# ANALISIS KRIMINOLOGIS PENYALAHGUNAAN KECERDASAN BUATAN DALAM KEJAHATAN SIBER

**Rudi Nopiansyah**

Fakultas Hukum, Universitas Sultan Ageng Tirtayasa, Serang, Indonesia
Jl. Raya Jkt No.3, Sindangsari, Kec. Pabuaran, Kota Serang, Banten 42163
e-mail : rudi.nopiansyah@untirta.ac.id

**Mega Fitri Hertini, Parulian Siagian, Sri Ismawati, Herlina**

Fakultas Hukum, Universitas Tanjungpura, Pontianak, Indonesia
Jl. Profesor Dokter H. Hadari Nawawi, Bansir Laut, Kalimantan Barat 78124
e-mail: mega.fitri.h@hukum.untan.ac.id, parulian.siagian@hukum.untan.ac.id,
sri.ismawati@hukum.untan.ac.id, herlina@hukum.untan.ac.id

**Abstrak:** From a criminological perspective and its implications for criminal law in Indonesia using a qualitative literature review of scientific sources, legal documents, and relevant cases.""Results show that AI functions as a tool, object, and in some cases an autonomous element in cybercrime. Common forms include deepfakes, automated phishing, and algorithm-based hacking. AI-related crime is influenced by individual, structural, and cultural factors such as technological expertise, economic and ideological motives, and the anonymity of digital environments, which weakens social control. It also reflects a shift from manual to automated crime and from individual to network-based offenses.""The study concludes that current criminal law is not yet fully adequate to address AI-based crime, particularly in determining legal responsibility. Therefore, regulatory adaptation and integration of ethical and technological governance are required.

**Keywords:** Artificial Intelligence, Cybercrime, Criminology, Criminal Law, Legal Liability

## Pendahuluan

Perkembangan teknologi dalam lintasan sejarah manusia selalu menghadirkan perubahan besar yang memengaruhi struktur sosial, ekonomi, dan sistem hukum. Dimulai dari Revolusi Industri 1.0 melalui penemuan mesin uap, manusia mengalami percepatan proses produksi dan peningkatan mobilitas. Revolusi 2.0 kemudian membawa listrik yang memungkinkan produksi massal dengan biaya lebih efisien. Selanjutnya, Revolusi 3.0 menghadirkan komputer yang tidak hanya meningkatkan efektivitas produksi, tetapi juga mempercepat pertukaran informasi lintas negara sehingga batas-batas sosial menjadi semakin kabur. Pada tahap ini, muncul pula identitas global citizen sebagai cerminan masyarakat yang semakin terhubung secara digital. Kini, dunia memasuki Revolusi Industri 4.0, di mana kecerdasan buatan (Artificial Intelligence/AI) menjadi kekuatan transformasi yang tidak hanya memudahkan pekerjaan manusia, tetapi juga mengotomatisasi berbagai fungsi yang sebelumnya membutuhkan kehadiran manusia. Pada perkembangan berikutnya, Revolusi Industri 5.0 berupaya mengembalikan manusia sebagai pusat inovasi sekaligus memastikan teknologi, termasuk AI, diarahkan untuk meningkatkan kualitas hidup manusia [1].

Kemajuan kecerdasan buatan dalam beberapa dekade terakhir telah menghadirkan dampak besar di berbagai sektor seperti kesehatan, transportasi, keuangan, dan keamanan. Dalam konteks hukum dan kriminologi, AI membawa dua sisi yang kontras: ia dapat dimanfaatkan untuk mendukung penegakan hukum, namun sekaligus berpotensi menjadi alat yang efektif bagi pelaku kejahatan. Teknologi seperti deepfake, algoritma manipulatif, dan sistem generatif membuka peluang terjadinya bentuk kejahatan baru yang bersifat otomatis, kompleks, serta sulit dilacak [2]. Fenomena ini menantang teori-teori kriminologi tradisional dan memunculkan problem baru dalam hukum pidana, terutama karena sistem hukum selama ini selalu berpijak pada pelaku manusia, sedangkan AI dapat beroperasi secara semi-otonom [3].

Sejumlah kasus menunjukkan bagaimana penyalahgunaan AI dapat menimbulkan kerugian sosial. Di Indonesia, penyebaran video deepfake yang dikaitkan dengan figur publik Bulan Sutena memperlihatkan bagaimana teknologi ini dapat mencemarkan nama baik seseorang melalui manipulasi digital. Di tingkat global, kasus di Provinsi Gansu, China, di mana seorang pria ditangkap karena menggunakan ChatGPT untuk memproduksi artikel palsu, menunjukkan bagaimana AI dapat menjadi sarana penyebaran disinformasi secara masif. Terbaru adalah kasus penyalahgunaan teknologi Grok AI dari *Platform X (Twitter)* yang disalahgunakan untuk memanipulasi foto menjadi konten pornografi palsu atau *Non-Consensual Deepfake Sexual Imagery* (NCDSI). Kasus-kasus tersebut menegaskan bahwa penyalahgunaan kecerdasan buatan tanpa pemahaman etika, norma sosial, serta hukum dapat menjadi ancaman serius bagi masyarakat.

