya terutama pada teknologi berbasis *deepfake*. Penyalahgunaan teknologi AI berbasis *deepfake* sangat berbahaya bagi semua masyarakat yang dapat menimbulkan sanksi hukum, sosial, dan moral. Terdapat motif yang mendorong pelaku untuk melakukan penyalahgunaan *deepfake*, salah satu motif dari kasus yang diamati yaitu balas dendam pribadi yang disebabkan karena sakit hati. Oleh karena itu, untuk mencegah terjadinya hal tersebut perlu adanya edukasi etika dalam penggunaan teknologi AI berbasis *deepfake* dan pemahaman mengenai Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pornografi, dan Undang-Undang Perlindungan Data Pribadi.

6.2 *Saran*

Dalam mencegah dan mengurangi penyelahgunaan teknologi *deepfake*, perlu kerja sama dari berbagai pihak terkait. Pemerintah perlu memperkuat dan memperbaharui hukum terkait *deepfake* dan menindak tegas pelaku kejahatan teknologi AI berbasis *deepfake*. Lalu, edukasi masyarakat agar lebih waspada terhadap konten ilegal dan menerapkan nilai etika, tanggung jawab, serta tanggung jawab dalam penggunaan teknologi AI. Selain itu, upaya koordinasi antara regulator, penyedia platform digital, dan masyarakat dapat memperkuat pencegahan penyalahgunaan teknologi ini secara lebih efektif.

DAFTAR PUSTAKA

[1] N. Ramadhina, F. Jason, M. F. Pratama, L. A. Raihan, S. Al Mufti, and M. Meranti, "Dinamika Perubahan dalam Komunikasi Manusia di Era Teknologi Artificial Intelligence," *Commun. Sph.*, vol. 3, no. 2, pp. 114–123, 2023, doi: 10.55397/cps.v3i2.57.

[2] S. Arkha, A. Nugroho, and A. Wibowo, "Evaluating Digital Transformation within Integration Limitations using Desk-Based Analytical Case Study," *J. Technol. Informatics Eng.*, vol. 4, no. 2, pp. 289–299, Aug. 2025, doi: 10.51903/jtie.v4i2.365.

[3] K. D. Purnama and G. Manalu, "Evolution and Challenges of Customer Relationship Management (CRM) Implementation in the Digital Economy: A Systematic Review," *J. Manag. Informatics*, vol. 3, no. 1, pp. 71–86, Apr. 2024, doi: 10.51903/jmi.v3i1.40.

[4] S. U. Anggono and S. Supriyanto, "Peluang dan Tantangan Sistem Pelatihan Berbasis AI dalam Meningkatkan Keterampilan Tenaga Kerja di Era Digital," *J. Ilm. Sist. Inf.*, vol. 4, no. 2, pp. 224–231, May 2025, doi: 10.51903/6mbmzk12.

[5] A. Wahyudi, M. B. T. Assyamiri, W. Al Aluf, M. R. Fadhillah, S. Yolanda, and M. I. Anshori, "Dampak Transformasi Era Digital Terhadap Manajemen Sumber Daya Manusia," *J. Bintang Manaj.*, vol. 1, no. 4, pp. 99–111, 2023, doi: 10.55606/jubima.v1i4.2222.

[6] M. Farwati, I. T. Salsabila, K. R. Navira, and T. Sutabri, "Analisa Pengaruh Teknologi Artificial Intelligence (AI) dalam Kehidupan Sehari-Hari," *J. Sist. Inform. dan Menejemen*, vol. 11, no. 1, pp. 41–42, 2023, doi: 10.47024/js.v11i1.563.

[7] Arnolus Juantri E. Oktavianus, Lamhot Naibaho, and Djoys Anneke Rantung, "Pemanfaatan Artificial Intelligence pada Pembelajaran dan Asesmen di Era Digitalisasi," *J. Kridatama Sains Dan Teknol.*, vol. 5, no. 2, pp. 473–476, 2023, doi: 10.53863/kst.v5i02.975.

