PESHUM : Jurnal Pendidikan, Sosial dan Humaniora
Vol.4, No.4, Juni 2025

Kriminalitas Di Era Digital: Kajian Kriminologi Terhadap Kejahatan Online

Vincent Tanaka[1], Jansen Chandra [2], Ricky Banke[3]
[1,2]Program Studi Hukum,
[3]Universitas Pelita Harapan Medan, Indonesia
E-mail: 03051220024@student.uph.edu[1],03051220007@student.uph.edu[2], ricky.banke@uph.edu[3]

Article History:
Received: 01 Mei 2025
Revised: 10 Mei 2025
Accepted: 20 Mei 2025

Keywords: *Kejahatan siber, Kriminologi, Motif pelaku, Literasi digital, Penanggulangan*

Abstract: *Penelitian ini bertujuan untuk mengkaji karakteristik kejahatan siber yang berkembang di era digital serta mengidentifikasi motif pelaku berdasarkan pendekatan kriminologi. Fenomena kejahatan online seperti phishing, pencurian identitas, peretasan, dan penipuan investasi semakin meningkat seiring dengan pesatnya penggunaan teknologi informasi. Metode yang digunakan dalam penelitian ini adalah deskriptif kualitatif melalui studi pustaka terhadap peraturan perundang-undangan, jurnal ilmiah, dan laporan lembaga resmi. Hasil pembahasan menunjukkan bahwa sebagian besar pelaku cybercrime terdorong oleh motif ekonomi dan didukung oleh kemampuan teknis yang tinggi. Kejahatan ini menimbulkan dampak signifikan terhadap individu, dunia usaha, hingga stabilitas negara. Oleh karena itu, penanggulangan kejahatan digital memerlukan strategi pencegahan yang berbasis literasi digital, pembaruan regulasi, dan kolaborasi antarnegara dalam menghadapi ancaman siber lintas batas.*

PENDAHULUAN

Beberapa dekade terakhir, perkembangan teknologi digital telah memberikan banyak manfaat bagi masyarakat, mulai dari kemudahan komunikasi, efisiensi dalam transaksi ekonomi, hingga perkembangan industri berbasis digital. Namun, seiring dengan kemajuan tersebut, muncul pula tantangan baru dalam bentuk kriminalitas digital yang semakin kompleks. Kejahatan online tidak lagi hanya berupa penipuan sederhana, tetapi telah berkembang menjadi bentuk kejahatan yang lebih terstruktur, melibatkan sindikat internasional, dan memanfaatkan teknologi canggih seperti kecerdasan buatan, enkripsi, serta jaringan anonim.

Kejahatan siber di Indonesia semakin meningkat dengan beragam modus operandi, termasuk phishing, pencurian identitas, peretasan akun, penyebaran malware, serta penipuan berbasis aplikasi. Kondisi ini memunculkan berbagai pertanyaan, baik dari sisi hukum, sosial, maupun kriminologi, terkait bagaimana kejahatan ini terjadi, siapa saja pelakunya, bagaimana dampaknya terhadap korban, serta upaya yang dapat dilakukan untuk mencegah dan menangani tindak kriminalitas ini secara efektif.

Studi ini berupaya mengkaji lebih dalam mengenai kriminalitas digital dari perspektif kriminologi, dengan menyoroti faktor-faktor yang menyebabkan seseorang terlibat dalam

kejahatan siber, dampaknya terhadap individu maupun masyarakat, serta langkah-langkah penegakan hukum dan pencegahan yang dapat dilakukan untuk mengatasi fenomena ini.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi pustaka (library research). Metode ini dipilih karena fokus penelitian adalah untuk memahami karakteristik kejahatan siber dan motif pelaku berdasarkan pendekatan kriminologi. Data dikumpulkan dari berbagai sumber sekunder, seperti buku teks kriminologi, jurnal ilmiah nasional dan internasional, dokumen hukum (terutama UU ITE dan peraturan pelaksanaannya), serta laporan resmi dari lembaga-lembaga seperti BSSN, Kominfo, dan Interpol. Studi pustaka memungkinkan peneliti menggali perspektif yang lebih dalam mengenai perkembangan dan dinamika kejahatan digital tanpa melakukan survei atau wawancara langsung.

