

ETIKA DIGITAL & PENCEGAHAN PENYALAHGUNAAN SISTEM

Ade Novia Maulana, Salsabila Zahrani, Serin Fitri Wanti, M Roni Harfaris

UIN Sulthan Thaha Saifuddin Jambi

ARTICLE INFO

Article history:

Received Desember 2025

Revised Desember 2025

Accepted Desember 2025

Available online Desember 2025

Email:

ade@uinjambi.ac.id

salsabilazahrani14@gmail.com

serinfitri.20@gmail.com

muhammadroniharfari@gmail.com



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

Copyright © 2025 by Author.

Abstrak

Perkembangan teknologi informasi yang semakin pesat menghadirkan berbagai kemudahan dalam aktivitas digital, namun juga membuka peluang terjadinya penyalahgunaan sistem yang dapat mengancam keamanan informasi. Artikel ini membahas secara komprehensif mengenai etika digital sebagai fondasi perilaku pengguna dalam ruang siber serta pentingnya penerapan langkah-langkah preventif untuk mencegah penyalahgunaan sistem. Etika digital tidak hanya mencakup kepatuhan terhadap norma dan aturan hukum, tetapi juga tanggung jawab moral dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi. Melalui pendekatan literatur dan analisis konseptual, artikel ini menekankan bahwa pemahaman etika digital perlu ditanamkan sejak dini untuk membangun budaya keamanan digital yang berkelanjutan. Selain itu, upaya pencegahan penyalahgunaan sistem dapat dilakukan melalui penerapan kebijakan keamanan, penguatan kontrol akses, edukasi pengguna, serta penggunaan teknologi deteksi dan mitigasi ancaman. Hasil kajian menunjukkan bahwa integrasi antara etika digital dan manajemen keamanan sistem memiliki peran krusial dalam menciptakan ekosistem digital yang aman dan bertanggung jawab. Artikel ini diharapkan dapat memberikan kontribusi bagi peningkatan kesadaran dan perilaku etis dalam penggunaan teknologi informasi di berbagai sektor.

Kata Kunci: etika digital, keamanan informasi, penyalahgunaan sistem, keamanan siber, literasi digital.

Abstract

The rapid development of information technology offers various conveniences in digital activities, but also opens up opportunities for system abuse that can threaten information security. This article comprehensively discusses digital ethics as the foundation of user behavior in cyberspace and the importance of implementing preventive measures to prevent system abuse. Digital ethics encompasses not only compliance with legal norms and regulations but also the moral responsibility to maintain the integrity, confidentiality, and availability of information. Through a literature review and conceptual analysis, this article emphasizes the need to instill an understanding of digital ethics from an early age to build a sustainable digital security culture. Furthermore, efforts to prevent system abuse can be implemented through the implementation of security policies, strengthening access controls, user education, and the use of threat detection and mitigation technology. The study's results indicate that the integration of digital ethics and system security management plays a crucial role in creating a safe and responsible digital ecosystem. This article is expected to contribute to increasing awareness and ethical behavior in the use of information technology across various sectors.

Keywords: digital ethics, information security, system abuse, cybersecurity, digital literacy.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) dalam dua dekade terakhir telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia (Mildawati & Masyhuri, 2025). Transformasi digital yang terjadi tidak hanya memudahkan proses komunikasi, pekerjaan, dan pembelajaran, tetapi juga menciptakan ruang baru bagi masyarakat untuk berinteraksi, bertransaksi, dan berbagi informasi. Dalam konteks ini, dunia digital telah menjadi bagian integral dari aktivitas sehari-hari, mulai dari penggunaan media sosial, layanan perbankan elektronik, sistem informasi organisasi, hingga perangkat berbasis Internet of Things (IoT) (Santia et al., 2025). Namun, kemajuan tersebut juga diikuti dengan meningkatnya risiko yang berkaitan dengan keamanan informasi dan penyalahgunaan sistem digital. Fenomena

seperti peretasan, pencurian data, penipuan daring, penyebaran malware, dan pelanggaran privasi menunjukkan bahwa ruang digital tidak sepenuhnya aman dan memerlukan perhatian serius dari seluruh pihak.

