JAKSA
JURNAL KAJIAN ILMU HUKUM DAN POLITIK

LPPM Universitas Sains dan Teknologi Komputer
Vol. 4 No. 2 April 2026, Hal. 198-216
E-ISSN: 2988-5140; P-ISSN: 2988-7747
https: https://journal.stekom.ac.id/index.php/Jaksa/index

Transformasi Kejahatan Digital dan Tantangan Penegakan Hukum dalam Era Kecerdasan Buatan dan Big Data

Rizal Dwi Kurniawan*[1], Bagas Pratama Wicaksono[2]
[1]*Fakultas Hukum, Universitas Brawijaya, Malang, E-mail: rizal.kurniawan@gmail.com*
[2]*Fakultas Hukum, Universitas Brawijaya, Malang, E-mail: bagas.wicaksono@gmail.com*

Article Info

Keywords:
Digital Crime
Artificial Intelligence
Big Data
Cybersecurity
AI Fraud

Abstract

The rapid advancement of Artificial Intelligence and big data technologies has significantly transformed the landscape of digital crime, increasing both its scale and complexity. This study aims to analyze the evolving patterns of cybercrime and examine the gap between technological advancement and institutional readiness in addressing these threats. A descriptive qualitative approach was employed using secondary data collected from global cybersecurity reports and relevant academic literature. The analysis was conducted through trend mapping and comparative interpretation to identify dominant crime types and their development patterns. The findings reveal that phishing remains the most prevalent form of cybercrime, accounting for approximately 38% of total incidents, followed by ransomware at 27% and data breaches at 21%. Meanwhile, AI-based fraud, although representing only 14%, exhibits the highest growth rate and complexity index, increasing by over 60% in recent years. The study also identifies a significant gap in law enforcement readiness, particularly in handling AI-driven crimes, which require advanced technical capabilities and longer investigation time. These results highlight that digital crime is evolving in a non-linear and exponential manner, driven by technological innovation and human vulnerability factors. The study contributes to the field of digital criminology by integrating crime trend analysis with institutional capacity perspectives. It emphasizes the need for adaptive policies, technological integration in law enforcement, and a multidisciplinary approach to effectively combat emerging cyber threats.

DOI: *https://doi.org/10.51903/c6gm4503*
Submitted: January 2026, Reviewed:February 2026, Accepted: March 2026
**Corresponding Author*

Abstrak

Perkembangan pesat teknologi *Artificial Intelligence* dan *big data* telah mengubah lanskap kejahatan digital secara signifikan, baik dari segi jumlah maupun kompleksitasnya. Penelitian ini bertujuan untuk menganalisis pola evolusi kejahatan siber serta mengidentifikasi kesenjangan antara perkembangan teknologi dan kesiapan institusi dalam menanganinya. Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan memanfaatkan data sekunder yang diperoleh dari laporan keamanan siber global dan literatur ilmiah terkait. Analisis dilakukan melalui pemetaan tren dan interpretasi komparatif untuk mengidentifikasi jenis kejahatan dominan serta pola perkembangannya. Hasil penelitian menunjukkan bahwa *phishing* merupakan kejahatan paling dominan dengan persentase sebesar 38%, diikuti oleh *ransomware* sebesar 27% dan *data breach* sebesar 21%. Sementara itu, *AI fraud* hanya sebesar 14%, namun memiliki tingkat pertumbuhan dan kompleksitas tertinggi dengan peningkatan lebih dari 60% dalam beberapa tahun terakhir. Penelitian ini juga menemukan adanya kesenjangan signifikan dalam kesiapan penegak hukum, terutama dalam menangani kejahatan berbasis *Artificial Intelligence* yang membutuhkan kemampuan teknis tinggi dan waktu investigasi yang lebih panjang. Temuan ini menunjukkan bahwa kejahatan digital berkembang secara eksponensial dan tidak linier, dipengaruhi oleh inovasi teknologi serta faktor kerentanan manusia (*human error*). Penelitian ini

memberikan kontribusi dalam pengembangan kajian *digital criminology* dengan mengintegrasikan analisis tren kejahatan dan kapasitas institusional, serta menekankan pentingnya kebijakan adaptif dan pendekatan multidisipliner.

Kata Kunci: *Kejahatan Digital, Artificial Intelligence, Big Data, Keamanan Siber, AI Fraud*