Sejumlah penelitian terdahulu telah memberikan kontribusi penting dalam memahami relasi antara kecerdasan buatan dan kejahatan. [4] Menjelaskan kecerdasan buatan memiliki potensi besar untuk dimanfaatkan dalam hal hal bersifat positif, tetapi manfaatnya hanya tercapai jika dibarengi dengan pengembangan dan penerapan norma serta prinsip etika yang kuat yang memastikan teknologi ini tetap berada di bawah kendali manusia dan melindungi hak serta nilai-nilai kemanusia. [5] Mengemukakan konsep *AI-Crime* dimana konsep yang menggambarkan kemungkinan AI digunakan sebagai alat utama dalam pelaksanaan aksi kriminal bukan hanya sebagai alat bantu sederhana, tetapi sebagai faktor yang berkontribusi penting dalam terjadinya kejahatan. Bryson mengemukakan argumen bahwa kecerdasan buatan bukan fenomena terpisah dari dinamika sosial manusia, melainkan bagian dari evolusi interaksi antara teknologi dan struktur sosial. Karena itu, memahami AI memerlukan pendekatan lintas disiplin yang mempertimbangkan konsekuensi sosial-politik dan nilai-nilai kemanusiaan, bukan hanya kemajuan teknis. [6] menunjukkan bahwa meskipun manusia tetap menjadi subjek hukum utama, keberadaan AI menimbulkan pertanyaan

baru terkait tanggung jawab hukum, perlindungan hak asasi manusia, dan pengakuan status hukum AI. Oleh karena itu, diperlukan reformasi regulasi yang komprehensif dan berorientasi pada prinsip-prinsip etika humanisme untuk menjaga martabat dan hak-hak manusia dalam konteks perkembangan AI. Implikasi dari kajian ini menegaskan pentingnya integrasi aspek hukum dan etika dalam penyusunan kebijakan AI di Indonesia guna memastikan perlindungan subjek hukum manusia tetap terjaga di tengah kemajuan teknologi.

Meskipun demikian, penelitian-penelitian tersebut belum membahas secara komprehensif hubungan antara penyalahgunaan AI dan kriminologi. Penelitian yang ada cenderung fokus pada aspek teknologi atau hukum secara terpisah, sehingga belum menghasilkan analisis integratif mengenai bagaimana kejahatan berbasis AI dapat terjadi jika dilihat dari sudut pandang kriminologi . Selain itu, literatur yang ada belum memberikan kerangka konseptual untuk menjawab kesenjangan mengapa terjadi penyalahgunaan kecerdasan buatan dalam kejahatab siber. Kondisi ini diperburuk oleh cepatnya perkembangan teknologi AI generatif, sehingga kajian akademik sering kali tertinggal dibandingkan dinamika kasus nyata.

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk memberikan analisis mendalam mengenai fenomena kecerdasan buatan dari perspektif kriminologi. Penelitian ini tidak hanya mendeskripsikan potensi ancaman dan bentuk-bentuk penyalahgunaan AI, tetapi juga mengidentifikasi faktor risiko yang memungkinkan terjadinya kejahatan berbasis teknologi tersebut. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi teoritik dan praktis bagi pengembangan kerangka hukum nasional yang lebih adaptif terhadap perkembangan teknologi global dan mampu melindungi masyarakat dari ancaman kejahatan berbasis kecerdasan buatan.

## Metode

Penelitian ini menggunakan pendekatan kualitatif dengan metode kepustakaan (*library research).* Pendekatan ini dipilih karena penelitian berfokus pada analisis konsep, teori, regulasi, dan temuan-temuan ilmiah yang relevan dengan perkembangan kecerdasan buatan serta implikasinya dalam kriminologi dan hukum pidana. Seluruh data penelitian diperoleh dari literatur ilmiah berupa buku, artikel jurnal nasional maupun internasional, laporan penelitian, dokumen hukum, serta berita yang kredibel terkait fenomena penyalahgunaan kecerdasan buatan.

Pemilihan literatur dilakukan dengan mempertimbangkan standar akademik yang ketat. Artikel jurnal internasional yang digunakan umumnya berasal dari publikasi yang terindeks Scopus atau Web of Science, dengan preferensi pada jurnal bereputasi Internasional. Untuk jurnal nasional, prioritas diberikan pada jurnal yang terakreditasi sebagai jaminan kualitas ilmiah dan relevansi topik dalam konteks Indonesia. Tahun publikasi yang digunakan terutama berada dalam rentang 2018–2024, mengingat perkembangan kecerdasan buatan yang sangat cepat dan kebutuhan untuk memastikan bahwa analisis didasarkan pada literatur yang mutakhir. Namun, beberapa literatur klasik yang dianggap fundamental bagi pengembangan teori kriminologi tetap disertakan, walaupun diterbitkan sebelum tahun 2018.

