Jurnal Perkembangan Hukum dan Keadilan Berkelanjutan

https://ejurnals.com/ojs/index.php/jphkb Vol. 7, No. 1, Maret 2026

KEJAHATAN SIBER DAN DAMPAKNYA TERHADAP MASYARAKAT DIGITAL

Nabila Febrina[1], Hendriko Berni Richardo Katuuk[2], Alpiansyah[3], Ronny Mulya Perangin Angin[4], Titania Elvindry Jafri[5]

[1,2,3,4,5]Universitas Langlangbuana

mail@unla.ac.id

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah mendorong terbentuknya masyarakat digital yang semakin bergantung pada internet dalam berbagai aspek kehidupan. Namun, kemajuan tersebut juga diiringi dengan meningkatnya kejahatan siber sebagai bentuk kejahatan modern. Kejahatan siber mencakup berbagai tindakan ilegal seperti penipuan daring, pencurian data pribadi, peretasan sistem, penyebaran malware, hingga penyalahgunaan media digital. Penelitian ini bertujuan untuk mengkaji kejahatan siber serta dampaknya terhadap masyarakat digital, baik dari aspek sosial, ekonomi, maupun keamanan informasi. Metode penelitian yang digunakan adalah studi literatur dengan menganalisis berbagai sumber ilmiah, laporan resmi, dan regulasi terkait. Hasil kajian menunjukkan bahwa kejahatan siber tidak hanya menimbulkan kerugian finansial, tetapi juga menurunkan kepercayaan masyarakat terhadap teknologi digital, mengancam privasi individu, serta mengganggu stabilitas sistem informasi. Oleh karena itu, diperlukan upaya komprehensif melalui peningkatan literasi digital, penguatan sistem keamanan siber, serta penegakan hukum yang efektif guna meminimalkan dampak kejahatan siber di masyarakat digital.

Kata Kunci: Kejahatan Siber.

ABSTRACT

The development of information and communication technology has fostered a digital society that is increasingly reliant on the internet in various aspects of life. However, this progress has also been accompanied by an increase in cybercrime, a form of modern crime. Cybercrime encompasses various illegal acts such as online fraud, personal data theft, system hacking, malware distribution, and misuse of digital media. This study aims to examine cybercrime and its impact on the digital society, from a social, economic, and information security perspective. The research method used is a literature review, analyzing various scientific sources, official reports, and relevant regulations. The study results indicate that cybercrime not only causes financial losses but also undermines public trust in digital technology, threatens individual privacy, and disrupts the stability

of information systems. Therefore, comprehensive efforts are needed through increasing digital literacy, strengthening cybersecurity systems, and effective law enforcement to minimize the impact of cybercrime in the digital society.

Keywords: *Cyber Crime.*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam kehidupan masyarakat, terutama dengan terbentuknya masyarakat digital yang memanfaatkan internet dalam berbagai aktivitas, seperti komunikasi, transaksi ekonomi, pendidikan, dan pelayanan publik. Digitalisasi memberikan kemudahan serta efisiensi, namun di sisi lain juga membuka peluang munculnya berbagai bentuk kejahatan siber yang semakin kompleks dan sulit dikendalikan.

Kejahatan siber merupakan tindakan melanggar hukum yang dilakukan melalui atau terhadap sistem elektronik dan jaringan komputer. Bentuk kejahatan ini meliputi penipuan daring, pencurian identitas, peretasan sistem, penyebaran malware, hingga penyalahgunaan data pribadi. Meningkatnya ketergantungan masyarakat terhadap teknologi digital menjadikan kejahatan siber sebagai ancaman serius yang dapat berdampak luas, tidak hanya bagi individu, tetapi juga bagi organisasi dan stabilitas sosial.

Dampak kejahatan siber terhadap masyarakat digital sangat beragam, mulai dari kerugian ekonomi, gangguan keamanan informasi, hingga menurunnya kepercayaan publik terhadap penggunaan teknologi digital. Selain itu, kejahatan siber juga dapat menimbulkan dampak psikologis bagi korban, seperti rasa takut, trauma, dan ketidaknyamanan dalam beraktivitas di ruang digital. Kondisi ini menunjukkan bahwa kejahatan siber tidak lagi menjadi isu teknis semata, melainkan persoalan sosial yang memerlukan perhatian multidisipliner.

Meskipun berbagai regulasi dan upaya pengamanan telah diterapkan, tingkat kejahatan siber masih menunjukkan tren peningkatan seiring dengan pesatnya inovasi teknologi. Oleh karena itu, kajian mengenai kejahatan siber dan dampaknya terhadap masyarakat digital menjadi penting untuk memahami karakteristik kejahatan ini serta

merumuskan strategi pencegahan dan penanggulangan yang efektif. Penelitian ini diharapkan dapat memberikan kontribusi akademik serta menjadi bahan pertimbangan bagi pemangku kepentingan dalam menciptakan lingkungan digital yang aman dan berkelanjutan.

B. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan mengumpulkan dan menganalisis sumber-sumber ilmiah berupa jurnal nasional dan internasional, buku, laporan lembaga resmi, serta peraturan perundang-undangan yang berkaitan dengan kejahatan siber. Data yang diperoleh dianalisis secara deskriptif-kualitatif untuk menggambarkan bentuk dan dampak kejahatan siber terhadap masyarakat digital.

C. HASIL DAN PEMBAHASAN

1. Bentuk Kejahatan Siber dalam Masyarakat Digital

Dalam masyarakat digital, kejahatan siber berkembang seiring dengan kemajuan teknologi. Bentuk kejahatan yang sering terjadi antara lain penipuan daring, pencurian identitas, peretasan akun, dan penyebaran malware. Kejahatan tersebut memanfaatkan rendahnya kesadaran keamanan digital serta lemahnya sistem perlindungan data.

Berikut adalah bentuk-bentuk kejahatan siber dalam masyarakat digital yang umum terjadi seiring meningkatnya penggunaan internet dan teknologi digital:

1. *Phishing*

   Kejahatan dengan cara menipu korban agar memberikan data pribadi seperti kata sandi, PIN, OTP, atau data perbankan melalui email, pesan singkat, atau situs palsu yang menyerupai pihak resmi.

2. Penipuan Online

   Meliputi penipuan jual beli online, investasi bodong, undian palsu, hingga lowongan kerja fiktif yang bertujuan mengambil uang atau data korban.

3. Pencurian Data Pribadi

   Pengambilan dan penyalahgunaan data pribadi seperti NIK, alamat, nomor telepon, atau data akun digital tanpa izin pemiliknya, sering digunakan untuk penipuan lanjutan.

4. *Malware*

   Penyebaran perangkat lunak berbahaya seperti virus, trojan, *spyware*, dan *ransomware* yang dapat merusak sistem, mencuri data, atau mengunci perangkat korban.

5. Peretasan (*Hacking*)

   Upaya masuk ke sistem, akun, atau jaringan tanpa izin untuk mencuri data, merusak sistem, atau mengambil alih kendali akun digital.

6. *Cyberbullying*

   Tindakan perundungan, penghinaan, ancaman, atau pelecehan yang dilakukan melalui media sosial, aplikasi pesan, atau platform digital lainnya.

7. Penyebaran Hoaks dan Disinformasi

   Penyebaran berita palsu atau informasi menyesatkan yang dapat memicu kepanikan, konflik sosial, atau manipulasi opini publik.

8. *Cyberstalking*

   Penguntitan secara digital dengan memantau, mengintimidasi, atau mengganggu korban melalui media sosial dan platform online.

9. *Doxxing*

   Penyebaran data pribadi seseorang ke ruang publik tanpa izin dengan tujuan merugikan, mempermalukan, atau mengintimidasi korban.

10. Kejahatan Siber Terorganisir

Kejahatan yang dilakukan oleh kelompok terstruktur, sering berskala besar dan lintas negara, seperti sindikat penipuan internasional dan perdagangan data di *dark web.*

Kejahatan siber berdampak luas, mulai dari kerugian finansial, gangguan psikologis, hingga menurunnya kepercayaan masyarakat terhadap teknologi. Oleh karena itu, literasi digital dan kesadaran keamanan siber sangat penting dalam masyarakat digital saat ini.

2. Dampak Sosial dan Ekonomi

Dari aspek ekonomi, kejahatan siber menyebabkan kerugian finansial baik bagi individu maupun organisasi. Sementara itu, dari aspek sosial, kejahatan siber dapat menimbulkan rasa takut, trauma, dan menurunnya rasa aman dalam beraktivitas di ruang digital. Hal ini berpengaruh pada tingkat kepercayaan masyarakat terhadap teknologi digital. Kejahatan siber seperti phishing, penipuan online, dan pencurian data menyebabkan masyarakat menjadi waspada berlebihan saat berinteraksi di ruang digital. Kepercayaan terhadap *e-commerce*, media sosial, layanan perbankan digital, dan platform pemerintah menurun, sehingga menghambat pemanfaatan teknologi secara optimal.

Dalam kasus *cyberbullying* dan *doxxing*, dampaknya bisa sangat serius hingga memengaruhi kehidupan sosial dan produktivitas korban. Penyebaran hoaks, fitnah digital, atau kebocoran data pribadi dapat merusak reputasi seseorang secara luas dan permanen. Jejak digital yang sulit dihapus membuat korban kesulitan memulihkan nama baik, memengaruhi peluang kerja, pendidikan, dan hubungan sosial. Kejahatan siber berupa penyebaran ujaran kebencian, propaganda, dan disinformasi dapat memecah belah masyarakat, memperkuat polarisasi, dan memicu konflik sosial yang berdampak pada stabilitas sosial dan keamanan publik.