Di tengah pesatnya perkembangan digital, aspek etika digital menjadi semakin relevan (Putri Hakiki et al., 2025). Etika digital berkaitan dengan seperangkat nilai, prinsip, dan norma yang mengatur bagaimana individu dan organisasi seharusnya berperilaku ketika memanfaatkan teknologi informasi. Ruang digital tidak hanya membutuhkan keterampilan teknis, tetapi juga kesadaran moral agar pemanfaatan teknologi tidak menimbulkan dampak negatif bagi orang lain maupun bagi sistem itu sendiri (Ady Riyansyah & Miswan Ansori, 2024). Misalnya, tindakan sederhana seperti berbagi informasi tanpa verifikasi, menggunakan perangkat lunak bajakan, atau menyebarkan konten berbahaya dapat berkontribusi terhadap rusaknya tatanan digital yang aman dan sehat. Oleh karena itu, pembahasan mengenai etika digital merupakan bagian penting dalam upaya menciptakan lingkungan siber yang bertanggung jawab.

Selain etika digital, pencegahan penyalahgunaan sistem juga merupakan isu utama dalam keamanan informasi (Michael, 2025). Penyalahgunaan sistem dapat terjadi dalam berbagai bentuk, seperti akses ilegal terhadap data, manipulasi sistem untuk keuntungan pribadi, sabotase infrastruktur digital, serta eksploitasi kerentanan dalam perangkat lunak atau jaringan (Setiawan et al., 2025). Tantangan ini tidak hanya dihadapi oleh organisasi besar seperti perusahaan dan lembaga pemerintah, tetapi juga oleh individu pengguna teknologi. Ancaman keamanan seperti phishing, ransomware, dan rekayasa sosial seringkali menasar pengguna yang memiliki tingkat literasi digital rendah. Dengan kata lain, setiap individu dan organisasi memiliki potensi menjadi target maupun pelaku penyalahgunaan sistem apabila tidak memiliki pemahaman yang memadai mengenai keamanan digital.

Kondisi tersebut menunjukkan perlunya integrasi antara etika digital dan upaya pencegahan penyalahgunaan sistem sebagai langkah strategis dalam menjaga keamanan informasi (Anisah et al., 2021). Keduanya tidak dapat dipisahkan karena kesadaran etis yang kuat dapat meminimalkan tindakan yang berpotensi merusak sistem, sementara strategi pencegahan yang efektif membutuhkan partisipasi aktif dari pengguna yang memiliki pemahaman etis. Misalnya, penerapan kebijakan keamanan seperti autentikasi berlapis, manajemen kata sandi yang baik, serta pengelolaan izin akses akan lebih terlaksana dengan optimal apabila didukung oleh perilaku pengguna yang sadar dan bertanggung jawab. Tanpa etika digital, teknologi keamanan secanggih apa pun tetap dapat dilanggar melalui kelalaian manusia.

Selain itu, perkembangan regulasi terkait keamanan informasi dan perlindungan data pribadi semakin memperkuat urgensi penerapan etika digital dalam kehidupan sehari-hari. Pemerintah di berbagai negara, termasuk Indonesia, telah mengimplementasikan perangkat hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP) sebagai landasan untuk mengatur perilaku di ruang digital (Judijanto & Madah Khulaili Harsya, 2025). Namun, regulasi tidak akan efektif tanpa adanya kesadaran kolektif dari masyarakat untuk mematuhi nilai-nilai etis dalam menggunakan teknologi. Oleh karena itu, edukasi etika digital harus menjadi bagian dari kurikulum pendidikan, pelatihan organisasi, dan kampanye sosial agar masyarakat memahami hak dan kewajiban dalam ruang digital.