Selain mempertimbangkan akreditasi dan reputasi jurnal, proses seleksi literatur juga memperhatikan keterkaitan langsung dengan topik penelitian, yakni hubungan antara kecerdasan buatan dan tindak kriminal. Literatur yang dipilih harus membahas konsep-konsep seperti AI crime, deepfake, kejahatan siber, pertanggungjawaban pidana, teori kriminologi modern, serta etika dan tata kelola AI. Literatur yang bersifat opini populer, tidak terverifikasi, atau tidak memiliki dasar ilmiah yang jelas tidak dimasukkan sebagai objek kajian, kecuali sebagai bahan kontekstual untuk menggambarkan fenomena empiris tertentu. Berita daring hanya digunakan sejauh diperlukan untuk menunjukkan kasus konkret yang relevan dengan analisis, dan hanya media yang kredibel yang dijadikan rujukan.

## Hasil dan Pembahasan

Hasil penelitian perkembangan kecerdasan buatan (*Artificial Intelligence*/ AI) telah mengubah secara radikal lanskap kejahatan digital. Jika sebelumnya pelaku bergantung pada kemampuan teknis manual, kini AI berperan sebagai pengganda kemampuan kriminal dengan memberikan kecepatan, presisi, dan kapasitas otomatisasi yang belum pernah ada sebelumnya. Dalam konteks hukum pidana siber, AI tidak hanya berfungsi sebagai alat bantu kejahatan, tetapi juga objek dan entitas yang berperilaku otonom, sehingga memunculkan persoalan yuridis baru tentang pelaku, korban, dan pertanggungjawaban hukum.

A.Wajah Baru Kejahatan Digital Menggunakan Kecerdasan Buatan

Dalam konteks saat ini, kecerdasan buatan semakin sering digunakan dalam pola kejahatan siber modern. Bentuk penyalahgunaan AI dalam kejahatan siber dapat diklasifikasikan ke dalam tiga posisi fungsional:

1.AI sebagai sarana kejahatan *(AI as a Tool of Crime)*

Dalam konteks ini, AI berperan sebagai alat yang mempermudah pelaku manusia dalam melakukan kejahatan siber. AI digunakan untuk mengotomatisasi tindakan ilegal, mulai dari proses persiapan sampai pada proses pelaksanaannya dimana penggunaan AI dapat meningkatkan peluang keberhasilan, serta mengaburkan identitas pelaku di ruang siber. Bentuk-bentuk utama modus kejahatan semacam ini meliputi:

a.Pemanfaatan *Deepfake* untuk Penipuan dan Pemerasan.

Algoritma *deep learning* yang dirancang untuk menghasilkan konten sintetis kini banyak disalahgunakan untuk menciptakan *deepfake*, yaitu rekayasa wajah, suara, atau video yang sangat menyerupai individu nyata. Kejahatan yang sering muncul adalah pemerasan digital (*cyber extortion*), di mana pelaku menciptakan video palsu korban untuk memperoleh uang tebusan, serta penipuan berbasis identitas palsu, seperti mengelabui pejabat keuangan dengan suara palsu atasannya [7]. Dampak sosial deepfake bukan hanya kerugian ekonomi, tetapi juga erosi kepercayaan publik terhadap bukti digital dan media elektronik [8].

b. Otomatisasi Serangan Phishing dan Manipulasi Opini Publik

Kecerdasan buatan memperkuat taktik *phishisng* dengan cara yang lebih canggih.[9] *AI* dapat memproduksi pesan phishing secara besar-besaran dengan personalisasi tinggi melalui *natural language processing* (NLP) dan behavioral analytics. Sistem ini menganalisis kebiasaan komunikasi target, lalu menghasilkan pesan yang seolah-olah ditulis manusia, meningkatkan efektivitas serangan secara drastis.[10] Dalam konteks ini, AI menjadi mesin propaganda otomatis yang mampu memanipulasi kesadaran kolektif masyarakat digital. Selain itu, AI botnets juga dipakai untuk mengendalikan jutaan akun palsu dalam penyebaran disinformasi atau information warfare, terutama pada momentum politik dan konflik internasional.[11] Dalam konteks ini, AI menjadi mesin propaganda otomatis yang mampu memanipulasi kesadaran kolektif masyarakat digital.

c. Serangan Peretasan Otomatis *(AI-Driven Hacking)*

Teknologi AI kini mampu melakukan peretasan adaptif tanpa campur tangan manusia secara langsung. Melalui metode reinforcement learning, sistem dapat menguji kelemahan sistem keamanan dan menyesuaikan strategi berdasarkan respons target. IBM Research mendemonstrasikan potensi serangan ini melalui DeepLocker, sebuah malware berbasis AI yang hanya mengaktifkan diri setelah mengenali target tertentu.[12] Fenomena ini menunjukkan bahwa kejahatan siber telah berevolusi dari sekadar eksploitasi manual menjadi peretasan yang bersifat self-learning dan situasional, yang jauh lebih sulit dideteksi oleh sistem pertahanan konvensional.