Kejahatan siber menyebabkan kerugian ekonomi langsung seperti Kehilangan tabungan akibat penipuan, Penyalahgunaan rekening dan kartu kredit, Pinjaman online ilegal atas nama korban, Kerugian ini dapat berdampak jangka panjang terhadap kondisi ekonomi keluarga korban. Tingginya kejahatan siber membuat masyarakat enggan

bertransaksi secara online, sehingga menghambat perkembangan sektor *e-commerce*, *fintech*, dan ekonomi kreatif digital. Serangan siber dapat melumpuhkan sistem kerja pemerintahan dan swasta, menyebabkan terhentinya layanan, keterlambatan produksi, serta menurunkan efisiensi dan daya saing ekonomi nasional.

Kejahatan siber memiliki dampak sosial dan ekonomi yang luas, kompleks, dan jangka panjang. Oleh karena itu, diperlukan kolaborasi antara pemerintah, pelaku usaha, dan masyarakat melalui peningkatan literasi digital, penguatan sistem keamanan, serta penegakan hukum siber yang efektif.

3. Dampak terhadap Keamanan dan Privasi

Kejahatan siber juga berdampak besar pada keamanan informasi dan privasi data pribadi. Kebocoran data dapat disalahgunakan untuk kepentingan ilegal, yang pada akhirnya merugikan korban dan mengancam stabilitas sistem digital secara keseluruhan. Kejahatan siber seperti peretasan, *malware*, dan serangan DDoS dapat melumpuhkan sistem komputer, jaringan perusahaan, hingga infrastruktur vital negara. Gangguan ini dapat menyebabkan Terhentinya layanan publik dan bisnis, Hilangnya kendali atas sistem digital dan Kerusakan perangkat keras dan lunak. Dalam skala besar, serangan ini dapat mengganggu stabilitas keamanan nasional.

Serangan siber sering menargetkan data sensitif seperti data pelanggan, rahasia bisnis, dan dokumen negara. Kebocoran data dapat dimanfaatkan oleh pelaku untuk Pemerasan, Penipuan lanjutan dan Spionase digital. Data yang bocor sulit ditarik kembali dan berpotensi disalahgunakan dalam jangka panjang. Kejahatan siber sering melibatkan pencurian dan penyalahgunaan data pribadi seperti NIK, alamat, nomor telepon, foto, dan data biometrik. Pelanggaran ini menghilangkan hak individu atas kendali data pribadinya. Data yang dicuri dapat digunakan untuk pencurian identitas, seperti Pembuatan akun palsu, Pengajuan pinjaman online ilegal dan Penipuan atas nama korban. Korban sering kali tidak menyadari penyalahgunaan ini hingga mengalami kerugian serius. Seringnya kasus kebocoran data membuat masyarakat kehilangan kepercayaan terhadap platform digital, termasuk media sosial, *e-commerce*, dan layanan keuangan digital. Akibatnya, partisipasi masyarakat dalam ekosistem digital menurun.

Kejahatan siber memberikan dampak serius terhadap keamanan dan privasi, baik pada tingkat individu, organisasi, maupun negara. Ancaman ini tidak hanya merugikan secara teknis, tetapi juga mengganggu rasa aman, kebebasan, dan kepercayaan dalam kehidupan digital. Oleh karena itu, perlindungan keamanan siber dan privasi data harus menjadi prioritas melalui literasi digital, penguatan sistem keamanan, dan penegakan hukum yang tegas.

D. KESIMPULAN DAN SARAN

Kejahatan siber merupakan ancaman nyata bagi masyarakat digital dengan dampak yang meluas pada aspek sosial, ekonomi, dan keamanan informasi. Tingginya ketergantungan masyarakat terhadap teknologi digital menjadikan kejahatan siber sebagai permasalahan serius yang memerlukan penanganan komprehensif. Upaya pencegahan dapat dilakukan melalui peningkatan literasi digital, penguatan sistem keamanan siber, serta penegakan hukum yang tegas dan berkelanjutan.

DAFTAR PUSTAKA

Anderson, R. (2019). *Security Engineering: A Guide to Building Dependable Distributed Systems.* Wiley.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Sage Publications.

Furnell, S. (2020). *Cybercrime: Vandalizing the Information Society.* Pearson Education.

Kshetri, N. (2017). *Cybercrime and cybersecurity in the global South*. International Journal of Information Management, 37(1), 1–10.

Maras, M. H. (2015). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Jones & Bartlett Learning.

Moore, T., Clayton, R., & Anderson, R. (2009*). The economics of online crime.* Journal of Economic Perspectives, 23(3), 3–20.

Organisation for Economic Co-operation and Development. (2020). *Cybersecurity Policy Making at a Turning Point.* OECD Publishing.

Republik Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Wall, D. S. (2017). *Cybercrime: The Transformation of Crime in the Information Age.* Polity Press.

Yar, M. (2013). *Cybercrime and Society*. Sage Publications