Analisis data dilakukan secara tematik, dengan cara mengidentifikasi isu-isu utama seperti jenis kejahatan siber, profil dan motif pelaku, serta dampak sosial dari kejahatan digital. Dalam pendekatan kriminologi, peneliti menyoroti faktor-faktor penyebab seperti motif ekonomi, ideologi, dan kepuasan intelektual yang mendorong individu melakukan kejahatan digital. Dengan mengintegrasikan data dari berbagai sumber, penelitian ini bertujuan memberikan gambaran komprehensif mengenai bentuk kejahatan siber serta rekomendasi penanggulangannya secara sistemik dan preventif.

HASIL DAN PEMBAHASAN

Definisi dan Karakteristik Kejahatan Siber

Kejahatan siber dapat didefinisikan sebagai aktivitas ilegal yang dilakukan dengan memanfaatkan teknologi komputer dan internet sebagai sarana utama dalam pelaksanaannya. Berbeda dengan kejahatan konvensional yang biasanya melibatkan interaksi fisik antara pelaku dan korban, kejahatan siber sering kali dilakukan secara anonim dan dapat terjadi dalam skala global tanpa adanya batasan geografis.

Salah satu karakteristik utama kejahatan siber adalah kecepatan penyebarannya. Dalam hitungan detik, sebuah serangan malware dapat menyebar ke jutaan perangkat di seluruh dunia, atau informasi pribadi seseorang dapat dicuri dan dijual di pasar gelap digital. Selain itu, sifat tidak langsung dari kejahatan ini juga membuat banyak korban tidak segera menyadari bahwa mereka telah menjadi sasaran kriminal, sehingga memungkinkan pelaku untuk terus beroperasi tanpa terdeteksi dalam waktu yang lama.

Keunikan lain dari kejahatan siber adalah keterlibatan teknologi tingkat tinggi dalam modus operandi pelaku. Banyak kejahatan siber yang tidak hanya mengandalkan kecerdikan sosial dalam menipu korban, tetapi juga menggunakan perangkat lunak canggih, serangan brute force, eksploitasi celah keamanan, dan teknik enkripsi untuk menyamarkan jejak digital mereka. Hal ini membuat investigasi terhadap kejahatan siber menjadi lebih sulit dibandingkan dengan kejahatan konvensional.

Jenis-Jenis Kejahatan Siber

Kejahatan di era digital semakin berkembang seiring dengan kemajuan teknologi. Salah satu bentuk kejahatan yang sering terjadi adalah phishing dan penipuan online, di mana pelaku mengelabui korban agar memberikan informasi pribadi mereka, seperti kata sandi atau data kartu kredit. Modus yang digunakan biasanya berupa email atau situs web palsu yang menyerupai institusi resmi, sehingga korban tidak menyadari bahwa mereka sedang diperdaya. Selain melalui email, phishing juga sering dilakukan melalui pesan singkat (smishing) atau panggilan telepon (vishing), di mana pelaku berpura-pura sebagai pihak berwenang untuk mendapatkan informasi sensitif. Dampak dari kejahatan ini bisa sangat merugikan, mulai dari kehilangan akses ke akun keuangan hingga penyalahgunaan data pribadi untuk tujuan ilegal.

Pencurian identitas juga menjadi ancaman besar di dunia digital. Pelaku kejahatan dapat memperoleh informasi pribadi seseorang dan menggunakannya untuk melakukan berbagai tindakan ilegal, seperti mengakses rekening bank korban, mengajukan pinjaman atas nama mereka, atau bahkan menjual informasi tersebut di pasar gelap digital. Pencurian identitas tidak hanya menyebabkan kerugian finansial, tetapi juga dapat berakibat pada rusaknya reputasi korban serta kesulitan hukum jika identitas mereka digunakan untuk tindakan kriminal.

