VISA: Journal of Visions and Ideas
Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

Penerapan Etika Profesi di Bidang Keamanan Cyber untuk Mencegah Kejahatan Dunia Maya

Aan Nur Idzhand[1], Alif Irfan Harahap[2], T. Raihan Yudisthira[3], Amiruddin[4]
[123]Program Studi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara
[4]Universitas Muhammadiyah Sumatera Utara
idzhandaannur@gmail.com[1]

ABSTRACT

Cybercrime is currently attracting worldwide attention as a type of international crime. Cybercrime via the Internet is a new type of cybercrime that has emerged as a result of advances in internet technology. This research uses qualitative methodology, which is related to the meaning, concepts, definitions, attributes, metaphors, symbols and descriptions of an object. The research results show that cyber security has an important role in improving information network security. Cybercrime and data privacy and security are closely related fields where ethics and technology interact. When using technology, ethics serves as a guide to reduce adverse impacts on data security and privacy. Data security and privacy go hand in hand with data protection. To prevent cybercrime and maintain data security and privacy, cyber security knowledge is essential. Data security for privacy is not only important, it is also essential for political, spiritual, religious and even freedom of expression. Ethics places great emphasis on protecting data security and blocking genuine, unauthorized access.
Keywords*: ethics, cyber security, cyber crime*

ABSTRAK

Kejahatan dunia maya saat ini menarik perhatian seluruh dunia sebagai salah satu jenis kejahatan internasional. Kejahatan dunia maya melalui internet merupakan jenis kejahatan dunia maya baru yang muncul sebagai akibat dari kemajuan teknologi internet. Penelitian ini menggunakan metodologi kualitatif, yang berkaitan dengan makna, konsep, definisi, atribut, metafora, simbol, dan deskripsi suatu objek. Hasil penelitian menunjukkan bahwa keamanan siber mempunyai peran penting dalam meningkatkan keamanan jaringan informasi. Kejahatan dunia maya dan privasi serta keamanan data merupakan bidang yang terkait erat di mana etika dan teknologi berinteraksi. Saat menggunakan teknologi, etika berfungsi sebagai panduan untuk mengurangi dampak buruk terhadap keamanan data dan privasi. Keamanan dan privasi data berjalan seiring dengan perlindungan data. Untuk mencegah kejahatan dunia maya dan menjaga keamanan dan privasi data, pengetahuan keamanan siber sangatlah penting. Keamanan data untuk privasi tidak hanya penting, tetapi juga penting untuk kebebasan politik, spiritual, agama, dan bahkan berekspresi. Etika sangat menekankan pada perlindungan keamanan data dan pemblokiran akses asli yang tidak sah.
Kata kunci: etika, keamanan cyber, kejahatan dunia maya

PENDAHULUAN

Saat ini, banyak negara menghubungkan data mereka dan memiliki manajemen *online* atau berbasis internet di banyak industri. Saat ini belum ada kategorisasi atau istilah yang disepakati untuk terorisme siber-Siberia karena terdapat begitu banyak jenis terorisme yang berbeda. Di sisi lain, kejahatan dunia

Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

maya saat ini menarik perhatian seluruh dunia sebagai salah satu jenis kejahatan internasional (Herdiana et al., 2021). Kejahatan dunia maya melalui internet merupakan jenis kejahatan dunia maya baru yang muncul sebagai akibat dari kemajuan teknologi internet. Di Indonesia, sejumlah kejahatan *cybercrime* bermunculan, antara lain pencurian kartu kredit, peretasan situs *web*, manipulasi data dengan memasang perintah yang tidak diinginkan pada komputer pemrograman, dan penyadapan transfer data orang lain (seperti email). Kejahatan dunia maya telah berkembang menjadi ancaman terhadap stabilitas, sehingga menyulitkan pemerintah untuk mencapai keseimbangan antara kejahatan komputer dan teknologi, khususnya yang berkaitan dengan jaringan internet dan intranet (Irawati et al., 2021).

Komunikasi digital juga memerlukan etika, sehingga tidak hanya komunikasi langsung saja yang membutuhkannya. Seperangkat pedoman yang dikenal sebagai "etika digital" dikembangkan untuk mengurangi dampak buruk yang timbul akibat penggunaan teknologi digital. Menjaga kemudahan yang didapat dari penggunaan teknologi digital adalah tujuan dari pembentukan etika digital (Zakariah, 2022).

Untuk berinteraksi dengan orang lain dan lingkungannya, seseorang atau sekelompok individu, organisasi, atau komunitas harus menghasilkan dan menggunakan informasi melalui proses komunikasi. Komunikasi digital juga memerlukan etika, sehingga tidak hanya komunikasi langsung saja yang membutuhkannya. Seperangkat pedoman dan praktik yang dikenal sebagai "etika digital" dikembangkan untuk mengurangi dampak buruk penggunaan komunikasi digital. Oleh karena itu, kemampuan mewujudkan, mencontohkan, mengadaptasi, merasionalisasi, mempertimbangkan, dan membangun “tata kelola etis digital” dalam kehidupan sehari-hari itulah yang dimaksud dengan etika digital (Himawan et al., 2022).