Di lingkungan akademik, pembahasan mengenai etika digital dan pencegahan penyalahgunaan sistem menjadi penting karena mahasiswa sebagai generasi digital native merupakan pengguna aktif teknologi dan calon profesional yang akan bekerja di sektor berbasis informasi. Penguatan pemahaman mengenai kedua aspek tersebut dapat membantu mahasiswa membangun karakter yang bertanggung jawab dalam mengembangkan, mengakses, maupun mengelola sistem informasi. Dalam konteks mata kuliah Keamanan Informasi, kajian etika

digital tidak hanya memberikan pengetahuan teoritis, tetapi juga membentuk pola pikir kritis agar mahasiswa mampu menilai tindakan yang tepat dalam berbagai situasi digital.

Artikel ini disusun untuk mengkaji lebih dalam mengenai konsep etika digital dan langkah-langkah preventif yang dapat dilakukan dalam mencegah penyalahgunaan sistem. Dengan menggunakan pendekatan literatur dan analisis konseptual, artikel ini berupaya memberikan pemahaman komprehensif mengenai pentingnya hubungan antara perilaku etis pengguna dan keamanan sistem informasi. Pembahasan dilakukan dengan menyoroti aspek-aspek kunci seperti prinsip etika digital, bentuk-bentuk penyalahgunaan sistem, peran teknologi keamanan, serta pentingnya budaya keamanan digital di berbagai sektor.

Dengan adanya kajian ini, diharapkan pembaca dapat memahami bahwa etika digital bukan sekadar aturan tertulis, tetapi merupakan panduan moral yang berfungsi menjaga keberlangsungan ekosistem digital. Sementara itu, pencegahan penyalahgunaan sistem bukan hanya tanggung jawab tenaga profesional IT, tetapi merupakan kewajiban semua pengguna teknologi. Sinergi antara keduanya akan menjadi fondasi penting dalam menciptakan lingkungan digital yang aman, produktif, dan berkelanjutan. Artikel ini juga diharapkan dapat menjadi referensi bagi mahasiswa, praktisi, dan peneliti yang ingin mendalami isu keamanan informasi secara lebih holistik.

METODELOGI

Penelitian ini menggunakan pendekatan kualitatif-deskriptif dengan tujuan untuk menganalisis konsep etika digital dan strategi pencegahan penyalahgunaan sistem dalam konteks keamanan informasi. Metode ini dipilih karena memungkinkan peneliti untuk menggali secara mendalam fenomena, konsep, serta isu-isu yang relevan melalui penelusuran literatur ilmiah dan analisis dokumen (Dinarti et al., 2024). Sumber data utama dalam penelitian ini berasal dari jurnal ilmiah, buku, laporan penelitian, peraturan perundang-undangan, serta publikasi digital yang membahas etika digital, keamanan informasi, dan bentuk-bentuk penyalahgunaan sistem. Literatur yang digunakan dipilih berdasarkan relevansi tema, kemutakhiran publikasi (minimal tahun 2018 ke atas), dan kredibilitas sumber.

Proses pengumpulan data dilakukan melalui teknik studi pustaka (library research). Tahapan ini meliputi identifikasi sumber literatur, klasifikasi konten berdasarkan topik kajian, dan ekstraksi informasi penting terkait prinsip etika digital, jenis ancaman keamanan, serta langkah-langkah preventif dalam mencegah penyalahgunaan sistem (Puspitarani et al., 2025). Selanjutnya, data dianalisis menggunakan metode analisis isi (content analysis). Analisis ini dilakukan dengan membaca, memahami, dan menginterpretasikan isi literatur untuk menemukan pola, hubungan antar konsep, serta kesimpulan yang dapat menjelaskan pentingnya integrasi etika digital dalam keamanan informasi.

Penelitian ini juga memanfaatkan teknik triangulasi sumber guna memastikan validitas informasi. Triangulasi dilakukan dengan membandingkan temuan dari berbagai literatur untuk menghindari bias dan memastikan bahwa data yang digunakan bersifat akurat dan konsisten. Hasil analisis kemudian disusun dalam bentuk uraian deskriptif yang sistematis, yang mencakup pemaparan konsep etika digital, penjelasan mengenai penyalahgunaan sistem, serta rekomendasi strategis terkait pencegahannya.