Kejahatan lain yang marak terjadi adalah peretasan dan penyebaran malware. Para peretas sering kali menargetkan individu, perusahaan, bahkan lembaga pemerintahan untuk mencuri data, merusak sistem, atau memata-matai aktivitas pengguna. Salah satu metode yang sering digunakan adalah ransomware, yaitu jenis malware yang mengenkripsi data korban dan meminta tebusan agar data tersebut dapat dipulihkan. Ada pula spyware yang bekerja secara diam-diam untuk mencuri informasi sensitif, serta serangan DDoS yang dapat melumpuhkan layanan digital dengan membanjiri server dengan lalu lintas palsu. Kejahatan semacam ini dapat menyebabkan kerugian besar, baik dari segi finansial maupun operasional.

Dunia investasi digital, penipuan berkedok investasi juga semakin marak terjadi. Banyak orang tergiur dengan iming-iming keuntungan tinggi dari investasi digital, tetapi tidak menyadari bahwa mereka sedang menjadi korban skema ponzi atau aset kripto palsu. Dalam skema ponzi, keuntungan yang didapatkan investor lama sebenarnya berasal dari dana investor baru, bukan dari keuntungan bisnis yang nyata. Begitu aliran dana berhenti, sistem ini akan runtuh, dan banyak investor kehilangan seluruh uang mereka. Selain itu, banyak platform trading palsu yang mengklaim dapat memberikan keuntungan besar tetapi pada akhirnya hanya menipu dan membawa kabur dana para investor.

Tidak hanya berkaitan dengan finansial, eksploitasi anak dan kejahatan seksual digital juga menjadi ancaman serius di era digital. Kejahatan ini melibatkan berbagai modus, mulai dari pelecehan di media sosial, penyebaran konten ilegal, hingga perdagangan manusia yang memanfaatkan platform digital untuk mencari korban. Banyak pelaku menggunakan metode grooming, di mana mereka membangun kepercayaan dengan anak-anak secara daring sebelum akhirnya melakukan eksploitasi. Dampaknya sangat berat, tidak hanya secara psikologis bagi korban, tetapi juga dapat mengancam keselamatan mereka di dunia nyata.

Menghadapi berbagai bentuk kejahatan digital ini, masyarakat perlu meningkatkan kewaspadaan dan kesadaran terhadap keamanan siber. Salah satu langkah yang dapat dilakukan adalah selalu berhati-hati saat menerima email atau pesan dari sumber yang tidak jelas, serta tidak sembarangan memberikan informasi pribadi di internet. Menggunakan autentikasi dua faktor pada akun online juga dapat meningkatkan keamanan. Selain itu, penting untuk lebih kritis terhadap tawaran investasi digital yang terdengar terlalu menggiurkan dan selalu memeriksa legalitasnya sebelum berinvestasi. Di sisi lain, bagi para orang tua, mengawasi aktivitas anak di internet menjadi langkah penting dalam mencegah eksploitasi anak secara daring. Dengan perkembangan teknologi yang semakin pesat, kejahatan digital juga terus berkembang dengan metode yang semakin canggih. Oleh karena itu, kesadaran dan kehati-hatian dalam menggunakan teknologi menjadi kunci utama dalam melindungi diri dari berbagai ancaman kejahatan di era digital ini.

Motivasi dan Profil Pelaku Kejahatan Siber

Kejahatan siber dilakukan oleh individu atau kelompok dengan beragam latar belakang dan motivasi. Secara umum, pelaku kejahatan siber dapat dikategorikan ke dalam beberapa kelompok, di antaranya hacker individu, sindikat kejahatan siber, teroris siber, serta aktor negara yang terlibat dalam spionase digital dan perang siber. Motivasi utama pelaku kejahatan siber bervariasi, tetapi sebagian besar didorong oleh keuntungan finansial. Peretas profesional sering menargetkan sistem perbankan, e-commerce, dan perusahaan besar untuk mencuri data pelanggan, yang kemudian

dijual di pasar gelap digital. Selain itu, ada juga pelaku yang menggunakan metode ransomware, yaitu mengunci data korban dan meminta tebusan dalam bentuk mata uang kripto agar data tersebut dikembalikan. Selain motif ekonomi, beberapa pelaku kejahatan siber juga memiliki motivasi ideologis dan politik. Mereka bisa berasal dari kelompok aktivis digital atau yang dikenal sebagai "hacktivists," yang menyerang sistem pemerintah atau korporasi dengan tujuan tertentu, seperti memprotes kebijakan atau mengungkap skandal. Contoh terkenal dari kelompok ini adalah Anonymous, yang sering kali melancarkan serangan terhadap institusi yang dianggap korup atau tidak adil.