Karena semakin banyak orang yang menggunakan komputer desktop, laptop, ponsel pintar, *server*, dan jaringan komputer seperti internet dalam kehidupan sehari-hari, keamanan siber semakin populer. Menurut BSSN (Badan Siber dan Sandi Negara), terdapat sekitar 190 juta upaya serangan siber di Indonesia antara Januari dan Agustus tahun lalu. Jumlah ini meningkat empat kali lipat dibandingkan tahun sebelumnya, atau sekitar 39 juta upaya, berdasarkan jangka waktu tahun 2019. Sejumlah situs juga memperkirakan pada tahun 2021 masih akan terjadi serangan siber (Putri et al., 2023).

Berdasarkan latar belakang yang telah dipaparkan diatas, maka tujuan penelitian ini adalah untuk mengetahui bagaimana peran keamaanan siber di dalam dunia maya dan apa dampak dari penggunaan keamanan siber terhadap pencegahan kejahatan di unia maya.

METODE PENELITIAN

Penelitian ini menggunakan metodologi kualitatif, yang berkaitan dengan makna, konsep, definisi, atribut, metafora, simbol, dan deskripsi suatu objek. Pendekatan kualitatif dan deskriptif analitis digunakan dalam metodologi penelitian,

VISA: Journal of Visions and Ideas
Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

dan data sekunder serta tinjauan literatur dari penelitian sebelumnya digunakan sebagai metode pengumpulan data.

Untuk menemukan solusi, penelitian kualitatif melihat konteks sosial yang berbeda, serta kelompok atau orang dalam suatu sistem sosial. Dalam hal ini, simbol, ritual, struktur sosial, peran sosial, dan elemen lainnya digunakan oleh peneliti kualitatif untuk memahami *setting* yang diteliti. Di sini, peneliti dapat menyelidiki bagaimana individu mengatur dan memberikan makna pada kehidupan sehari-hari dan berpartisipasi dalam pemahaman dan persepsi orang lain melalui penggunaan pendekatan kualitatif.

HASIL DAN PEMBAHASAN

Kejahatan dunia maya menjadi ancaman yang lebih nyata dan signifikan bagi masyarakat dan perusahaan di era digital ini. Serangan yang dilakukan oleh penjahat dunia maya dapat sangat membahayakan stabilitas sistem, kepercayaan, serta keamanan dan privasi data. Seseorang yang mahir menggunakan media sosial dapat memperoleh beberapa manfaat yang akan meningkatkan kualitas hidupnya, antara lain kemampuan menjalin persahabatan, belajar lebih mudah, mempermudah pembelian, dan banyak keuntungan lainnya. Di sisi lain, ketika seseorang menyalah gunakan media sosial, mereka kehilangan hal-hal seperti koneksi, pengungkapan privasi, dan reaksi negatif dari pengguna lain.

Gambar 1. Aspek-aspek etika digital.

Karena meluasnya penggunaan komputer canggih dan bidang informatika dengan media utamanya adalah komputer dan internet, kejahatan dunia maya dapat dipahami sebagai jenis kejahatan yang dapat menimbulkan banyak kerugian jika tidak ditangani dengan tepat. Tindakan ini melibatkan penyalahgunaan dan penyalahgunaan teknologi digital secara cepat, yang mudah diakses dan disalahgunakan untuk tujuan yang merugikan banyak orang. Pornografi, penipuan

Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

telepon atau SMS, pencurian identitas, penipuan kartu kredit atau pinjaman *online*, dan masih banyak lagi pelanggaran merupakan contoh kejahatan. Dilema hubungan kejahatan dunia maya, privasi, dan keamanan data semuanya berkaitan erat dengan etika dan moralitas. Menurut Dinarti (2024) etika juga berperan penting dalam mengatur penggunaan teknologi serta pemrosesan dan pemeliharaan data. khususnya:

1) menggunakan etika sebagai pedoman dalam menggunakan teknologi untuk mengurangi dampak buruk terhadap keamanan data dan privasi. Etika mencakup standar dan prinsip yang harus diikuti saat menggunakan teknologi untuk melindungi keamanan dan privasi masyarakat, baik secara individu maupun kolektif. Etika menekankan betapa pentingnya menjaga informasi pribadi dan menghormati privasi individu. Informasi pribadi harus ditangani dengan hati-hati dan hanya digunakan untuk alasan yang sah, sesuai dengan norma etika.
2) Keamanan dan privasi data bersama-sama mencakup perlindungan data. Fitur perlindungan data mencakup manajemen informasi, pemrosesan, berbagi, penyimpanan, dan penggunaan. Oleh karena itu, keamanan data untuk privasi tidak hanya penting, tetapi juga penting untuk kebebasan politik, spiritual, agama, dan bahkan berekspresi. Etika sangat menekankan pada perlindungan keamanan data dan pemblokiran akses asli yang tidak sah. Hal ini termasuk memiliki kewajiban etis untuk melindungi data pribadi dan informasi sensitif. Solusi keamanan data, seperti *firewall*, enkripsi, dan pemantauan keamanan, dikembangkan menggunakan teknologi. Teknologi yang dapat melindungi data dari serangan siber dan pelanggaran keamanan dikembangkan sebagai hasil dari etika keamanan.
3) Kesadaran untuk menghentikan kejahatan dunia maya dan menjaga keamanan dan privasi data, keamanan siber sangatlah penting. Hal ini dapat meningkatkan pemahaman masyarakat mengenai kelebihan dan kekurangan teknologi serta mendorong penggunaan teknologi secara bertanggung jawab. Etika yang menangani tindakan kejahatan dunia maya sebagai tindakan yang melanggar hukum dan tidak bermoral. Peretasan, pencurian data, dan penipuan *online* adalah contoh serangan siber yang melanggar standar etika yang mengutamakan kejujuran dan rasa hormat.
4) Di era digital, kerusakan moral mungkin diakibatkan oleh kemajuan teknologi informasi modern, khususnya di bidang media sosial. Permasalahan ini dapat menyebabkan menurunnya kesadaran moral dan etika dalam menggunakan teknologi.

VISA: Journal of Visions and Ideas
Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

Gambar 3. Etika dalam media social.

Tantangan dan Strategi Keamanan *Cyber*

a. Perkembangan Teknologi
   Kemajuan teknologi yang pesat menghadirkan tantangan baru bagi keamanan siber. Menghadirkan keamanan siber dengan kesulitan baru. Penyerang mungkin bias memanfaatkan kerentanan tambahan jika semakin banyak perangkat yang *online* untuk mengambil keuntungan dari kerentanan tambahan semakin banyak perangkat yang *online*. Selain itu, peretas dapat melakukan lebih banyak serangan-serangan yang rumit dan canggih dengan memanfaatkan teknologi seperti komputasi awan dan kecerdasan buatan .dengan memanfaatkan teknologi seperti komputasi awan dan kecerdasan buatan.
b. Serangan dari Berbagai Belahan Pihak
   Serangan siber dilakukan telah membawa oleh negara atau kelompok terorganisir selain orang atau kelompok tertentu .dikeluarkan oleh negara atau kelompok terorganisir selain orang atau kelompok tertentu. Serangan mungkin terwujud seperti sabotase, pencurian data, atau bahkan pencurian data, serangan siber bahkan serangan siber yang mempunyai kekuatan untuk menghancurkan infrastruktur vital suatu negara .yang memiliki kekuatan untuk menghancurkan infrastruktur vital suatu negara. Kompleksitas-kompleksitas sistem pengamanan dan data meningkat seiring dengan frekuensi dan intensitas serangan .dari sistem pengamanan dan data meningkat seiring dengan frekuensi dan intensitas serangan.
c. Kekurangan Pakar Keamanan *Cyber*
   Salah satu masalah utamanya adalah kurangnya spesialis keamanan siber. Terdapat kebutuhan yang jauh lebih besar akan spesialis keamanan siber yang kompeten dibandingkan jumlah spesialis yang tersedia. Hal ini

Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

mengakibatkan hilangnya keamanan dan membatasi kapasitas organisasi untuk melawan dan mencegah serangan.

d. Sosial Teknik Serangan
   Taktik media sosial sering digunakan oleh penyerang dalam serangannya. Mereka memanfaatkan kecerdasan emosional, kecerobohan, atau ketidaktahuan korban untuk mendapatkan data pribadi atau akses yang tidak disetujui. *Phishing*, *spear phishing*, dan rekayasa sosial adalah teknik yang paling sering digunakan oleh penyerang.
e. Kelemahan Sistem dan Aplikasi
   Penyerang sering kali memanfaatkan kelemahan sistem operasi, perangkat lunak, atau aplikasi. Perangkat lunak yang tidak diperbarui secara berkala atau kerentanan yang tidak terdeteksi dapat menjadi titik masuk serangan siber.
f. Keberlanjutan Ancaman
   Ancaman terhadap keamanan siber terus terjadi. Penyerang tidak pernah berhenti menemukan cara baru untuk menghindari deteksi dan melemahkan pertahanan. Untuk menjaga keamanan sistem dan data, ancaman dinamis harus diatasi dengan cepat dan adaptif.