2. AI sebagai sasaran kejahatan *(AI as an Object of Crime)*

Dalam posisi ini, sistem AI menjadi korban atau target serangan. Kejahatan ini menunjukkan bahwa perangkat cerdas tidak hanya digunakan untuk berbuat salah, tetapi juga menjadi aset bernilai tinggi yang dilindungi hukum.

a. Serangan terhadap Integritas Sistem AI

Serangan terhadap sistem AI biasanya berbentuk data poisoning

atau model manipulation. Pelaku dengan sengaja memasukkan data yang salah, bias, atau berbahaya ke dalam dataset pelatihan sehingga model menghasilkan keputusan keliru.

Contohnya, sistem AI perbankan dapat dimanipulasi agar salah menilai kelayakan kredit seseorang, atau sistem pengenalan wajah dipaksa gagal mengenali pelaku kriminal.[13] Selain itu, praktik model theft, pencurian arsitektur atau parameter algoritma kerap dilakukan untuk keuntungan industri atau spionase ekonomi.

b. Pembajakan Sistem Otonom Berbasis AI

Kejahatan jenis ini terjadi ketika pelaku mengambil alih sistem berbasis AI yang mengendalikan objek fisik seperti drone, kendaraan otonom, atau robot industri. Akibatnya, sistem tersebut dapat diarahkan untuk melakukan tindakan berbahaya, misalnya penyelundupan, spionase, atau serangan terencana.

3. AI sebagai entitas pelaku semu *(AI as a Virtual Offender)*

Fenomena paling problematik dalam penyalahgunaan AI adalah ketika sistem cerdas bertindak secara mandiri tanpa kontrol manusia langsung, dan tindakan itu menimbulkan kerugian hukum bagi pihak lain. Kejadian semacam ini menimbulkan perdebatan filosofis dan yuridis: apakah AI dapat dianggap sebagai pelaku yang memiliki tanggung jawab hukum?

a. Otonomi Algoritmik dan Dampak Hukumnya

Sistem AI yang dirancang dengan autonomous decision-making dapat mengambil tindakan berdasarkan data dan konteks tanpa instruksi eksplisit manusia. Misalnya, algoritma transaksi saham dapat menimbulkan kejatuhan pasar *(flash crash)* karena keputusan otomatis yang ekstrem; atau sistem keamanan digital menyerang server sah akibat salah deteksi ancaman. Meskipun tindakan tersebut nyata *(actus reus),* AI tidak memiliki kesadaran atau kehendak sehingga unsur *mens rea* tidak terpenuhi. Dilema ini menempatkan AI di wilayah abu-abu antara alat pasif dan pelaku aktif.

b. Atribusi Pertanggungjawaban *(Liability Attribution)*

Dalam literatur hukum kontemporer, terdapat beberapa pendekatan untuk menentukan tanggung jawab atas tindakan AI:[14]

i. Pendekatan berbasis manusia (*human responsibility model*) dimana tanggung jawab tetap pada pengguna AI.

ii. Pendekatan tanggung jawab korporasi *(corporate or vicarious liability)* jika AI dimiliki atau dikembangkan oleh badan hukum, maka entitas tersebut memikul tanggung jawab atas kelalaiannya.

iii. Pendekatan persona elektronik *(electronic personhood)* mengakui AI tertentu sebagai subjek hukum terbatas yang dapat menanggung akibat hukum atas tindakannya.

Setiap model memiliki kelemahan. Model manusia sulit diterapkan ketika AI bertindak di luar ekspektasi. Model korporasi rentan pada *burden of proof* yang kompleks, sedangkan model persona elektronik menimbulkan perdebatan moral tentang status hukum entitas non-biologis.

Ketiga bentuk penyalahgunaan AI tersebut memperlihatkan transformasi pola kejahatan digital, dari sekadar eksploitasi perangkat keras menuju manipulasi sistem cerdas yang dapat berpikir dan bertindak secara mandiri. Dari sisi kriminologi, hal ini menggeser paradigma klasik tentang pelaku dan alat kejahatan, AI menempati ruang di antara keduanya. Sementara dari perspektif hukum pidana, penyalahgunaan AI menantang prinsip *nullum crimen sine lege dan actus non facit reum nisi mens sit rea,* karena hukum positif belum sepenuhnya mengenali "perbuatan" oleh entitas non-manusia.

Dengan demikian, kejahatan siber berbasis AI menuntut model pemidanaan yang baru, berbasis *risk governance, ethical accountability, dan technological foresight*, agar hukum dapat berfungsi bukan sekadar menghukum, tetapi juga mengantisipasi bentuk kejahatan masa depan.