Pelaku yang didorong oleh kepuasan intelektual dan keinginan untuk menunjukkan keahlian mereka dalam meretas sistem keamanan. Kelompok ini umumnya terdiri dari individu yang memiliki keahlian teknologi tinggi, tetapi tidak selalu memiliki niat jahat. Namun, jika tidak diarahkan dengan baik, mereka dapat berubah menjadi peretas kriminal yang mengeksploitasi celah keamanan untuk keuntungan pribadi. Selain itu, kelompok teroris siber juga semakin marak menggunakan teknologi untuk menyebarkan propaganda, merekrut anggota, hingga melancarkan serangan terhadap infrastruktur penting suatu negara. Mereka memanfaatkan media sosial dan platform digital lainnya untuk menyebarkan pesan radikal dan mengorganisir aksi-aksi terorisme secara global.

Berkembangnya teknologi, aktor negara juga mulai memanfaatkan kejahatan siber sebagai alat untuk melakukan spionase terhadap negara lain. Beberapa negara menggunakan teknologi peretasan untuk mencuri data strategis, mengganggu sistem pemilu, atau bahkan melancarkan serangan terhadap infrastruktur kritis negara lain dalam konteks perang siber. Dari segi usia dan latar belakang sosial, pelaku kejahatan siber tidak terbatas pada kelompok tertentu. Banyak pelaku yang masih berusia muda dan memiliki latar belakang pendidikan teknologi informasi. Namun, ada juga yang merupakan bagian dari jaringan kriminal terorganisir dengan operasi yang sangat kompleks dan canggih.

Dampak Kriminalitas Digital terhadap Masyarakat

Kejahatan digital memberikan dampak yang luas dan kompleks terhadap berbagai aspek kehidupan, baik secara individu maupun kolektif. Dampaknya tidak hanya terbatas pada kerugian materi, tetapi juga menyentuh aspek psikologis, sosial, hingga geopolitik. Berikut adalah uraian mengenai berbagai dampak kriminalitas digital:

a. Dampak terhadap Individu

Kejahatan siber terhadap individu sangat nyata dan beragam, mulai dari kerugian finansial hingga gangguan psikologis yang serius. Banyak individu menjadi korban penipuan online, phishing, atau pencurian data pribadi yang digunakan untuk mengakses akun perbankan atau identitas digital mereka. Akibatnya, korban kehilangan tabungan, akses terhadap layanan penting, dan bahkan mengalami beban hukum jika data pribadi mereka disalahgunakan untuk aktivitas ilegal. Psikologis menyebabkan korban dapat mengalami stres berat, gangguan kecemasan, hingga depresi. Dalam kasus cyberbullying atau pelecehan daring, trauma psikologis yang ditimbulkan bisa mengganggu hubungan sosial korban, menurunkan rasa percaya diri, dan dalam kasus ekstrem, mendorong korban ke arah tindakan menyakiti diri sendiri atau bahkan bunuh diri.

b. Dampak terhadap Dunia Usaha

Sektor bisnis juga sangat rentan terhadap dampak dari kriminalitas digital. Serangan siber terhadap perusahaan dapat mengakibatkan gangguan operasional, kerugian finansial, dan rusaknya reputasi. Kasus seperti kebocoran data pelanggan, gangguan sistem akibat serangan DDoS (Distributed Denial-of-Service), atau serangan ransomware yang mengenkripsi data perusahaan dan meminta tebusan, merupakan contoh nyata dari risiko tersebut. Perusahaan harus menanggung biaya tinggi untuk pemulihan sistem, kompensasi kepada pelanggan, dan peningkatan keamanan

pasca insiden. Selain itu, kehilangan kepercayaan publik terhadap merek atau institusi bisnis dapat berdampak jangka panjang terhadap kinerja dan keberlangsungan usaha.

