Nusantara Journal of Multidisciplinary Science
Vol. 2, No. 5, Desember 2024
Hal 1130-1137
E-ISSN : 3024-8752
P-ISSN : 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Pentingnya Etika Siber pada Era Digital

Dimas Abimanyu Prasetyo[1], Farhan Dwi Setiawan[2], Jeremiah Marvin Kapoyos[3], Mochamad Reyhan Gusnaldi[4], Wildan Hamzah Nur Fadholi[5], Nurfiyah[6]
[1,2,3,4,5,6] Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

Article Info

Article history:

Received Desember 17, 2024
Revised Desember 20, 2024
Accepted Desember 26, 2024

Kata Kunci:

Etika Siber,
Era Digital,
Kejahatan Siber

Keywords:

Cyber Ethics,
Digital Era,
Cybercrime

ABSTRAK

Masalah etika terkait berkomunikasi digital, juga dikenal sebagai "etika siber", muncul sebagai akibat dari penggunaan teknologi komunikasi yang semakin meningkat. Masalah etika ini berkaitan dengan bagaimana masyarakat dapat berinteraksi satu sama lain di dunia digital melalui media sosial. Penelitian Microsoft, yang memperkirakan kesopanan pengguna internet pada tahun 2020, mendukung hal ini. Hasilnya, Indonesia berada di urutan ke-29 dalam hal pengguna internet di antara 32 negara yang disurvei. Hasilnya, Indonesia adalah negara yang paling tidak beradab di Asia Tenggara. Perbaikan lebih lanjut diperlukan untuk meningkatkan moral internet di Indonesia Dalam penelitian ini, metode deskriptif kualitatif digunakan. 'Pentingnya Etika Siber pada Era Digital' dibahas dalam jurnal ini. Melalui sejumlah inisiatif untuk melindungi data pribadi, menjunjung tinggi hak asasi manusia secara online, dan mencegah kejahatan di ranah digital, hal ini menunjukkan pentingnya dunia maya di era modern. Penggunaan teknologi harus dipandu oleh etika untuk mengurangi dampak buruk pada keamanan dan privasi data. Dalam hal teknologi, etika mencakup prinsip dan panduan yang harus diikuti untuk melindungi privasi dan keamanan orang. Nilai melindungi informasi pribadi dan menjunjung tinggi privasi individu ditekankan oleh etika. Informasi pribadi harus ditangani dengan bermartabat dan hanya digunakan untuk tujuan yang tepat, sesuai dengan norma etika di era digital, kemajuan teknologi telah membawa dampak besar dalam kehidupan manusia, baik dalam komunikasi, pendidikan, maupun bisnis. Namun, hal ini juga menimbulkan tantangan etis yang signifikan, seperti penyalahgunaan data pribadi, serangan siber, penyebaran informasi palsu, dan pelanggaran privasi. Oleh karena itu, penerapan etika siber menjadi sangat penting untuk menjaga keamanan dan kestabilan di dunia maya.

ABSTRACT

Ethical issues related to digital communication, also known as "cyber ethics", arise as a result of the increasing use of communication technologies. These ethical issues relate to how people can interact with each other in the digital world through social media. Microsoft's research, which estimates the civility of internet users in 2020, supports this. It found that Indonesia ranks 29th in terms of internet users among the 32 countries surveyed. As a result, Indonesia is the least civilized country in Southeast Asia. Further improvements are needed to improve internet morale in Indonesia In this study, a qualitative descriptive method was used. 'The Importance of Cyber Ethics in the Digital Age' is discussed in this journal. Through initiatives to protect personal data, uphold human rights online, and prevent crime in the digital realm, it shows the importance of cyberspace in the modern era. When it comes to technology, ethics includes principles and guidelines that must be followed to protect people's privacy and security. The value of protecting personal information and upholding individual privacy is emphasized by ethics. Personal information should be handled with dignity and only used for appropriate purposes, in accordance with ethical norms. In the digital

age, technological advancements have brought great impact in human life, whether in communication, education or business. However, it also poses significant ethical challenges, such as misuse of personal data, cyberattacks, dissemination of false information, and privacy violations. Therefore, the application of cyber ethics is very important to maintain security and stability in cyberspace.