Dengan menggunakan metodologi ini, penelitian diharapkan mampu menghasilkan kajian teoritis yang komprehensif dan relevan dalam menjawab kebutuhan penguatan keamanan informasi berbasis perilaku etis pengguna di ruang digital.

HASIL DAN PEMBAHASAN

Perkembangan teknologi informasi yang semakin masif dalam kehidupan masyarakat telah menempatkan ruang digital sebagai bagian penting dari aktivitas sehari-hari (Elvis et al., 2025). Namun, perubahan ini membawa dampak ganda: di satu sisi memberikan kemudahan, tetapi di sisi lain meningkatkan potensi ancaman keamanan informasi (Saguni, 2025). Hasil kajian literatur menunjukkan bahwa etika digital dan pencegahan penyalahgunaan sistem merupakan dua komponen yang saling berkaitan dan tidak dapat dipisahkan dalam menciptakan ekosistem digital yang aman dan bertanggung jawab (Tri Setia Ningrum et al., 2025). Pembahasan berikut memaparkan hasil analisis mengenai konsep etika digital, bentuk penyalahgunaan sistem, serta strategi pencegahannya berdasarkan sintesis dari berbagai sumber ilmiah.

1. Konsep Etika Digital sebagai Fondasi Keamanan Informasi

Etika digital merujuk pada seperangkat nilai, norma, dan prinsip moral yang mengatur perilaku manusia dalam menggunakan teknologi informasi (Astuti et al., 2025). Hasil analisis menunjukkan bahwa etika digital tidak hanya mencakup kepatuhan terhadap hukum dan aturan formal, tetapi juga penginternalisasian nilai moral yang memandu perilaku pengguna. Menurut beberapa literatur, etika digital terdiri atas beberapa prinsip dasar: tanggung jawab, integritas, keadilan, penghormatan terhadap privasi, dan kesadaran akan dampak.

Prinsip tanggung jawab mengharuskan setiap pengguna untuk memahami konsekuensi dari setiap tindakan digital, termasuk cara mengelola data, menggunakan platform digital, dan menyebarkan informasi (Amala et al., 2023). Prinsip integritas menekankan kejujuran dalam setiap aktivitas digital, seperti tidak melakukan manipulasi data atau penyebaran informasi palsu. Prinsip keadilan menuntut pengguna untuk memperhatikan hak-hak digital orang lain, seperti hak privasi, hak akses, dan hak atas keamanan. Sementara itu, penghormatan terhadap privasi berkaitan dengan bagaimana individu menjaga informasi sensitif baik milik sendiri maupun orang lain. Prinsip ini sangat penting mengingat banyaknya kasus pelanggaran privasi di dunia digital. Kesadaran akan dampak (impact awareness) menuntut pengguna untuk mempertimbangkan dampak jangka panjang dari perilaku digitalnya.

Dari hasil pembahasan literatur, etika digital juga berkaitan erat dengan literasi digital. Pengguna yang memiliki tingkat literasi digital tinggi cenderung lebih memahami risiko dan mampu mengaplikasikan prinsip etika dalam aktivitas digital. Sebaliknya, rendahnya literasi digital sering menjadi faktor penyebab perilaku berbahaya, baik yang disengaja maupun tidak disengaja.

2. Bentuk-bentuk Penyalahgunaan Sistem dalam Ruang Digital

Penyalahgunaan sistem adalah segala bentuk aktivitas yang melibatkan penggunaan sistem informasi untuk tujuan yang tidak sah, merusak, atau memberikan kerugian kepada pihak lain. Dari analisis dokumen dan literatur, beberapa bentuk penyalahgunaan sistem yang umum terjadi antara lain:

a. Akses ilegal (Unauthorized Access)

Merupakan tindakan memasuki sistem tanpa izin untuk mengakses atau mencuri data. Pelaku sering memanfaatkan kelemahan pada jaringan atau menerapkan teknik seperti brute force untuk menembus autentikasi (Rahmawati et al., 2025).