Mengembangkan Keamanan Siber yang Aktif

Penilaian risiko adalah salah satu langkah pertama dalam menciptakan rencana keamanan siber yang sukses. Tergantung pada jenis data yang mereka miliki dan seberapa penting data tersebut, setiap perusahaan menghadapi bahaya yang berbeda-beda. Organisasi harus mengembangkan daftar risiko yang mungkin terjadi dan memperkirakan sejauh mana risiko tersebut dapat mempengaruhi bisnis mereka sebelum melakukan tinjauan risiko. Organisasi mungkin menemukan celah dalam sistem keamanan mereka dan mengambil tindakan proaktif untuk melindungi data mereka dengan mewaspadai ancaman yang mereka hadapi.

Tahap berikutnya adalah meningkatkan keamanan jaringan dan sistem dalam menciptakan rencana keamanan siber yang sukses. Berinvestasi dalam solusi keamanan mutakhir, seperti *firewall* yang kuat, pemantauan jaringan berkelanjutan, dan aplikasi keamanan yang dapat mengidentifikasi aktivitas mencurigakan, dapat membantu mencapai hal ini. Organisasi juga harus melibatkan anggota stafnya dalam inisiatif keamanan siber. Serangan siber dapat dihindari dengan mengajari anggota staf tentang prosedur keamanan yang aman, seperti membuat kata sandi yang kuat dan menghindari membaca *email* atau lampiran yang meragukan (Laksana & Mulyani, 2024).

Karena banyak negara kini menghubungkan data dan kendali mereka atas beberapa sektor melalui internet atau *online*, kejahatan dunia maya dapat mengganggu dan membahayakan keamanan nasional suatu negara. Karena ada begitu banyak jenis kejahatan dunia maya yang mungkin terjadi secara *online*, istilah ini belum memiliki klasifikasi atau arti yang jelas. Salah satu negara dengan penggunaan internet yang sangat tinggi adalah Indonesia. Hal ini ditunjukkan oleh penelitian yang dilakukan pada tahun 2019 bekerja sama dengan Asosiasi

Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

Penyelenggara Jasa Internet Indonesia (APJII), yang menemukan bahwa dari total 264 juta penduduk Indonesia, 171,17 juta, atau 64,8%, memiliki akses internet. Karena meluasnya penggunaan internet oleh masyarakat. internet, terdapat risiko kejahatan dunia maya yang signifikan (Rosy, 2020).

KESIMPULAN

Berdasarkan hasil penelitian maka dapat disimpulkan bahwa keamanan siber mempunyai peran penting dalam meningkatkan keamanan jaringan informasi. Kejahatan dunia maya dan privasi serta keamanan data merupakan bidang yang terkait erat di mana etika dan teknologi berinteraksi. Saat menggunakan teknologi, etika berfungsi sebagai panduan untuk mengurangi dampak buruk terhadap keamanan data dan privasi. Keamanan dan privasi data berjalan seiring dengan perlindungan data. Untuk mencegah kejahatan dunia maya dan menjaga keamanan dan privasi data, pengetahuan keamanan siber sangatlah penting. Pemahaman etika dan moralitas dalam penggunaan teknologi mungkin akan tergerus oleh kemerosotan moral di era digital. Oleh karena itu, sangat penting untuk melindungi privasi kita saat *online* dan memanfaatkan media sosial dengan cara yang etis. Saat menjalani kehidupan sehari-hari, kita harus mengingat bagaimana teknologi mempengaruhi masyarakat dan lingkungan. Kita juga harus memastikan bahwa teknologi bermanfaat bagi masyarakat secara keseluruhan dan tidak menimbulkan kesenjangan.

Vol 4 No 3 (2024) 1792–1799 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v4i3.3482

DAFTAR PUSTAKA

Dinarti, N. S., Salsabila, S. R., & Herlambang, Y. T. (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*(1), 8-16.

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *21*(1), 42-52.

Himawan, I. S., Wahyuni, S., Hamidin, D., Andriani, A. D., Meidelfi, D., & Khairunisa, Y. (2022). *Etika Profesi Teknologi Informasi Dan Komunikasi*. TOHAR MEDIA.

Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021, August). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin*, *3*(01), 109-122.

Putri, E., Pratama, G. A., & Fithri, B. S. (2023). Keamanan Nasional dalam Menghadapi Perubahan Cyber Warfare. *JURNAL MERCATORIA*, *16*(2), 201-208.

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security. *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan*, *1*(2), 118-129.

Sephira, A., Abrar, MH, Angin, SLSP, & Hidayatullah, H. (2024). Analisis Keamanan Siber (Cyber Security) dalam Era Digital "Tantangan Dan Strategi Pengamanan". *Jurnal Ilmu Komputer Revolusioner* , *8* (2).

Zakaria, H. (2022). *Etika Profesi di Bidang Teknologi Informasi*. Pascal Books.