[8] A. M. Fauzan, J. Mudjrimin, and S. Sulfikar, "Kejahatan Dunia Maya (Cybercrime) dalam Prespektif Hukum Islam dan Hukum Positif Masyarakat di Indonesia," *Bayt Al Hikmah J. Pendidik. dan Pengemb. Masy. Islam*, vol. 1, no. 1, pp. 143–153, 2025, doi: 10.54065/baytal-hikmah.414.

[9] Markus Djarawula, Novita Alfiani, and Hanita Mayasari, "Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) di Indonesia Ditinjau dari Perspektif Undang-Undang Nomor 11

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Tahun 2008 Tentang Informasi dan Transaksi Elektronik," *J. Cakrawala Ilm.*, vol. 2, no. 10, pp. 3799–3806, 2023, doi: 10.53625/jcijurnalcakrawalailmiah.v2i10.5842.

[10] M. T. Darmawan, A. Junaidi, and A. Khaerudin, "Penegakan Hukum terhadap Penyalahgunaan Deepfake Pada Pornografi Anak di Era Artifical Intelegence di Indonesia," *J. Serambi Huk.*, vol. 18, no. 1, pp. 42–54, 2025, doi: 10.59582/sh.v18i01.1257.

[11] I. D. Kasita, "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) di Era Pandemi Covid-19," *J. Wan. dan Kel.*, vol. 3, no. 1, pp. 16–26, 2022, doi: 10.22146/jwk.5202.

[12] L. Rachmaria and Andy Susanto, "Potensi Kekerasan Gender Berbasis Online pada Penyalahgunaan Teknologi Kecerdasan Buatan Bagi Perempuan di Media," *J. Netnografi Komun.*, vol. 2, no. 2, pp. 51–63, 2024, doi: 10.59408/jnk.v2i2.25.

[13] Y. S. Kristiyenda, J. Faradila, and C. Basanova, "Pencegahan Kejahatan Deepfake: Studi Kasus terhadap Modus Penipuan Deepfake Prabowo Subianto dalam Tawaran Bantuan Uang," *ALADALAH J. Polit. Sos. Huk. dan Hum.*, vol. 3, no. 2, pp. 149–164, 2025, doi: 10.59246/aladalah.v3i2.1263.

[14] Desty Aster Yansen Basah, A. Wijaya, and I. Januardy, "Kriminalisasi Pelanggaran Protokol Digital: Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake di Media Sosial," *Innov. J. Soc. Sci. Res.*, vol. 5, no. 4, pp. 386–398, 2025, doi: 10.31004/innovative.v5i4.20258.

[15] H. Prayoga and H. Tuasikal, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis terhadap Penegakan Hukum dan Perlindungan Publik di Indonesia," *Abdurrauf Law Sharia*, vol. 1, no. 2, pp. 22–38, 2024, doi: 10.70742/arlash.v2i1.194.

[16] I. & Y. D. H. Antonius Havik, "Analisis Hukum terhadap Instrumen Kebijakan Pemerintah dalam Mewujudkan Akselerasi Literasi Digital," *Pros. Semin. Nas. Progr. Stud. Ilmu Pemerintahan. Univ. Galuh*, vol. 13, no. 1, pp. 104–116, 2022, [Online]. Available: https://repository.unigal.ac.id/handle/123456789/1177

[17] A. Aprilianti, "Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi," *Begawan Abioso*, vol. 15, no. 1, pp. 41–50, 2025, doi: 10.37893/abioso.v15i1.1002.

[18] S. L. Zahara, Z. U. Azkia, and M. M. Chusni, "Implementasi Teknologi Artificial Intelligence (AI) dalam Bidang Pendidikan," *J. Penelit. Sains dan Pendidik.*, vol. 3, no. 1, pp. 15–20, 2023, doi: 10.23971/jpsp.v3i1.4022.

[19] N. Fatimah and D. Octaviani, "Sejarah Pendidikan Indonesia Baru: Perkembangan Pembelajaran Sejarah Berbasis Artificial Intelligence (AI) 4.0," *J. Sej. Indones.*, vol. 6, no. 2, pp. 168–179, 2023, doi: 10.62924/jsi.v6i2.32607.