Corresponding Author:

Nurfiyah
Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya,
Bekasi, Indonesia
Email: nurfiyah@dsn.ubharajaya.ac.id

1. PENDAHULUAN

Media sosial adalah salah satu contoh majunya teknologi dan komunikasi online yang sekarang ini banyak dimanfaatkan. Selain digunakan oleh sebagian orang untuk publikasi, komunikasi, dan integrasi sosial, media sosial telah berevolusi untuk digunakan untuk tujuan bisnis, seperti pemasaran dan promosi. Tidak diragukan lagi bahwa perkembangan hukum akan dipengaruhi oleh kemajuan teknologi informasi dan komunikasi (TI). Undang-Undang Nomor 11 Tahun 2008, yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dibuat oleh pemerintah untuk memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara TI [1].

Seperti halnya telepon dan televisi yang sudah menjadi hal yang sering kita jumpai dalam keseharian, internet dan berbagai platform media baru juga telah menjadi fenomena sosial yang ada di mana-mana. Kehidupan masyarakat mengalami perubahan yang signifikan sebagai hasil dari perkembangan internet dan meningkatnya penggunaan sistem informasi. Dengan semua media barunya, internet telah merevolusi pertumbuhan di banyak negara, menghilangkan hambatan perdagangan, dan memungkinkan orang untuk berinteraksi, bekerja sama, dan berbagi ide secara global, mengatasi batasan konvensional waktu, tempat, dan kelas [2]. Dalam hal implementasi teknologi dan standar akses serta penggunaan di seluruh jaringan, penting untuk diingat bahwa Internet tidak memiliki tata kelola yang terpusat; sebaliknya, setiap individu dalam jaringan membuat peraturannya sendiri. [3].

Etika adalah konsep yang menggambarkan karakter moral atau perilaku seseorang. Di sisi lain, moralitas mengacu pada perilaku baik dan tidaknya seseorang. Etika adalah keyakinan dan prinsip-prinsip mengenai moralitas perilaku manusia. Sementara moralitas selalu menilai seberapa baik contoh yang diberikan oleh etika diterapkan, etika selalu berhubungan dengan hal yang baik. Dengan demikian, manusia yang bermoral adalah manusia yang mengikuti contoh perilaku yang patut diteladani, sedangkan manusia yang beretika adalah manusia yang memberikan contoh [4].

Masalah etika terkait berkomunikasi digital, juga dikenal sebagai "etika siber", muncul sebagai akibat dari penggunaan teknologi komunikasi yang semakin meningkat. Masalah etika

ini berkaitan dengan bagaimana masyarakat bisa berinteraksi dengan yang lain di dunia digital dengan melalui media sosial. Penelitian Microsoft, yang memperkirakan kesopanan pengguna internet pada tahun 2020, mendukung hal ini. Hasilnya, Indonesia berada di urutan ke-29 dalam hal pengguna internet di antara 32 negara yang disurvei. Hasilnya, Indonesia adalah negara yang paling tidak beradab di Asia Tenggara. Perbaikan lebih lanjut diperlukan untuk meningkatkan moral internet di Indonesia [5].

Kemajuan teknologi digital dan penggunaan internet yang cepat telah memberikan perubahan besar dalam berbagai macam aspek pada kehidupan manusia, termasuk komunikasi, pendidikan, dan bisnis [6]. Di era digital ini, interaksi manusia dengan teknologi semakin meningkat, sehingga menimbulkan tantangan baru terkait penerapan etika dalam penggunaan dan pengelolaan teknologi. Oleh karena itu, memiliki etika dunia maya sangat penting ketika terlibat dalam aktivitas online. Salah satu masalah utama dalam etika siber adalah terjadinya perilaku manusia yang tidak sesuai dengan fungsinya. Lingkungan online menghadirkan tantangan hukum dan etika, termasuk peretasaan, pelecehan, pencurian, pembajakan, virus, plagiarism, dan informasi palsu. Etika dunia maya berhubungan dengan perilaku pengguna online. Perilaku pengguna di internet [7].