c. Dampak terhadap Pemerintahan dan Keamanan Nasional

Kejahatan digital terhadap pemerintahan dan keamanan nasional tidak dapat diabaikan. Serangan terhadap sistem pemerintahan, seperti peretasan data sensitif lembaga negara, gangguan terhadap proses pemilu, atau sabotase terhadap infrastruktur vital seperti jaringan listrik dan transportasi, dapat mengguncang stabilitas negara. Hal ini menunjukkan bahwa kejahatan siber tidak hanya menjadi ancaman terhadap individu dan bisnis, tetapi juga terhadap kedaulatan dan keamanan suatu negara.

Serangan siber yang dilakukan oleh aktor negara lain (state-sponsored attacks) atau kelompok teroris dapat digunakan sebagai instrumen perang non-militer dalam era konflik modern, yang dikenal sebagai cyber warfare. Serangan ini dapat menciptakan disinformasi, mengadu domba masyarakat, atau bahkan merusak sistem pertahanan negara tanpa perlu menggunakan senjata konvensional.

d. Dampak terhadap Struktur Sosial

Kriminalitas digital juga memengaruhi struktur sosial masyarakat. Penyebaran berita palsu (hoaks), ujaran kebencian, dan propaganda ekstremis di media sosial dapat menimbulkan perpecahan sosial, memperkuat polarisasi politik, serta menciptakan ketidakpercayaan terhadap institusi publik. Kejahatan siber dalam bentuk penyebaran konten ilegal, seperti eksploitasi anak atau konten kekerasan, juga mengancam norma sosial dan nilai-nilai kemanusiaan. Fenomena ini memperlihatkan bahwa dunia digital dapat menjadi alat yang sangat kuat dalam membentuk opini publik, baik secara positif maupun negatif. Tanpa regulasi dan pengawasan yang tepat, ruang digital dapat berubah menjadi medan baru bagi konflik sosial dan ideologis.

e. Dampak terhadap Pendidikan dan Anak-anak

Anak-anak dan remaja termasuk kelompok paling rentan dalam dunia digital. Mereka lebih mudah menjadi korban eksploitasi daring, cyberbullying, atau terpapar konten yang tidak sesuai usia. Ketidaksiapan orang tua dan pendidik dalam mengawasi serta membimbing aktivitas digital anak-anak semakin memperbesar risiko ini. Selain itu, adanya konten digital yang mengandung kekerasan, ujaran kebencian, atau perilaku menyimpang dapat membentuk pola pikir yang menyimpang pula pada anak-anak, yang secara psikologis masih dalam tahap perkembangan identitas. Hal ini dapat berdampak pada penurunan kualitas pendidikan dan pembentukan karakter generasi muda.

KESIMPULAN

Kriminalitas di era digital merupakan tantangan baru yang kompleks dalam bidang penegakan hukum dan perlindungan masyarakat. Berbeda dengan kejahatan konvensional, kejahatan digital melibatkan penggunaan teknologi informasi dan komunikasi sebagai sarana utama, yang memungkinkan pelaku untuk beroperasi secara anonim, lintas batas negara, dan dalam skala yang jauh lebih luas. Melalui pendekatan kriminologi, penelitian ini mengungkap bahwa motif pelaku kejahatan digital dapat sangat beragam, mulai dari dorongan ekonomi, ideologi, hingga kebutuhan akan eksistensi sosial, sementara dampaknya tidak hanya bersifat personal terhadap korban, tetapi juga mengancam stabilitas ekonomi, keamanan data, serta kepercayaan publik terhadap sistem digital.