B. Analisis Kriminoligis

Analisis kriminologis terhadap penyalahgunaan kecerdasan buatan (AI) dalam kejahatan siber berfungsi untuk memahami struktur motivasional, lingkungan sosial, dan karakter pelaku di balik tindakan kriminal digital yang semakin kompleks. Berbeda dengan kejahatan konvensional yang berakar pada faktor sosial-ekonomi tradisional, kejahatan siber berbasis AI mencerminkan transformasi bentuk kejahatan dari fisik ke kognitif, di mana kecerdasan, informasi, dan algoritma menjadi instrumen baru penyimpangan. Dalam pandangan kriminologi modern, tindakan kriminal bukan hanya pelanggaran hukum, tetapi juga manifestasi dari proses sosial yang menormalisasi perilaku menyimpang di ruang digital.[15] Analisis ini menguraikan bagaimana individu atau kelompok dapat terdorong menggunakan AI untuk kejahatan, dengan meninjau aspek profil pelaku, struktur motivasi, dan lingkungan sosial yang memfasilitasi perilaku tersebut.

1. Profil dan Karakteristik Pelaku

a. Pelaku Individual *(Tech-Savvy Offenders)*

Sebagian besar pelaku kejahatan siber berbasis AI berasal dari individu dengan latar belakang teknologi informasi, sains data, atau rekayasa perangkat lunak. Mereka memiliki tingkat literasi digital tinggi, namun tidak jarang mengalami alienasi sosial atau marginalisasi ekonomi, yang mendorong mereka menggunakan keahliannya untuk tujuan ilegal.[16] Bentuk kejahatan yang dilakukan cenderung rasional dan terencana, bukan impulsif. Mereka mengandalkan algoritma sebagai alat *displacement of intent*, yaitu pemindahan niat jahat ke sistem otomatis agar risiko pribadi dapat diminimalkan.

b. Pelaku Korporasi dan Kelompok Terorganisasi

Selain individu, korporasi atau entitas organisasi juga dapat menjadi pelaku kejahatan berbasis AI, khususnya dalam bentuk *corporate cybercrime* seperti manipulasi algoritmik, penyalahgunaan data pelanggan, maupun praktik surveillance capitalism. Dalam konteks ini, penyimpangan tidak

selalu bersifat individual, melainkan terinstitusionalisasi dalam proses pengambilan keputusan organisasi yang memanfaatkan teknologi untuk mencapai keuntungan ekonomi secara tidak sah.[17] Fenomena ini menunjukkan bahwa struktur korporasi modern dapat menciptakan *criminogenic environments*, yaitu kondisi organisasi yang secara sistemik mendorong terjadinya pelanggaran hukum.[18] Praktik seperti eksploitasi data pengguna secara masif tanpa persetujuan atau manipulasi perilaku konsumen melalui algoritma mencerminkan pergeseran kejahatan dari tindakan individual menuju kejahatan korporasi yang kompleks dan tersembunyi.[19] Bahkan, dalam beberapa kasus, teknologi AI digunakan untuk mempengaruhi dinamika pasar atau keputusan ekonomi secara tidak transparan, sehingga menimbulkan risiko serius terhadap integritas sistem ekonomi digital.

c. Kejahatan Kolektif dan Subkultur Siber

Kemunculan komunitas hacker underground dan AI black market menunjukkan lahirnya subkultur digital, yaitu kelompok sosial dengan nilai, simbol, dan norma tersendiri yang seringkali bertentangan dengan hukum formal. Dalam perspektif teori subkultural, kelompok ini membangun sistem rasionalisasi moral yang membenarkan penyimpangan, seperti gagasan bahwa "informasi harus bebas" atau bahwa sistem keamanan digital layak untuk diuji dan ditembus.[20] Nilai-nilai tersebut berfungsi sebagai mekanisme legitimasi internal yang memperkuat identitas kelompok sekaligus menormalisasi perilaku menyimpang.[21] Dalam konteks ini, AI tidak hanya berfungsi sebagai alat kejahatan, tetapi juga sebagai simbol kekuasaan, keahlian, dan status dalam subkultur tersebut.[22] Dengan demikian, kejahatan siber berbasis AI tidak dapat dipahami semata sebagai tindakan individual, melainkan sebagai fenomena kolektif yang tumbuh dalam ekosistem sosial digital yang memiliki logika dan etika tersendiri.[23]

2. Motif dan Rasionalisasi Perilaku Pelaku

Penyalahgunaan AI didorong oleh kombinasi motif instrumental dan ekspresif, yang saling berinteraksi dalam konteks sosial digital.