Ketergantungan masyarakat terhadap teknologi digital yang semakin tinggi memunculkan berbagai risiko etis. Masalah-masalah seperti penyalahgunaan data pribadi, serangan siber, dan penyebaran informasi palsu merupakan tantangan utama yang dapat mengancam keamanan dan stabilitas di ruang digital. Untuk dipastikannya bahwa teknologi dapat digunakan dengan tanggung jawab dan tidak menimbulkan dampak yang merugikan bagi orang atau masyarakat, sangat penting untuk memahami isu-isu moral, sosial, dan hukum yang melingkupi penggunaan dan pengembangan teknologi di zaman sekarang [8].

Jurnal ini bertujuan untuk mengkaji pentingnya cyber ethics di era digital serta tantangan yang ada dalam implementasinya. Artikel ini juga akan mengulas beberapa pendekatan untuk mendorong penerapan teknologi secara etis dan bertanggung jawab, baik di tingkat individu maupun organisasi.

2. METODE

Dalam penelitian ini, metode deskriptif kualitatif digunakan. 'Pentingnya Etika Siber pada Era Digital' dibahas dalam jurnal ini. Melalui sejumlah inisiatif untuk melindungi data pribadi, menjunjung tinggi hak asasi manusia secara online, dan mencegah kejahatan di ranah digital, hal ini menunjukkan pentingnya dunia maya di era modern.

3. HASIL DAN PEMBAHASAN

3.1 Etika Siber pada era Digital

Kejahatan yang terjadi di dunia siber sangat erat kaitannya dengan teknologi yang terutama jaringan telekomunikasi dan berbasis komputer. Teknologi ini dikategorikan ke dalam berbagai bentuk dalam praktik dan beberapa literatur, seperti:

1. Unauthorized Access to Computer System and Service

Kriminalitas dilakukan melalui akses atau pembobolan jaringan pada komputer secara ilegal. Hal ini biasa dilakukan oleh para peretas yang ingin mencuri atau menyabotase data sensitif dan penting. Di sisi lain, beberapa orang melakukannya hanya karena mereka merasa sulit untuk

menggunakan kemampuan mereka untuk membobol sistem yang sangat aman. Seiring dengan kemajuan teknologi internet/intranet, kejahatan ini menjadi lebih umum.

2. Ilegal Contents

Informasi atau data tentang sesuatu yang tidak senonoh, tidak bermoral, mengganggu ketertiban dan melanggar hukum yangtidak dapat diposting secara online. Contoh-contoh tersebut termasuk menyebarkan informasi palsu yang dapat menurunkan harga diri dan/atau martabat orang lain, masalah yang melibatkan pornografi atau memposting informasi rahasia negara, serta propaganda dan agitasi terhadap pemerintah yang sah.

3. Data Forgery

Kejahatan ini merupakan pemalsuan informasi pada berkas penting yang tersimpan secara online sebagai dokumen tidak tertulis. Dokumen e-commerce biasanya menjadi target kejahatan ini, yang memberikan kesan palsu bahwa ada "kesalahan ketik" yang dapat membantu kriminal.

4. Cyber Espionage

Digunakannya internet sebagai alat untuk memata-matai orang lain dengan cara membobol jaringan komputer target yang merupakan tindakan ilegal. Seperti, saingan bisnis yang memiliki catatan dan/atau informasi penting yang tersimpan dalam sistem komputer menjadi target kejahatan ini.

5. Cyber Sabotage and Extortion

Pelanggaran ini meliputi manipulasi, perubahan, atau penghancuran *software*, data, atau jaringan komputer yang terkoneksi pada internet. Kriminalitas ini dilakukan dengan cara memasukkan virus pada komputer, bom logika, atau suatu program untuk membuat data, *software*, atau tidak bisa digunakannya jaringan komputer, rusak, atau tidak berfungsi sesuai keinginan pelaku. Dengan imbalan tertentu, tentu saja, pelaku mungkin menawarkan bantuan untuk memulihkan data, perangkat lunak, atau sistem jaringan komputer yang telah disusupi. Terminologi umum yang digunakan untuk menggambarkan kejahatan ini adalah cyber-terrorist.