Penelitian ini menunjukkan bahwa kejahatan digital memerlukan penanganan yang tidak hanya mengandalkan perangkat hukum yang ada, tetapi juga pendekatan multidisipliner. Upaya penanggulangan harus dimulai dari penguatan literasi digital masyarakat, terutama dalam memahami bentuk-bentuk ancaman siber seperti phishing, pencurian identitas, peretasan, dan penyebaran malware. Materi keamanan siber juga perlu diintegrasikan dalam kurikulum

pendidikan sejak dini, agar generasi muda terbentuk menjadi individu yang tanggap terhadap risiko digital. Selain itu, pembaruan regulasi merupakan aspek krusial yang harus dilakukan secara terus-menerus agar mampu menyesuaikan dengan perkembangan teknologi informasi yang sangat dinamis. Penegakan hukum terhadap pelaku kejahatan siber pun harus dilakukan secara cepat, terkoordinasi, dan dilengkapi dengan teknologi pendukung seperti kecerdasan buatan (AI), big data analytics, serta teknik forensik digital. Pelatihan intensif bagi aparat penegak hukum dalam bidang tersebut menjadi hal yang tak terelakkan agar mampu menghadapi kejahatan siber secara profesional dan akurat.

Kerja sama internasional juga menjadi landasan penting dalam pemberantasan kejahatan digital. Mengingat sebagian besar pelaku beroperasi secara global, diperlukan kesepakatan antarnegara dalam hal ekstradisi, pertukaran informasi intelijen, dan pelaksanaan investigasi lintas negara. Di sisi lain, penting juga untuk membangun infrastruktur keamanan siber yang kuat, baik di sektor publik maupun swasta, dengan penerapan sistem keamanan berlapis yang mencakup enkripsi, firewall, dan deteksi dini ancaman. Tidak kalah pentingnya, pendekatan yang humanis juga diperlukan untuk pelaku kejahatan siber, terutama mereka yang terdorong oleh kondisi sosial ekonomi tertentu. Pemerintah perlu menyediakan program rehabilitasi dan pelatihan keahlian digital yang diarahkan pada kegiatan legal dan produktif. Hal ini dapat mendorong para pelaku untuk kembali ke jalur yang benar dan turut berkontribusi bagi masyarakat. Secara keseluruhan, penanggulangan kejahatan digital membutuhkan sinergi antara pendekatan preventif, represif, dan rehabilitatif, serta dukungan penuh dari seluruh elemen masyarakat dan negara. Dengan pendekatan yang holistik dan adaptif, diharapkan Indonesia mampu menciptakan ruang digital yang aman, adil, dan bertanggung jawab di tengah arus transformasi teknologi global yang semakin pesat.

DAFTAR REFERENSI

APTIKA (2022). *"Indonesia Hadapi 1,6 Miliar Serangan Siber Sepanjang 2022"* https://aptika.kominfo.go.id/2022/12/serangan-siber-2022/

BSSN – Statistik Serangan Siber Indonesia 2023. https://www.bssn.go.id/laporan-tahunan-bssn-2023

Dewi, M. P., & Santoso, B. (2021). *Cybercrime di Indonesia: Studi Kasus dan Aspek Kriminologis. Jurnal Keamanan Nasional*, 7(2), 128–143. https://jurnal.uki.ac.id/index.php/jkn

Gillespie, Alisdair & T.J. Sorell. (2020). *Cybercrime and Society (3rd Edition).* London: SAGE Publications. ISBN: 9781526484687

Handayani, T. R., & Pramudito, A. (2022). *Kejahatan Siber dan Penegakan Hukumnya di Era Digital. Jurnal Kriminologi Indonesia*, 18(2), 101–115. https://jurnal.ui.ac.id/kriminologi/article/view/18234

Kurniawan, Andi. (2021). *Cybercrime dan Penegakan Hukumnya di Indonesia.* Jakarta: Prenadamedia Group. ISBN: 9786232180126

Nurrahman, D. (2023). *Peran Penegakan Hukum dalam Menanggulangi Kejahatan Siber di Indonesia. Jurnal Hukum dan Pembangunan*, 53(1), 45–60. https://doi.org/10.21143/jhp.vol53.no1.4532

Rahardjo, Satjipto. (2020). *Kriminologi Modern: Teori dan Aplikasi dalam Dunia Digital.* Yogyakarta: Genta Publishing. ISBN: 9786025411950

UU NOMOR 19 TAHUN 2016 ITE