b. Manipulasi dan pencurian data

Melibatkan pengubahan, penghapusan, atau pencurian data untuk keuntungan pribadi. Dampaknya sangat besar bagi organisasi, terutama dalam konteks perlindungan data pribadi.

c. Malware dan serangan siber

Termasuk penyebaran virus, worm, trojan, ransomware, dan spyware. Serangan ini bertujuan merusak sistem, mencuri data, atau memeras korban. Ransomware merupakan salah satu bentuk serangan paling berkembang dalam dekade terakhir.

d. Rekayasa sosial (social engineering)

Serangan ini memanipulasi psikologis pengguna untuk mendapatkan akses atau informasi sensitif (Nurmayuli et al., 2024). Bentuk paling umum adalah phishing melalui email, pesan instan, atau situs palsu.

e. Penyalahgunaan sumber daya sistem

Misalnya menggunakan server organisasi untuk kegiatan ilegal seperti mining cryptocurrency, penyebaran konten terlarang, atau aktivitas hacking.

f. Penyebaran konten ilegal atau berbahaya

Seperti pornografi anak, ujaran kebencian, hoaks, dan propaganda yang mengancam keamanan sosial dan stabilitas digital.

Hasil kajian mengungkap bahwa perkembangan penyalahgunaan sistem sangat dipengaruhi oleh faktor teknologi, sosial, dan perilaku pengguna. Keberadaan teknologi yang semakin canggih tidak serta-merta meningkatkan keamanan apabila tidak diimbangi dengan perilaku etis yang kuat.

3. Faktor Penyebab Penyalahgunaan Sistem

Hasil analisis literatur menunjukkan tiga faktor utama yang mendorong terjadinya penyalahgunaan sistem:

a. Faktor Individu

Kurangnya etika, motif ekonomi, kepuasan pribadi, atau keinginan untuk menunjukkan kemampuan teknis menjadi penyebab utama tindakan penyalahgunaan sistem. Selain itu, rendahnya kesadaran keamanan digital meningkatkan risiko penyalahgunaan, baik secara sengaja maupun tidak.

b. Faktor Teknologi

Kerentanan pada perangkat lunak, lemahnya enkripsi, sistem autentikasi yang tidak kuat, dan kegagalan pembaruan perangkat menjadi celah bagi pelaku kejahatan (Windarto, 2023). Sistem yang tidak memiliki kontrol keamanan memadai sangat rentan terhadap eksploitasi.

c. Faktor Organisasi dan Regulasi

Banyak organisasi belum menerapkan kebijakan keamanan informasi secara optimal. Lemahnya pengawasan, kurangnya pelatihan bagi pengguna, serta ketidaktahuan terhadap regulasi seperti UU ITE atau UU PDP meningkatkan risiko pelanggaran digital.

4. Pentingnya Integrasi Etika Digital dalam Keamanan Informasi

Hasil pembahasan menunjukkan bahwa teknologi keamanan saja tidak cukup untuk melindungi sistem dari penyalahgunaan. Faktor manusia tetap menjadi elemen paling rentan dalam keamanan informasi. Oleh karena itu, integrasi etika digital menjadi keharusan (Ady Riyansyah & Miswan Ansori, 2024).

Etika digital membantu mencegah penyalahgunaan sistem melalui pembentukan kesadaran moral pada pengguna. Individu yang memahami etika digital cenderung menghindari tindakan seperti penggunaan software ilegal, penyebaran data tanpa izin, atau mengakses sistem orang lain.

Etika digital juga berkontribusi dalam menciptakan budaya keamanan (security culture) di organisasi. Budaya ini meliputi pola pikir, kebiasaan, dan praktik sehari-hari yang mendukung keamanan informasi. Organisasi yang menerapkan etika digital dengan baik cenderung memiliki tingkat pelanggaran lebih rendah.