6. Offense against Intellectual Property

Hak kekayaan intelektual online milik orang lain adalah objek kejahatan ini. Penggandaan situs web orang lain secara tidak sah, contohnya adalah penyebaran informasi di internet yang ternyata merupakan rahasia bisnis orang lain.

7. Infringements of Privacy

Kejahatan ini berfokus pada data yang sangat pribadi dan sensitif dari seseorang. Kejahatan ini sering kali menargetkan data pribadi yang terkomputerisasi, diantaranya: PIN adan/atau nomor ATM dan Kartu Kredit, penyakit atau disabilitas tertutup, dan informasi lain yang, jika diketahui orang lain, dapat menyebabkan korban mengalami kerugian material atau imaterial [9].

3.2 Peran Penting Etika Siber di Era Digital

Privasi data, keamanan, dan kejahatan siber berkaitan erat dengan tantangan hubungan teknologi dengan etika dan moral. Etika memainkan peran penting dalam mengendalikan penggunaan teknologi dan penanganan serta perlindungan data dengan:

1. Penggunaan teknologi harus dipandu oleh etika untuk mengurangi dampak buruk pada keamanan dan privasi data. Dalam hal teknologi, etika mencakup prinsip dan panduan yang harus diikuti untuk melindungi privasi dan keamanan orang. Nilai melindungi informasi pribadi dan menjunjung tinggi privasi individu ditekankan oleh etika. Informasi pribadi harus ditangani

dengan bermartabat dan hanya digunakan untuk tujuan yang tepat, sesuai dengan norma-norma etika.

2. Privasi dan keamanan data mencakup perlindungan data. Informasi dikelola, diproses, dibagikan, disimpan, dan digunakan dengan bantuan perlindungan data. Dengan demikian, perlindungan dan privasi data tidak hanya penting, tetapi juga penting untuk pengabdian agama, kebebasan politik, dan bahkan kegiatan sehari-hari. Etika menekankan betapa pentingnya melindungi data dan menghentikan akses ilegal. Hal ini termasuk kewajiban moral untuk menjaga kerahasiaan data dan informasi sensitif. Teknologi seperti firewall, enkripsi, dan pemantauan keamanan digunakan untuk menciptakan sistem keamanan data. Sebagai hasil dari etika keamanan, solusi yang bisa melindungi data dari pelanggaran serangan dan keamanan siber dikembangkan.
3. Untuk mencegah kejahatan siber dan menjaga keamanan serta privasi data, pengetahuan tentang keamanan siber sangatlah penting. Pengetahuan ini dapat membantu orang dalam menggunakan teknologi secara bijaksana dan lebih memahami kelebihan dan kekurangannya. Kejahatan siber dipandang oleh etika sebagai tindakan yang melanggar hukum dan tidak bermoral. Peretasan, pencurian data, dan penipuan online adalah contoh serangan siber yang bertentangan dengan norma-norma etika yang menghargai kejujuran dan rasa hormat. Memanfaatkan Teknologi untuk Memerangi Kejahatan Siber: Kejahatan siber dideteksi, dihentikan, dan ditangani oleh teknologi. Etika mengharuskan teknologi ini digunakan untuk mempertahankan diri dari serangan siber dengan menggunakan prinsip-prinsip etika, seperti melindungi privasi dan hak-hak individu.
4. Modernisasi yang dibawa oleh kemajuan teknologi informasi, khususnya media sosial, dapat menyebabkan penurunan moral pada era digital. Hal ini bisa menurunkan pemahaman masyarakat akan moralitas dan etika saat menggunakan teknologi [10].

