

Penjahat Dunia Maya: Studi Literatur Permasalahan Etika pada Teknologi Informasi

Adi Wijaya

Program Magister Teknik Informatika

Universitas Bina Darma

email : adiw1201@gmail.com

Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

This study aims to examine ethical issues arising from the development of information technology and cybersecurity, particularly within the context of cyberspace. A literature review approach was used to analyze various scholarly sources discussing cybercrime issues such as hacking, digital law violations, and information security threats. A comprehensive analysis was conducted to identify the root causes of ethical issues, their social implications, and possible mitigation strategies. The results indicate that the increase in cybercrime activity has significantly affected individual privacy, national security, and the stability of the digital economy. Therefore, a thorough understanding of information technology ethics, heightened cybersecurity awareness, and strengthened legal policies are crucial for building a safe and ethical digital ecosystem.

Kata kunci: *information technology, cyber security, cybercrime, technology ethics.*

Abstrak

Penelitian ini bertujuan untuk mengkaji permasalahan etika yang timbul akibat perkembangan teknologi informasi dan keamanan siber, khususnya dalam konteks dunia maya (cyberspace). Kajian ini menggunakan pendekatan studi literatur untuk menelaah berbagai sumber ilmiah yang membahas isu-isu kejahatan dunia maya (cybercrime), seperti peretasan, pelanggaran hukum digital, dan ancaman keamanan informasi. Analisis dilakukan secara komprehensif untuk memahami akar permasalahan etika, implikasi sosial, serta strategi penanggulangannya. Hasil kajian menunjukkan bahwa peningkatan aktivitas kejahatan dunia maya berdampak signifikan terhadap privasi individu, keamanan nasional, serta stabilitas ekonomi digital. Oleh karena itu, pemahaman mendalam mengenai etika teknologi informasi, kesadaran keamanan siber, dan penguatan kebijakan hukum menjadi aspek penting dalam membangun ekosistem digital yang aman dan beretika.

Kata kunci: *teknologi informasi, keamanan siber, kejahatan dunia maya, etika teknologi*

1. PENDAHULUAN

Perkembangan teknologi informasi (TI) yang begitu pesat dalam beberapa dekade terakhir telah membawa perubahan besar terhadap berbagai aspek kehidupan masyarakat. Teknologi digital kini menjadi tulang punggung hampir seluruh aktivitas manusia—mulai dari komunikasi, pendidikan, ekonomi, hingga pemerintahan. Dunia maya (*cyberspace*) memungkinkan terjadinya pertukaran informasi, kolaborasi lintas batas, dan transaksi bisnis secara instan tanpa dibatasi ruang maupun waktu. Transformasi ini menjadikan teknologi informasi sebagai motor penggerak utama menuju masyarakat berbasis pengetahuan (*knowledge society*) dan ekonomi digital. Namun, seiring dengan meningkatnya ketergantungan terhadap teknologi, muncul pula permasalahan baru yang berkaitan dengan tanggung jawab etika dan keamanan digital.

Kemajuan teknologi yang semula dimaksudkan untuk meningkatkan kesejahteraan manusia, pada kenyataannya juga menghadirkan ancaman baru dalam bentuk kejahatan dunia maya (*cybercrime*). Aktivitas kriminal ini memanfaatkan jaringan komputer, perangkat digital, dan internet sebagai sarana utama untuk melakukan tindakan melanggar hukum. Bentuk-bentuk cybercrime sangat beragam, mulai dari peretasan sistem (hacking), pencurian data pribadi, penyebaran malware dan virus, hingga penipuan digital seperti phishing dan online scam. Dampak yang ditimbulkan tidak hanya bersifat material, tetapi juga mengancam keamanan informasi, privasi individu, reputasi lembaga, dan bahkan kedaulatan data negara. Menurut Simarmata et al. (2022), maraknya kejahatan siber menunjukkan bahwa kemajuan teknologi tanpa disertai kesadaran etis justru berpotensi merusak tatanan sosial dan kepercayaan publik terhadap sistem digital.

Permasalahan etika dalam konteks dunia siber tidak dapat dipandang semata sebagai persoalan hukum, melainkan juga sebagai permasalahan moral dan perilaku manusia dalam menggunakan teknologi. Etika berkaitan dengan kemampuan individu untuk membedakan antara tindakan yang benar dan salah dalam konteks digital. Sayangnya, dalam era globalisasi informasi, nilai-nilai etika tradisional sering kali terpinggirkan oleh budaya instan dan anonimitas di internet. Kemudahan akses dan lemahnya regulasi memungkinkan seseorang untuk menyebarkan informasi palsu, mencuri data, atau melakukan peretasan tanpa rasa tanggung jawab. Kondisi ini memperkuat urgensi untuk menanamkan kesadaran etika informasi sejak dulu sebagai dasar pembentukan masyarakat digital yang beradab dan bertanggung jawab.