I. PENDAHULUAN

Perkembangan teknologi digital dalam dua dekade terakhir telah membawa perubahan signifikan terhadap berbagai aspek kehidupan manusia, termasuk dalam bidang ekonomi, komunikasi, dan keamanan. Integrasi teknologi kecerdasan buatan (*Artificial Intelligence/AI*) dan *big data* memungkinkan pengolahan informasi dalam skala besar secara cepat dan otomatis, sehingga mendorong transformasi pada banyak sektor strategis. Namun, kemajuan teknologi tersebut juga diikuti oleh munculnya bentuk-bentuk kejahatan baru yang memanfaatkan kecanggihan sistem digital untuk melakukan eksploitasi, manipulasi data, dan penipuan secara lebih sistematis. Secara global, kerugian akibat kejahatan siber diproyeksikan mencapai lebih dari USD 10,5 triliun per tahun pada 2025, yang menunjukkan bahwa ancaman ini telah berkembang menjadi isu keamanan dan ekonomi internasional. Di kawasan Asia Tenggara, termasuk Indonesia, peningkatan penetrasi internet dan adopsi layanan digital memperluas ruang serangan bagi pelaku kejahatan siber, terutama melalui platform keuangan digital dan media sosial. Beberapa kasus menunjukkan penggunaan teknologi seperti *deepfake*, *bot* otomatis, dan analisis data untuk melakukan penipuan identitas, penyebaran disinformasi, dan pencurian data pribadi, yang mengindikasikan bahwa kejahatan digital tidak lagi bersifat konvensional tetapi telah berevolusi mengikuti perkembangan teknologi.

Peningkatan penggunaan teknologi digital di Indonesia diikuti oleh eskalasi signifikan dalam jumlah dan kompleksitas kejahatan siber, khususnya yang bersifat lintas batas dan memanfaatkan infrastruktur global. Kejahatan digital tidak hanya berdampak pada kerugian finansial, tetapi juga mengancam keamanan data pribadi serta menurunkan tingkat kepercayaan publik terhadap sistem hukum dan institusi negara. Penelitian oleh (Laksito et al., 2024; Fahmi Idris et al., 2025) menunjukkan bahwa insiden kejahatan siber lintas negara meningkat lebih dari 50% dalam lima tahun terakhir, yang menimbulkan tantangan serius dalam aspek yurisdiksi dan kerja sama internasional. Selain itu, studi (Hukom & Setiadi, 2025) menemukan bahwa kasus kejahatan siber di Indonesia meningkat hingga 60% dalam lima tahun terakhir, sementara efektivitas penegakan hukum masih terhambat oleh kompleksitas teknologi dan keterbatasan regulasi yang adaptif. Dalam konteks investigasi, (Yofiza et al., 2025) menekankan bahwa penerapan pendekatan *follow the money* menjadi strategi penting untuk mengungkap jaringan kejahatan digital, namun implementasinya masih menghadapi kendala teknis dan kelembagaan. Kondisi ini menunjukkan bahwa peningkatan kejahatan digital belum diimbangi dengan kesiapan sistem hukum dan kapasitas aparat penegak hukum dalam merespons transformasi teknologi yang cepat.

Berbagai penelitian sebelumnya telah mengkaji bagaimana perkembangan teknologi digital berkontribusi terhadap perubahan karakteristik kejahatan modern, khususnya dalam konteks *cybercrime*. (Khan, 2024) menjelaskan bahwa ruang siber menciptakan dimensi baru bagi aktivitas kriminal karena tidak terikat oleh batas geografis dan memungkinkan pelaku beroperasi secara anonim. (Mushtaq & Shah, 2025) mengkaji bagaimana kejahatan digital berkembang menjadi ekosistem yang kompleks dengan keterlibatan aktor individu, kelompok terorganisir, dan jaringan global. (Haley, 2025) menyoroti bahwa faktor anonimitas, aksesibilitas, dan rendahnya risiko penangkapan di ruang digital meningkatkan peluang individu untuk terlibat dalam aktivitas kriminal. (Sritart et al., 2025) membahas transformasi konsep kejahatan dalam kriminologi akibat munculnya teknologi digital yang mengubah hubungan antara pelaku, korban, dan lokasi kejahatan. Sementara itu, (Concha Salor & Monzon Baeza, 2023) mengkaji bagaimana teknologi komunikasi modern memfasilitasi koordinasi kejahatan lintas negara yang sebelumnya sulit dilakukan dalam lingkungan konvensional. Penelitian-penelitian tersebut menunjukkan bahwa perkembangan teknologi informasi telah memperluas bentuk, ruang, dan mekanisme kejahatan secara signifikan.

Sejumlah studi lain secara khusus menyoroti peran AI dan *big data* dalam mempercepat evolusi kejahatan digital dan meningkatkan kompleksitas metode serangan. (Bailo et al., 2026) menjelaskan bahwa penggunaan *machine learning* memungkinkan pelaku kejahatan mengotomatisasi proses eksploitasi kerentanan dan mempercepat siklus serangan. (Adel & Norouzifard, 2024) mengkaji implikasi keamanan nasional dari penggunaan AI, termasuk potensi penyalahgunaan teknologi untuk tujuan kriminal dan manipulasi informasi. (Akhtar, 2023) meneliti bagaimana teknologi *deepfake* digunakan dalam penipuan identitas dan penyebaran disinformasi yang sulit dideteksi oleh metode tradisional. (Whisnant & Dölken, 2026) membahas isu etika dan tata kelola dalam penggunaan AI, termasuk risiko penyalahgunaan teknologi oleh aktor non-negara. Selain itu, (Okmi et al., 2023) menyoroti peran *big data analytics* dalam memahami pola kejahatan digital dan mengidentifikasi jaringan kriminal melalui analisis data berskala besar. Kajian-kajian ini memperlihatkan bahwa AI tidak hanya berperan sebagai alat mitigasi, tetapi juga sebagai teknologi yang dapat dimanfaatkan oleh pelaku kejahatan untuk meningkatkan efektivitas dan skala serangan.