3.3 Penanggulangan dan Pemberantasan *Cybercrime*

1. Penanggulangan *Cybercrime*

Pencegahan kejahatan siber melalui penerapan hukum pidana berada di bawah domain kebijakan kriminal. Dari sudut pandang kebijakan kriminal, upaya pencegahan kejahatan, termasuk kejahatan siber, memerlukan pendekatan sistematis daripada hanya mengandalkan penerapan hukum pidana.

a) Dalam KUHP

KUHP masih menggunakan definisi tindak pidana yang sangat tradisional, yang tidak ada hubungannya dengan munculnya kejahatan siber. Selain itu, ada sejumlah kekurangan dan pembatasan dalam menangani kemajuan teknologi dan kejahatan berteknologi tinggi. Misalnya, karena tidak ada peraturan khusus yang berkaitan dengan penipuan kartu kredit atau transfer uang elektronik, KUHP kesusahan untuk mengatasi masalah ini. Pasal-pasal yang ada saat ini hanya membahas: a) sumpah/pernyataan palsu (Pasal 242); b) menghindari mata uang (Pasal 244-252); c) manipulasi stempel dan tanda (Pasal 253-262); dan d) manipulasi surat (Pasal263-276).

b) Luar KUHP:

1. UU No. 36 Tahun 1999 tentang Telekomunikasi menghukum kejahatan terhadap: a) mengendalikan akses ke jaringan telekomunikasi (Pasal 50 jo. Pasal 22); b) mengganggu secara fisik atau elektromagnetik terhadap penyelenggaraan telekomunikasi (Pasal 55 jo. Pasal 38);

dan c) melakukan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi (Pasal 56 jo. Pasal 40);

2. Undang-Undang No. 20 Tahun 2001 Pasal 26A tentang Perubahan atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, Undang-Undang No. 15 Tahun 2002 Pasal 38 tentang Tindak Pidana Pencucian Uang, dan Undang-Undang No. 30 Tahun 2002 Pasal 44 ayat (2) tentang Komisi Pemberantasan Tindak Pidana Korupsi, semuanya mengakui catatan elektronik sebagai alat bukti yang sah;

c) Undang-undang No. 32 Tahun 2022

UU No. 32 Tahun 2002 tentang Penyiaran mencantumkan beberapa tindak pidana sebagai berikut: 1) Pasal 57 jo. Pasal 36 ayat (5) melarang siaran yang: a) bersifat fitnah, menghasut, menyesatkan, atau bohong; b) menonjolkan unsur kekerasan, perjudian, penyalahgunaan narkotika dan obat terlarang; atau c) mempertentangkan suku, agama, ras, dan antargolongan (SARA). 2) Pasal 57 jo. Pasal 36 ayat (6) melarang siaran yang menghina, merendahkan, melecehkan, atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional; 3) Pasal 58 jo. Pasal 46 ayat (3) melarang siaran iklan niaga yang memuat: a) iklan ajaran agama, ideologi, perseorangan, atau kelompok yang menyinggung atau merendahkan perasaan orang lain, ideologi, perseorangan, atau kelompok lain; b) iklan minuman keras dan sejenisnya, serta zat atau bahan yang bersifat adiktif; c) iklan rokok yang menggambarkan bentuk rokok; d) muatan yang bertentangan dengan kesusilaan dan nilai-nilai agama; atau e) eksploitasi anak di bawah umur.