a. Motif ekonomi

Pelaku yang memiliki motif ekonomi dalam penyalahgunaan AI untuk keuntungan finansial melalui kejahatan seperti *ransomware automation, crypto-mining fraud*, dan *algorithmic market manipulation*. AI menurunkan biaya operasional dan risiko hukum, sehingga pelaku lebih terdorong mengambil keuntungan tinggi dengan risiko rendah.[24]

b. Motif ideologis

AI juga digunakan oleh kelompok tertentu untuk kepentingan ideologis, seperti hacktivism, spionase digital, atau propaganda politik berbasis information warfare. Fenomena ini menunjukkan bahwa operasi siber tidak lagi semata-mata berorientasi pada keuntungan ekonomi, melainkan juga sebagai instrumen strategis dalam konflik politik dan ideologis, termasuk untuk mempengaruhi opini publik, mendestabilisasi sistem sosial, atau memperkuat kepentingan geopolitik suatu negara.[25] Dalam konteks ini, penggunaan teknologi digital termasuk AI telah memperluas bentuk operasi informasi yang bersifat manipulatif dan persuasif, sebagaimana terlihat dalam model propaganda modern yang memanfaatkan diseminasi informasi secara masif dan berulang. Selain itu, praktik hacktivism dan keterlibatan aktor non-negara dalam konflik siber menunjukkan adanya pergeseran bentuk perlawanan dari yang bersifat fisik menjadi simbolik dan berbasis jaringan digital. Dengan demikian, motif ideologis menandai transformasi kejahatan siber dari sekadar aktivitas kriminal menuju bagian dari information operations dan bahkan instrumen statecraft dalam hubungan internasional.[26]

c. Motif psikologis dan sosial

Motif psikologis dalam kejahatan siber mencakup rasa ingin tahu, kebutuhan akan pengakuan, hingga pencarian sensasi *(thrill-seeking)*, yang sering kali menjadi pendorong utama terutama bagi pelaku non-profesional atau individu muda.[27] Dalam perspektif *control theory*, perilaku menyimpang tersebut terjadi karena lemahnya keterikatan sosial *(social bonds)* seperti hubungan dengan keluarga, institusi pendidikan, atau

nilai-nilai sosial yang seharusnya berfungsi sebagai mekanisme pengendali perilaku individu.[28] Akibatnya, pelaku tidak lagi merasa terikat oleh norma hukum maupun moral yang berlaku. Selain itu, karakteristik dunia maya yang memungkinkan anonimitas memperkuat terjadinya deindividuation effect, yaitu kondisi di mana identitas personal menjadi kabur sehingga individu mengalami penurunan kesadaran diri dan tanggung jawab moral atas tindakannya. Dalam situasi ini, individu cenderung bertindak lebih impulsif dan agresif karena merasa tidak dapat dikenali atau dimintai pertanggungjawaban.[29] Dengan demikian, kombinasi antara faktor psikologis internal dan kondisi sosial dalam ruang digital menciptakan lingkungan yang kondusif bagi munculnya perilaku menyimpang berbasis teknologi.

3. Lingkungan Sosial dan Ekosistem Kriminal Digital

Kejahatan siber berbasis AI tumbuh dalam ekosistem sosial yang berbeda dari kejahatan tradisional. Beberapa faktor lingkungan yang mendukungnya antara lain:

a. Ekonomi digital tidak merata

Ketimpangan akses terhadap sumber daya teknologi menyebabkan munculnya kelompok dengan kemampuan tinggi tetapi peluang ekonomi rendah. Fenomena ini memperkuat teori strain Merton dimana tekanan sosial akibat kesenjangan antara aspirasi dan sarana legal mendorong inovasi menyimpang, salah satunya melalui penggunaan AI secara ilegal.[30]

b. Budaya Anonimitas dan Ketidakhadiran Negara

Ruang siber bersifat tanpa batas geografis dan minim regulasi efektif, sehingga kontrol sosial sulit diterapkan. Negara kesulitan menegakkan hukum lintas yurisdiksi, sementara pelaku memanfaatkan kerahasiaan identitas digital untuk melarikan diri dari tanggung jawab hukum.[31]

c. Normalisasi Penyimpangan Teknologi

Masyarakat digital cenderung mentoleransi bentuk pelanggaran teknologi, seperti modifikasi perangkat lunak atau data scraping. Dalam

jangka panjang, toleransi ini menciptakan budaya deviasi ringan yang berkembang menjadi deviasi sistemik, di mana penyalahgunaan AI dianggap bagian wajar dari eksperimen teknologi.