[20] R. N. Akbari and A. Fithry, "Menganalisis Pengaruh Hak Cipta dalam Gangguan AI pada Sektor Media," *Pros. SNAPP Sos. Humaniora, Pertanian, Kesehat. dan Teknol.*, vol. 2, no. 1, pp. 377–383, 2024, doi: 10.24929/snapp.v2i1.3159.

[21] D. Wanda and S. Putri, "Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi Deepfake di Indonesia," *Rechtsvinding*, vol. 14, no. 2, p. 202, 2025, doi: 10.33331/rechtsvinding.v14i2.2135.

[22] C. T. Noerman and A. L. Ibrahim, "Kriminalisasi Deepfake di Indonesia Sebagai Bentuk Pelindungan Negara," *J. USM Law Rev.*, vol. 7, no. 2, pp. 1–4, 2024, doi: 10.26623/julr.v7i2.8995.

[23] K. A. R. Putri, H. D. Saputro, and A. Amanita, "Pertanggungjawaban Hukum Atas Penggunaan Artificial Intelligence untuk Deepfake Menurut UU Perlindungan Data Pribadi," *Rechtswetenschap J. Mhs. Huk.*, vol. 2, no. 2, 2025, doi: 10.36859/rechtswetenschap.v2i2.3962.

[24] A. Herdian and U. Sumarwan, "Analisis Kriminologi Deepfake Melalui Media Sosial Berdasarkan Teori Rational Choice," *Kraith-Humaniora*, vol. 9, no. 1, pp. 323–31, 2025, doi: 10.37817/ikraith-humaniora.

[25] C. N. P. Hernawan, D. T. Antow, and A. V. Sendow, "Tinjauan Hukum Mengenai Penyalahgunaan Artificial Intelligence dalam Tindak Pidana Kekerasan Seksual," *Lex Priv.*, vol. 15, no. 4, pp. 1–12, 2025, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/61860

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[26] M. R. P. Wijaya and I. M. W. Darma, "Pertanggungjawaban Pidana dan Perlindungan Korban dalam Penyebaran Deepfake Pornografi melalui Media Sosial," *J. Ilmu Sos. Huk.*, vol. 3, no. 4, pp. 4741–4750, 2025, doi: 10.61104/alz.v3i4.2082.

[27] H. P. Sari, D. I. Mulyani, M. A. Nilamsari, D. D. F. Sitorus, and Y. W. Harimurti, "Efektivitas Hukum Perlindungan Data Pribadi terhadap Kejahatan Siber di Indonesia," *J. Media Akad.*, vol. 2, no. 11, pp. 3031–5220, 2024, doi: 10.62281/v2i11.1009.

[28] T. Birkstedt, M. Minkkinen, A. Tandon, and M. Matti, "AI Governance: Themes, Knowledge Gaps and Future Agendas," *Internet Res.*, vol. 33, no. 7, pp. 133–167, 2025, doi: 10.1108/intr-01-2022-0042.

[29] E. Papagiannidis, I. Merete, E. Chirstian, D. Patrick, and M. John, "Toward AI Governance : Identifying Best Practices and Potential Barriers and Outcomes," *Inf. Syst. Front.*, pp. 123–141, 2023, doi: 10.1007/s10796-022-10251-y.

[30] M. A. Camilleri, "Artificial Intelligence Governance: Ethical Considerations and Implications for Social Responsibility," *Expert Syst.*, vol. 41, no. 7, p. 13406, 2024, doi: 10.1111/exsy.13406.

[31] F. Malahati, A. U. B, P. Jannati, Q. Qathrunnada, and S. Shaleh, "Kualitatif: Memahami Karakteristik Penelitian Sebagai Metodologi," *J. Pendidik. Dasar*, vol. 11, no. 2, pp. 341–348, 2023, doi: 10.46368/jpd.v11i2.902.