d) Undang-undang No. 11 Tahun 2008

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU-ITE) menjabarkan hukuman pidana bagi siapa pun yang dengan sengaja menyebarkan, mentransmisikan, atau memudahkan akses terhadap informasi atau dokumen elektronik yang memiliki bobot yang tidak memiliki pembenaran atau otorisasi yang sah. 1) Konten yang melanggar kesusilaan, mengandung perjudian, penghinaan atau pencemaran nama baik, atau mengandung ancaman atau pemerasan (Pasal 27); 2) Menyebarkan informasi palsu dan menipu yang menyebabkan konsumen merugi ketika melakukan pembelian secara online; menyebarkan informasi dengan tujuan menimbulkan rasa permusuhan atau kebencian seseorang atau kelompok masyarakat berdasarkan suku, agama, etnis, dan antargolongan (SARA) (Pasal 28); (Pasal 33) mencegat transmisi dokumen atau informasi elektronik yang bersifat rahasia; (Pasal 31) mencegat komunikasi elektronik atau mentransmisikan dokumen elektronik yang bersifat rahasia; Memproduksi, mengimpor, mendistribusikan, menyediakan, atau memiliki a) perangkat lunak atau perangkat keras yang secara khusus dibuat atau dirancang untuk memungkinkan perbuatan yang tercantum dalam Pasal 27-33; b) password, *access code*, atau yang serupa yang dimaksudkan untuk memungkinkan sistem elektronik untuk memungkinkan perbuatan yang tercantum dalam Pasal 27-33 (Pasal 34); 8) Membuat, mengubah, menghapus, dan merusak dokumen atau informasi elektronik agar terlihat seperti data yang autentik (Pasal 35); 9) Terlibat dalam perbuatan yang menyebabkan kerugian bagi orang lain yang melanggar Pasal 27-34; 10) Terlibat dalam kegiatan yang terlarang seperti didefinisikan dalam Pasal 27-36 pada sistem elektronik yang ada dalam yurisdiksi Indonesia (Pasal 37); 11) Terlibat dalam kegiatan yang terlarang seperti ditetapkan dalam Pasal 27-36 di dalam yurisdiksi Indonesia (Pasal 38).

2. Pemberantasan *Cybercrime*

Upaya komprehensif diperlukan untuk memerangi kejahatan dunia maya. Pendekatan terpadu antara kebijakan penal dan non-penal digunakan untuk mencegah dan mengendalikan kejahatan. Kebijakan penal memiliki sejumlah kelemahan, termasuk terfragmentasi, individualistis, lebih menindas, dan membutuhkan infrastruktur yang mahal. Oleh karena itu, kebijakan non-penal yang bersifat preventif merupakan cara yang lebih baik untuk mencegah kejahatan. Ada dua cara kebijakan yang dapat diterapkan untuk memerangi kejahatan dunia maya, yaitu:

a. kebijakan penal
b. kebijakan non penal

Kebijakan yang berkaitan dengan penerapan hukuman pidana ketika melakukan penyelesaian pada kasus kejahatan siber dikenal sebagai kebijakan penal. Beberapa metode berikut ini dapat digunakan untuk menerapkan kebijakan penal:

a) Membuat suatu tindakan menjadi ilegal di dunia maya dengan menjadikannya sebagai kejahatan menurut hukum.
b) Untuk memerangi kejahatan siber, ketentuan hukum nasional dan internasional harus diselaraskan.
c) Penegakan hukum dengan menegakkan hukuman pidana terhadap mereka yang melakukan kejahatan siber.

Untuk memerangi kejahatan siber secara efektif, politik hukum pidana harus diimbangi dengan langkah-langkah non-penal. Berikut ini adalah contoh-contoh kebijakan non-penal yang dapat diterapkan:

a) Membuat peraturan di luar hukum yang membantu pencegahan kejahatan siber, seperti yang berkaitan dengan ujaran kebencian, perundungan, dan promosi praktik internet yang aman di sekolah.
b) Mengedukasi pengguna internet untuk menghindari pengungkapan informasi pribadi, bertransaksi di lokasi yang memiliki akses internet yang aman, dan langkah-langkah lain untuk mencegah potensi kejahatan di dunia maya.
c) Untuk menciptakan sistem keamanan siber, berkolaborasilah dengan sektor swasta.

Membangun jaringan institusi untuk mencegah kejahatan siber pada skala nasional dan dunia. Mengingat bahwa kejahatan siber adalah kejahatan trans nasional yang terorganisir, kerja sama internasional sangat penting untuk memeranginya [11].