Selain faktor individu, aspek kelembagaan dan kebijakan publik juga berperan besar dalam menanggulangi kejahatan siber. Banyak organisasi dan lembaga pemerintah masih menghadapi tantangan dalam mengimplementasikan sistem keamanan informasi yang efektif. Kurangnya koordinasi antarinstansi, keterbatasan sumber daya manusia di bidang keamanan siber, serta kesenjangan literasi digital di masyarakat menyebabkan penegakan hukum terhadap kejahatan siber belum optimal. Hal ini menunjukkan bahwa pendekatan teknis semata tidak cukup untuk mengatasi kompleksitas masalah etika di dunia maya; diperlukan integrasi antara teknologi, regulasi, dan kesadaran moral.

Dalam perspektif global, kejahatan dunia maya kini dikategorikan sebagai ancaman lintas negara (*transnational crime*) yang menuntut kerja sama internasional. Negara-negara di dunia berlomba-lomba memperkuat kerangka hukum dan kebijakan keamanan siber untuk melindungi infrastruktur digital nasional. Indonesia sendiri telah memiliki regulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diperbarui dengan UU Nomor 19 Tahun 2016, namun implementasinya masih menghadapi tantangan dalam hal penegakan dan kesadaran hukum masyarakat. Oleh karena itu, pengembangan strategi

nasional yang mencakup aspek etika, pendidikan, dan perlindungan data pribadi menjadi sangat penting untuk memperkuat ketahanan siber nasional.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menelaah secara mendalam permasalahan etika yang muncul dalam perkembangan teknologi informasi, khususnya terkait kejahatan dunia maya (cybercrime), serta merumuskan langkah-langkah pencegahan, pengamanan, dan penegakan hukum yang relevan untuk menciptakan tata kelola dunia digital yang beretika dan berkeadilan. Kajian ini diharapkan dapat memberikan kontribusi terhadap penguatan literasi etika digital, pengembangan kebijakan keamanan informasi, serta peningkatan kesadaran masyarakat dalam memanfaatkan teknologi informasi secara bertanggung jawab. Dengan demikian, penelitian ini tidak hanya bersifat deskriptif, tetapi juga solutif dalam mendukung terciptanya ekosistem digital yang aman, etis, dan berkelanjutan.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode studi literatur (literature review) yang bersifat kualitatif. Pendekatan ini dipilih karena memberikan pemahaman mendalam terhadap berbagai hasil penelitian sebelumnya yang relevan dengan topik kejahatan dunia maya dan etika teknologi informasi.

2.1 Langkah- Langkah

1. Identifikasi Sumber DataPenelusuran dilakukan terhadap artikel jurnal, buku, dan laporan penelitian yang membahas isu kejahatan siber, keamanan informasi, dan etika teknologi. Hanya literatur yang relevan dan mutakhir (2019–2024) yang digunakan sebagai bahan kajian.
2. Seleksi dan Analisis LiteraturLiteratur yang diperoleh diseleksi berdasarkan relevansi, kualitas metodologi, serta kejelasan temuan penelitian. Analisis dilakukan untuk mengidentifikasi pola temuan dan isu-isu etika utama dalam teknologi informasi.
3. Integrasi dan Sintesis TemuanTemuan-literatur diintegrasikan untuk menghasilkan kerangka pemahaman komprehensif mengenai hubungan antara etika, kejahatan dunia maya, dan keamanan siber. Proses sintesis dilakukan secara tematik dengan menyoroti isu privasi, keamanan, dan tanggung jawab hukum.

3. HASIL DAN PEMBAHASAN

3.1 Karakteristik Dan Jenis Kejahatan Dunia Maya

Kejahatan dunia maya merupakan istilah umum yang mencakup berbagai aktivitas ilegal di internet, seperti peretasan (hacking), pornografi daring, pencurian identitas, penyebaran malware, dan penipuan digital (Nasution et al., 2023). Aktivitas ini dapat merugikan individu, lembaga, maupun negara secara ekonomi dan sosial.

Beberapa bentuk kejahatan dunia maya yang umum antara lain:

- Peretasan dan pelanggaran sistem keamanan komputer
- Penyebaran virus dan perangkat lunak berbahaya
- Pencurian data pribadi dan penipuan daring Kejahatan finansial digital seperti carding dan pencucian uang
- Kekerasan berbasis siber dan cyberbullying

Aktivitas tersebut menunjukkan bahwa ancaman digital semakin kompleks dan memerlukan pendekatan multidisipliner untuk penanganannya, mencakup aspek teknologi, hukum, dan etika.

3.2 Kesadaran dan Etika dalam Penggunaan Teknologi

Permasalahan etika dalam dunia siber berakar pada perilaku pengguna yang kurang memahami tanggung jawab moral terhadap penggunaan teknologi. Banyak kasus kejahatan bermula dari kelalaian individu dalam menjaga kerahasiaan data pribadi.

Rozi Sastra Purna et al. (2021) menjelaskan bahwa kecenderungan individu, khususnya perempuan, untuk mengungkapkan informasi pribadi secara terbuka di dunia maya meningkatkan risiko menjadi korban kejahatan siber. Oleh karena itu, pendidikan literasi digital menjadi salah satu strategi utama dalam mencegah terjadinya pelanggaran etika di dunia siber.