5. Strategi Pencegahan Penyalahgunaan Sistem

Berdasarkan analisis sumber ilmiah, terdapat beberapa langkah strategis yang dapat dilakukan untuk mencegah penyalahgunaan sistem:

a. Penguatan Kebijakan Keamanan Informasi

Organisasi perlu memiliki standar keamanan seperti SOP akses sistem, manajemen risiko, dan kebijakan penggunaan perangkat. Kebijakan harus disosialisasikan secara konsisten.

b. Penerapan Kontrol Akses yang Ketat

Kontrol akses meliputi autentikasi multi-faktor, enkripsi data, prinsip least privilege, dan audit berkala. Semakin ketat akses, semakin kecil peluang penyalahgunaan (Anisah et al., 2021).

c. Pelatihan Etika Digital dan Literasi Keamanan

Edukasi pengguna merupakan kunci utama. Pelatihan dapat mencakup cara mengenali phishing, mengelola kata sandi, menjaga privasi, dan memahami regulasi digital.

d. Implementasi Teknologi Deteksi dan Mitigasi

Teknologi seperti firewall, antivirus, sistem deteksi intrusi (IDS), dan SIEM (Security Information and Event Management) sangat penting dalam mendeteksi aktivitas mencurigakan (Santia et al., 2025).

e. Audit dan Monitoring Sistem Secara Berkala

Pemantauan sistem berfungsi untuk mendeteksi anomali lebih cepat. Audit keamanan memastikan bahwa sistem selalu diperbaharui dan bebas dari celah kritis.

f. Penerapan Regulasi dan Penegakan Hukum

Penerapan UU ITE dan UU PDP perlu ditegakkan untuk memberikan efek jera (Tri Setia Ningrum et al., 2025). Organisasi juga harus memahami aspek hukum untuk menghindari pelanggaran yang tidak disengaja.

6. Kolaborasi Pengguna, Organisasi, dan Pemerintah

Hasil pembahasan menunjukkan bahwa pencegahan penyalahgunaan sistem memerlukan kerja sama tiga pihak:

1. Pengguna: mematuhi etika digital dan menjaga keamanan akun pribadi.
 2. Organisasi: menerapkan kebijakan keamanan dan menyediakan pelatihan.
 3. Pemerintah: membuat regulasi dan menegakkan hukum secara tegas.
- Tanpa kolaborasi ini, sistem digital akan tetap rentan terhadap ancaman.

7. Dampak Positif Integrasi Etika Digital dan Keamanan Informasi

Hasil literatur menunjukkan bahwa integrasi etika digital dengan strategi keamanan dapat menghasilkan manfaat seperti:

1. Menurunnya tingkat serangan internal (insider threat).
2. Meningkatnya kepercayaan publik terhadap layanan digital.
3. Berkurangnya risiko kerugian ekonomi akibat kebocoran data.
4. Meningkatnya kualitas interaksi digital masyarakat.
5. Penguatan budaya keamanan jangka panjang (Dinarti et al., 2024).

Dari hasil analisis, dapat disimpulkan bahwa etika digital memegang peran penting dalam mencegah penyalahgunaan sistem. Tanpa perilaku etis, teknologi keamanan tidak akan efektif, karena sebagian besar kasus pelanggaran berasal dari human error atau kurangnya kesadaran pengguna. Pencegahan penyalahgunaan sistem harus dilakukan secara komprehensif melalui kebijakan, teknologi, edukasi, dan regulasi yang saling melengkapi. Dengan demikian, ekosistem digital yang aman dan berkelanjutan dapat terwujud melalui sinergi antara etika digital dan keamanan informasi.