4. KESIMPULAN

Di era digital, kemajuan teknologi telah sangat memengaruhi kehidupan manusia, terutama dalam hal komunikasi, pendidikan, dan bisnis. Namun, tantangan etis seperti penyalahgunaan data pribadi, serangan siber, penyebaran informasi palsu, dan pelanggaran privasi terkait dengan hal ini membuat penerapan etika siber sangat penting untuk menjaga keamanan dan kestabilan di internet.

Ini menunjukkan bahwa etika siber memengaruhi bagaimana pengguna internet berperilaku dengan lebih bertanggung jawab, melindungi privasi dan data pribadi, dan mencegah pelanggaran seperti peretasan, sabotase, dan penipuan. Selain itu, untuk memerangi

kejahatan siber, kebijakan kriminal, pendidikan literasi digital, dan kerja sama internasional diperlukan.

Selain itu, etika siber memberikan pedoman moral bagi individu dan organisasi untuk menggunakan teknologi dengan bijak, mendukung perlindungan data, dan mendorong penggunaan teknologi untuk tujuan positif. Dengan demikian, penerapan etika siber yang baik akan menghasilkan lingkungan digital yang lebih aman dan etis bagi semua pihak.

REFERENSI

[1] D. N. Sari *et al.*, "Etika Dalam Penggunaan Media Informasi," *JIKMAS (Jurnal Pengabdi. dan Pemberdaya. Masy. Desa)*, vol. 1, no. 1, pp. 14–17, 2023,
[2] D. M. Sueni and I. N. B. A. Putra, "Pentingnya Etika Komunikasi Di Era Siber," *Maha Widya Duta*, vol. 6, no. 2, pp. 131–140, 2022.
[3] A. Gani, "Sejarah dan Perkembangan Internet Di Indonesia," *J. Mitra Manaj.*, vol. 5, no. 2, pp. 68–71, 2020.
[4] A. A. Burhanudin, "Peran Etika Profesi Hukum Sebagai Upaya Penegakan Hukum Yang Baik," *J. El-Faqih*, vol. 4, no. 2, pp. 50–66, 2018.
[5] A. Romadhona Widodo, F. Salsabila, A. Fitria, R. Khoirunnisa, and S. M. Nuraini, "Pengaruh Pendidikan Etika Siber pada Anak Usia Usia Dini dalam Keluarga," *J. Educ. Technol.*, vol. 1, no. 01, pp. 43–47, 2021, [
[6] R. Trisudarmo, D. P. Wati, and D. Irawan, "Peningkatan Kesadaran Dan Penerapan Etika Digital Di Kalangan Pengguna Internet," *J. PASOPATI - Vol. 5, No. 3 Tahun 2023*, vol. 5, no. 3, pp. 117–124, 2023.
[7] L. S. Salsabil, "Perkembangan Etika Siber Dan Pengaturan Cyberlaw Di Indonesia," *Dialekt. KOMUNIKA J. Kaji. Komun. dan Pembang. Drh.*, vol. 9, no. 1, 2021
[8] M. I. Djamzuri and A. P. Mulyana, "Fenomena Netflix Platform Premium Video Streaming Membangun Kesadaran Cyber Etik Dalam Perspektif Ilmu Komunikasi," *JISIP (Jurnal Ilmu Sos. dan Pendidikan)*, vol. 6, no. 1, pp. 2247–2254, 2022, doi: 10.58258/jisip.v6i1.2804.
[9] D. A. Arifah, "Kasus Cybercrime di Indonesia," *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.
[10] N. S. Dinarti, S. R. Salsabila, Y. Tri, S. Rizkya Salsabila, and Y. T. Herlambang, "Dilema Etika dan Moral dalam Era Digital: Pendekatan Aksiologi Teknologi terhadap Privasi Keamanan, dan Kejahatan Siber," *J. Pendidik. Ilmu Ilmu Sos. dan Hum.*, vol. 2, no. 1, pp. 8–16, 2024, doi: 10.26418/jdn.v2i1.74931.
[11] Z. Kasim, "Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia," *Indragiri Law Rev.*, vol. 2, no. 1, pp. 19–24, 2023.