Kesadaran etis perlu dibangun melalui pendekatan edukatif dan kebijakan publik yang mendorong tanggung jawab pengguna. Hal ini mencakup etika berbagi informasi, perlindungan privasi, dan pemanfaatan teknologi untuk tujuan produktif.

3.3 Standar dan Kebijakan Keamanan Siber

Peningkatan ancaman kejahatan dunia maya menuntut penerapan standar keamanan siber yang kuat. Achmad Fauzi et al. (2023) menguraikan beberapa kerangka kerja internasional yang menjadi acuan, antara lain:

- ITU-T X.1205 (2008) – klasifikasi ancaman keamanan dan definisi keamanan siber.
- Kerangka Keamanan Siber NIST (Amerika Serikat) – panduan manajemen risiko keamanan siber berbasis standar dan praktik terbaik.
- Konvensi Budapest (Council of Europe) – instrumen hukum internasional untuk harmonisasi penanganan kejahatan siber.
- ISO/IEC 27032 dan 27103 – standar keamanan informasi global yang mengatur pencegahan dan mitigasi risiko siber.

Penerapan standar tersebut dapat memperkuat sistem perlindungan data, meningkatkan resiliensi organisasi, serta membangun kerja sama lintas negara dalam menghadapi ancaman digital.

3.4 Penegakan Hukum terhadap Kejahatan Dunia Maya

Penegakan hukum terhadap pelaku kejahatan dunia maya di Indonesia mengacu pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). Menurut Gede Wiradipa Ariawan (2002), undang-undang ini merupakan bentuk cyberlaw Indonesia yang mengatur berbagai pelanggaran di ruang digital.

Namun, efektivitas penegakan hukum masih menghadapi tantangan, seperti keterbatasan kapasitas aparat penegak hukum dan kesenjangan teknologi. Septia et al. (2023) menegaskan bahwa prinsip keadilan, proporsionalitas, serta kemampuan teknis aparat harus diperhatikan agar hukum tidak bersifat over-criminalization terhadap inovasi digital.

Pembahasan

Kejahatan dunia maya merupakan fenomena multidimensi yang tidak hanya berdampak pada aspek teknis, tetapi juga pada moral dan sosial. Perkembangan teknologi informasi memunculkan dilema etika baru, di mana kemudahan akses informasi sering kali disalahgunakan. Etika teknologi informasi menuntut tanggung jawab moral dalam penggunaan teknologi agar tidak merugikan orang lain. Kesadaran akan keamanan digital harus dimulai dari individu, disertai dengan kebijakan yang tegas dari lembaga pemerintah dan organisasi internasional.

Selain itu, sinergi antara aspek teknologi, hukum, dan pendidikan menjadi kunci utama dalam menanggulangi kejahatan siber. Pemanfaatan kecerdasan buatan (AI), sistem deteksi dini, dan pendekatan keamanan berbasis risiko dapat menjadi strategi preventif yang efektif.

4. KESIMPULAN

Perkembangan teknologi informasi membawa dampak positif sekaligus tantangan etika yang signifikan. Kejahatan dunia maya tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam keamanan nasional dan moralitas masyarakat digital.

Studi literatur ini menegaskan bahwa keamanan siber dan perlindungan data merupakan komponen penting dalam menjaga integritas dunia digital. Upaya preventif, edukatif, serta penegakan hukum yang adaptif terhadap perkembangan teknologi perlu terus diperkuat untuk menciptakan ruang siber yang aman dan beretika.

Referensi

- Achmad Fauzi, A., et al. (2023). Keamanan siber dan peretasan etis: Pentingnya melindungi data pengguna. *Jurnal Ilmu Multidisiplin*, 2(1), 36–41.
- Ariawan, G. W. (2002). Implementasi Undang-Undang tentang Informasi dan Teknologi Elektronik terkait penegakan hukum terhadap kejahatan dunia maya penyebaran berita bohong (Hoax) di Indonesia. 124–135.
- Fahrudin, E., Subariah, R., & Pamulang, U. (2024). Pentingnya memahami cybersecurity di era transformasi digital. *Jurnal Pendidikan dan Teknologi Informasi*, 2(1), 25–28.
- Nasution, D. A. F., Septiana, R., & Syaputri, W. (2023). Lingkup dunia cyber di Indonesia. *Comserva: Indonesian Journal of Community Service Development*, 2(11), 2477–2486.
- Purna, R. S. (2021). Pengungkapan diri di dunia maya dan kekerasan terhadap perempuan. *Kafa'ah: Jurnal Gender Studies*, 11(2), 159–169.
- Septia, R., Pansariadi, B., & Soekorini, N. (2023). Tindak pidana cybercrime dan penegakan hukumnya. *Jurnal Bhakti Hukum*, 12(2), 287–298.
- Simarmata, J., et al. (2022). Ancaman siber dan dampaknya terhadap pertahanan nasional. *Jurnal Keamanan Nasional*, 5(3), 55–67.