KESIMPULAN

Etika digital dan pencegahan penyalahgunaan sistem merupakan dua aspek yang saling berkaitan dan sangat penting dalam menciptakan ruang digital yang aman, bertanggung jawab, dan berkelanjutan. Etika digital berfungsi sebagai panduan moral bagi pengguna dalam berinteraksi dengan teknologi, sehingga dapat meminimalkan tindakan yang berpotensi merugikan, baik secara sengaja maupun tidak. Sementara itu, pencegahan penyalahgunaan sistem diperlukan untuk melindungi informasi, menjaga integritas data, serta mengurangi risiko ancaman siber yang semakin kompleks. Hasil kajian menunjukkan bahwa teknologi keamanan tidak akan efektif tanpa kesadaran etis dari pengguna sebagai elemen utama dalam sistem informasi. Oleh karena itu, integrasi antara etika digital, kebijakan keamanan, literasi digital, serta penegakan regulasi merupakan langkah penting yang harus dilakukan secara menyeluruh. Sinergi semua pihak akan memperkuat budaya keamanan digital dan meningkatkan kepercayaan masyarakat dalam memanfaatkan teknologi informasi.

SARAN

Penerapan etika digital perlu diperkuat melalui edukasi berkelanjutan bagi seluruh pengguna teknologi. Organisasi disarankan meningkatkan kebijakan keamanan dan pelatihan literasi digital secara rutin. Pemerintah juga perlu mempertegas regulasi serta pengawasan terhadap pelanggaran keamanan informasi. Kolaborasi semua pihak sangat penting untuk menciptakan ekosistem digital yang aman dan bertanggung jawab.

REFERENSI

- Ady Riyansyah, & Miswan Ansori. (2024). Implikasi Hukum dan Etika Perbankan Syariah Terhadap Transaksi yang Terkait dengan Judi Online. *Jurnal Ilmiah Akutansi*, 5(2), 262-281.
- Amala, Y. ', Thohir, M., Reditiya, V. E., Intan, N., & Sari, P. (2023). Refleksi Mahasiswa dalam Berkeadaban Digital melalui ChatGPT. *Intelektual: Jurnal Pendidikan Dan Studi Keislaman*, 13(2), 109-128. <https://doi.org/10.33367/ji.v13i2.3798>
- Anisah, Delpiah Wahyuningsih, Kiswanto, Chandra Kirana, Elly Yanuari, & Supardi. (2021). PENINGKATAN LITERASI DIGITAL DAN ETIKA SIBER BAGI SISWA MAN 1 BANGKA DI ERA TRANSFORMASI DIGITAL. *Sistem Informasi, Institut Sains Dan Bisnis Atma Luhur*, 6(2), 2745-8725.
- Astuti, A., Thoha, M., Dahliah, J., Maryanti, A., Ambarita, D., Rifa'i, R., & Hidayat, T. (2025). Etika Penggunaan AI di Sekolah: Menyeimbangkan Inovasi Dengan Integritas Akademik. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(2), 5893-5900. <https://doi.org/10.31004/riggs.v4i2.1639>
- Dinarti, N. S., Salsabila, S. R., Tri, Y., Rizky Salsabila, S., Herlambang, Y. T., Guru, P., & Dasar, S. (2024). Dilema Etika dan Moral dalam Era Digital: Pendekatan Aksiologi Teknologi terhadap Privasi Keamanan, dan Kejahatan Siber. *Daya Nasional Jurnal Pendidikan Ilmu-Ilmu Sosial Dan Humaniora*, 2, 8-16. <https://doi.org/10.26418/jdn.v2i1.74931>
- Elvis, A., Estyawati, L., Lutfiah, , Nafi'ah, S., & Duta Bangsa, U. (2025). Etika dan Hukum dalam Penggunaan Teknologi Pengawasan Digital oleh Negara Ethics and Law in the Use of Digital Surveillance Technology by States. *LITERA: Jurnal Ilmiah Multidisiplin*, 2(4), 510-516. <https://litera-academica.com/ojs/litera/>
- Judijanto, L., & Madah Khulaili Harsya, R. (2025). Etika dan Hukum dalam Penggunaan Artificial Intelligence terhadap Privasi Digital di Indonesia. *Sanskara Hukum Dan HAM*, 3(3), 141-149. <https://doi.org/10.58812/shh.v3.i03>