4. Dinamika Perubahan dalam Pola Kejahatan

Analisis kriminologis menunjukkan adanya perubahan signifikan dalam dinamika kejahatan seiring dengan perkembangan teknologi kecerdasan buatan (AI), yang tidak hanya mengubah modus operandi, tetapi juga struktur, skala, dan distribusi tanggung jawab dalam tindak pidana siber.

a. Dari tindakan manual menuju otomatisasi kriminalitas

AI menghapus kebutuhan keterlibatan langsung manusia dalam setiap tahapan kejahatan, sehingga memungkinkan terjadinya otomatisasi kriminalitas melalui sistem algoritmik yang mampu beroperasi secara mandiri.[32] Dalam konteks ini, pelaku tidak lagi harus melakukan tindakan secara fisik atau langsung, melainkan cukup merancang dan menginisiasi sistem yang kemudian menjalankan aksi secara otonom. Fenomena ini menandai pergeseran dari hands-on crime menuju autonomous cybercrime, di mana kecerdasan buatan berfungsi sebagai perpanjangan sekaligus substitusi dari pelaku manusia.[33]

b. Dari risiko personal menuju risiko terdistribusi

Perkembangan AI juga menggeser distribusi risiko dalam kejahatan, di mana pelaku dapat meminimalkan eksposur pribadi dengan memindahkan sebagian besar risiko kepada sistem digital yang mereka kendalikan.[34] Sementara itu, dampak kejahatan menjadi semakin luas dan terdistribusi, melintasi batas yurisdiksi negara serta berlangsung dalam jangka waktu yang lebih panjang. Hal ini menimbulkan tantangan serius bagi sistem penegakan hukum yang masih berbasis pada konsep yurisdiksi teritorial dan pertanggungjawaban individual.

c. Dari kejahatan individual ke kejahatan sistemik

Dalam era AI, pelaku kejahatan sering kali tidak lagi bertindak secara individual, melainkan sebagai bagian dari networked crime

yang terorganisasi dalam struktur yang menyerupai ekosistem teknologi.[35] Kejahatan menjadi bersifat sistemik karena melibatkan berbagai aktor, perangkat, dan infrastruktur digital yang saling terhubung. Dengan demikian, pendekatan kriminologi klasik yang berfokus pada individu menjadi kurang memadai untuk menjelaskan fenomena ini. Sebaliknya, diperlukan pendekatan interdisipliner yang menggabungkan kriminologi digital, psikologi perilaku, serta teori sistem kompleks untuk memahami dinamika kejahatan berbasis AI secara komprehensif.[36]

## Kesimpulan

Perkembangan kecerdasan buatan (Artificial Intelligence/AI) telah membawa transformasi fundamental dalam pola kejahatan siber, baik dari segi modus operandi, struktur pelaku, maupun distribusi risiko. Penelitian ini menunjukkan bahwa AI tidak lagi sekadar berfungsi sebagai alat bantu, melainkan telah berkembang menjadi sarana kejahatan *(tool of crime)*, objek kejahatan *(object of crime)*, dan bahkan entitas pelaku semu *(virtual offender)* yang menimbulkan persoalan baru dalam hukum pidana, khususnya terkait atribusi pertanggungjawaban. Dari perspektif kriminologi, penyalahgunaan AI dipengaruhi oleh kombinasi faktor individual, struktural, dan kultural, yang meliputi tingginya literasi teknologi pelaku, motif ekonomi dan ideologis, serta lingkungan sosial digital yang ditandai oleh anonimitas, lemahnya kontrol hukum, dan normalisasi penyimpangan teknologi. Selain itu, terjadi pergeseran signifikan dalam dinamika kejahatan, yaitu dari tindakan manual menuju otomatisasi, dari risiko personal menuju risiko terdistribusi, serta dari kejahatan individual menuju kejahatan sistemik berbasis jaringan.

Implikasi dari temuan ini menegaskan bahwa pendekatan hukum pidana konvensional tidak lagi memadai untuk menghadapi kompleksitas kejahatan berbasis AI. Oleh karena itu, diperlukan pembaruan paradigma hukum yang tidak hanya berorientasi pada pemidanaan, tetapi juga pada pencegahan berbasis risiko (*risk governance),* akuntabilitas etis (*ethical accountability*), serta penguatan regulasi yang adaptif terhadap

perkembangan teknologi. Dengan demikian, integrasi antara pendekatan kriminologi, hukum, dan teknologi menjadi kunci dalam merumuskan kebijakan yang mampu melindungi masyarakat sekaligus menjaga nilai-nilai kemanusiaan di era kecerdasan buatan.

## Pustaka Acuan

Asaro, Peter M. "The Liability Problem for Autonomous Artificial Agents." Conf. paper presented pada AAAI Symposium on Ethical and Moral Considerations in Non-Human Agents. 21 Maret 2016. https://cdn.aaai.org/ocs/12699/12699-56141-1-PB.pdf.

Bassiouni, M. Cherif. *Crimes against Humanity: Historical Evolution and Contemporary Application*. Cambridge: Cambridge University Press, 2011.

Biggio, Battista, dan Fabio Roli. "Wild Patterns: Ten Years after the Rise of Adversarial Machine Learning." *Pattern Recognition* 84 (Desember 2018): 317–31. https://doi.org/10.1016/j.patcog.2018.07.023.