- Michael, J. P. (2025). Integrasi Prinsip Etika Profesional dalam Data Governance untuk Mendukung Keamanan dan Akurasi Informasi di Era Digital. *Journal of Multidisciplinary Inquiry in Science*, 2(1), 828-834. <https://doi.org/10.32672/mister.v2i1.2570>
- Mildawati, & Masyhuri. (2025). Peran Kode Etik Dalam Mencegah Fraud di Era Transformasi Digital Pada Lembaga Keuangan Syariah di Indonesia. *JoSES: Journal of Sharia Economics Scholar*, 2(5), 124-134. <https://doi.org/10.5281/zenodo.15489620>
- Nurmayuli, Nafhiza Muchfazillah, Mir Atil Hayati, & Nurmali. (2024). Isu Sosial Dan Etika Dalam Sistem Informasi Manajemen. *Journal Education and Social Science*, 02(02), 15-32.
- Puspitarani, S., Palangka Raya Reina Dewi Masitoh, U., & Palangka Raya Jadianan Parhusip, U. (2025). Dampak Teknologi Informasi dan Etika Profesi terhadap Kinerja dan Integritas Profesional di Era Digital. *Jurnal Sains Student Research*, 3(1), 16-20. <https://doi.org/10.61722/jssr.v3i1.3101>
- Putri Hakiki, W., Meirisa, S., Marsyah, S., Dwi Yanti, A., Khaira, N., Nafisyah Qonita, W., Dedi Syaputra, F., Permana, H., & Marweny, E. (2025). Peran Pancasila Sebagai Sistem Etika Dalam Pencegahan Kecanduan Game Online Di Kalangan Remaja. *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, 1(3), 350-356. <https://jurnal.globalscients.com/index.php/jkhp>
- Rahmawati, R., Al Farizi, C. D., Magdalena, M., Sundawa, D., & Iman, D. (2025). Penyuluhan Kesadaran Hukum dan Etika Digital dalam Pencegahan Cyber Bullying bagi Peserta Didik SMA Santa Maria 2 Bandung. *Jurnal Pendidikan Dan Pengabdian Masyarakat*, 8(2), 224-230. <https://doi.org/10.29303/jppm.v8i2.9041>
- Saguni, F. (2025). Kecerdasan Buatan dalam Perspektif Islam: Etika dan Arah Pengembangan. *Prosiding Kajian Islam Dan Integrasi Ilmu Di Era Society 5.0 (KIIIES 5.0) Pascasarjana Universitas Islam Negeri Datokarama Palu 2025*, 2962-7257. <https://jurnal.uindatokarama.ac.id/index.php/kiiies50/index>
- Santia, O., Nurlia Ahmad, A., & Muwafiq, J. A. (2025). SOSIALISASI ETIKA DIGITAL DAN PENCEGAHAN PENYALAHGUNAAN BAGI PENGURUS DEMA-FST UNIVERSITAS ISLAM NEGERI SULTHAN THAHA SAIFUDDIN JAMBI. *Kohesi: Jurnal Multidisiplin Saintek*, 10(6), 1-5. <https://doi.org/10.8734/Kohesi.v1i2.365>
- Setiawan, I., Chalim, A., & Rahma Amalia, A. (2025). ETIKA DIGITAL DALAM PERSPEKTIF PENDIDIKAN AGAMA ISLAM. *AL-IMAN: Jurnal Keislaman Dan Kemasyarakatan*, 9(1), 284-304.
- Tri Setia Ningrum, Vika Dias Anspratiwi, & Muhamad Wahyudi. (2025). ETIKA DAN DAMPAK SOSIAL DARI PENERAPAN ARTIFICIAL INTELLIGENCE DALAM SISTEM INFORMASI MANAJEMEN. *Jurnal Riset Sistem Informasi*, 2(1), 06-15. <https://doi.org/10.69714/26ypxk67>
- Windarto, W. (2023). LITERASI DIGITAL DALAM ETIKA BERMEDIA SOSIAL YANG BERBUDI LUHUR BAGI WARGA KRENDANG, TAMBORA, JAKARTA BARAT. *Sebatik*, 27(1), 201-207. <https://doi.org/10.46984/sebatik.v27i1.2266>