Castells, Manuel, dan Manuel Castells. *The Rise of the Network Society*. 2. ed. with a new preface, [Reprint]. The Information Age / Manuel Castells 1. Malden, Mass.: Wiley-Blackwell, 2011.

Chesney, Robert, dan Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *SSRN Electronic Journal* 107, no. 6 (2018): 1753–820. https://doi.org/10.2139/ssrn.3213954.

Clinard, Marshall Barron, dan Peter C. Yeager. *Corporate Crime*. Law and Society. Piscataway: Transaction Publishers, 2005.

"Cohen, Albert K.: Delinquent Boys." Dalam *Encyclopedia of Criminological Theory*, oleh Francis Cullen dan Pamela Wilcox. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2010. https://doi.org/10.4135/9781412959193.n50.

Coleman, E. Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London New York: Verso, 2014.

Cornish, Derek B., ed. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Research in Criminology. New York Heidelberg: Springer [u.a.], 1986.

Crilley, Rhys. "Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know." *Journal of Communication* 69, no. 4 (Agustus 2019): E10–12. https://doi.org/10.1093/joc/jqz017.

European Union Agency for Cybersecurity. *ENISA Threat Landscape*. GR: European Union Agency for Cybersecurity, 2025. https://doi.org/10.2824/2445233.

European Union Agency for Law Enforcement Cooperation. *IOCTA, Internet Organised Crime Threat Assessment 2023*. LU: Publications Office, 2023. https://data.europa.eu/doi/10.2813/587536.

Goodfellow, Ian, Yoshua Bengio, dan Courville Aaron. *Deep Learning*. MT Press, 2016.

Helmus, Todd C. *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*. RAND Corporation, 2022. https://doi.org/10.7249/PEA1043-1.

Hirschi, Travis. *Causes of Delinquency*. First paperback edition, Third printing. Berkley Los Angeles London: University of California Press, 1974.

Holt, Thomas J. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. With Adam M. Bossler. Crime Science Series (Routledge (Firm)) 17. London New York: Routledge, 2016. https://doi.org/10.4324/9781315775944.

Holt, Thomas J., Adam M. Bossler, dan Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. Third edition. London New York: Routledge, 2022.

Hongladarom, Soraj. *Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: New York: Public Affairs, 2019, 704 Pp. ISBN 978-1-61039-569-4 (Hardcover) 978-1-61039-270-0 (Ebook)*. 38 (Desember 2023). https://doi.org/10.1007/s00146-020-01100-0.

Kaspersky. *Incident Response – Kaspersky Analyst Report 2023*. Kaspersky, 2023. https://media.kasperskycontenthub.com/wp-content/uploads/

sites/43/2024/05/13125640/Kaspersky-IR_Analyst_report_2023_EN.pdf?

King, Thomas, Nikita Aggarwal, Mariarosaria Taddeo, dan Luciano Floridi. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *SSRN Electronic Journal*, advance online publication, 2018. https://doi.org/10.2139/ssrn.3183238.

Maras, Marie-Helen. *Cybercriminology*. New York Oxford: Oxford University Press, 2017.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. 1 ed. Cambridge University Press, 2018. https://doi.org/10.1017/9781316422724.

Nopiansyah, Rudi. *Hukum dan Kecerdasan Buatan: Menyongsong Era Baru Dunia Hukum*. 1 ed. Jogjakarta: KBM Indonesia, 2025.

Stryker, Cole, dan Eda Kavlakoglu. "What Is Artificial Intelligence (AI)?" *IBM*, t.t. Diakses 22 Oktober 2025. https://www.ibm.com/think/topics/artificial-intelligence?

Sugistiyoko, Bambang Slamet Eko, dan Aulia Rahman Hakim. *Eksistensi Manusia sebagai Subjek Hukum di Era Kecerdasan Buatan: Kajian Hukum dan Etika untuk Reformasi Regulasi di Indonesia.* 11, no. 2 (Juli 2025): 116–38. https://doi.org/10.36563/yustitiabelen.v11i2.1719.

Sugiura, Lisa. "Industry of Anonymity: Inside the Business of Cybercrime. By Jonathan Lusthaus (Harvard University Press, 2018, 289pp. £31.95 Hb)." *The British Journal of Criminology* 61, no. 5 (September 2021): 1430–32. https://doi.org/10.1093/bjc/azab011.

Suler, John. "The Online Disinhibition Effect." *CyberPsychology & Behavior* 7, no. 3 (Juni 2004): 321–26. https://doi.org/10.1089/1094931041291295.

Taddeo, Mariarosaria, dan Luciano Floridi. "How AI Can Be a Force for Good." *Science* 361, no. 6404 (Agustus 2018): 751–52. https://doi.org/10.1126/science.aat5991.

Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Crime and Society Series. Cambridge: Polity, 2007.

Yar, Majid. *Cybercrime and Society*. 3rd edition. London: SAGE Publications, 2019.