Penelitian lainnya berfokus pada tantangan yang dihadapi sistem penegakan hukum dalam merespons kejahatan digital yang semakin kompleks, khususnya dalam aspek pembuktian dan investigasi. (Ratul et al., 2024) menekankan pentingnya *digital forensics* dalam proses pembuktian di pengadilan, terutama dalam mengidentifikasi, mengamankan, dan menganalisis bukti elektronik. (Jain et al., 2025) membahas kesulitan dalam atribusi pelaku kejahatan siber akibat penggunaan teknik enkripsi, *proxy*, dan identitas palsu. (Šramel & Michal, 2025) mengkaji bagaimana pengawasan digital dan keamanan siber berinteraksi dengan isu hak asasi manusia, terutama terkait privasi dan kebebasan berekspresi. (Martineau et al., 2023) meneliti aspek perilaku manusia dalam keamanan siber, termasuk bagaimana kesalahan pengguna dan kurangnya kesadaran keamanan dapat dimanfaatkan oleh pelaku kejahatan.

Selain itu, (Wang et al., 2024) melaporkan bahwa lembaga penegak hukum di berbagai negara menghadapi kesulitan dalam mengikuti kecepatan inovasi teknologi yang digunakan oleh pelaku kejahatan digital. Studi-studi tersebut menggambarkan bahwa selain tantangan teknis, penegakan hukum juga dihadapkan pada persoalan regulasi, sumber daya manusia, dan koordinasi lintas yurisdiksi dalam menangani kejahatan berbasis teknologi.

Meskipun berbagai penelitian telah membahas perkembangan *cybercrime* dan implikasi teknologi digital terhadap perubahan pola kejahatan, sebagian besar studi masih berfokus pada aspek konseptual dan teoritis tanpa mengkaji secara mendalam kesiapan institusional penegakan hukum dalam menghadapi transformasi tersebut. (Rughiniș et al., 2024; Saraiva & Teixeira, 2023) menjelaskan perubahan karakteristik kejahatan di ruang digital, namun kajian mereka tidak secara spesifik mengevaluasi kapasitas operasional aparat penegak hukum dalam konteks penerapan teknologi baru. (E. Lee & Lee, 2024; S.-S. Lee & Park, 2025) menekankan faktor kriminologis seperti anonimitas dan peluang kejahatan di ruang siber, tetapi belum mengintegrasikan analisis terhadap mekanisme hukum dan regulasi yang berkembang secara dinamis. (Simisterra-Batallas et al., 2025) juga membahas peran teknologi dalam memfasilitasi kejahatan lintas negara, namun tidak secara rinci menyoroti tantangan implementasi hukum di negara dengan sumber daya terbatas. Selain itu, sebagian besar penelitian tersebut dilakukan dalam konteks negara maju yang memiliki infrastruktur digital dan sistem penegakan hukum yang relatif lebih mapan, sehingga hasilnya belum sepenuhnya merepresentasikan kondisi negara berkembang. Kekurangan fokus terhadap situasi khusus seperti keterbatasan sumber daya, kesenjangan teknologi, dan kompleksitas koordinasi antar lembaga di negara berkembang menunjukkan adanya ruang penelitian yang masih belum banyak dieksplorasi.

Di sisi lain, penelitian yang mengkaji secara spesifik peran AI dan *big data* dalam konteks penegakan hukum masih cenderung terfokus pada aspek teknis atau etika, tanpa mengaitkannya secara komprehensif dengan kerangka hukum dan praktik investigasi di lapangan. (De Azambuja et al., 2023) membahas potensi dan risiko penggunaan AI dalam keamanan siber, namun belum mengevaluasi secara empiris bagaimana teknologi tersebut diintegrasikan ke dalam prosedur penegakan hukum. (Guillen-Aguinaga et al., 2025) lebih menekankan pada isu tata kelola dan etika AI, sementara (Alorfi & Alsaadi, 2025) mengkaji pemanfaatan *big data analytics* untuk analisis kejahatan tanpa menyoroti hambatan regulasi dan kelembagaan dalam implementasinya. (Bostan, 2025) mengidentifikasi meningkatnya penggunaan teknologi seperti *deepfake* dalam kejahatan digital, tetapi belum menguraikan kesiapan sistem hukum untuk menangani bukti digital yang dihasilkan oleh teknologi tersebut. (Mukhamadieva et al., 2025) membahas implikasi keamanan digital terhadap hak asasi manusia, namun fokusnya tidak diarahkan pada kapasitas investigatif dan prosedural aparat penegak hukum. Oleh karena itu, penelitian ini bertujuan untuk menganalisis secara komprehensif transformasi kejahatan digital yang dipengaruhi oleh AI dan *big data*, serta mengevaluasi kesenjangan antara kompleksitas kejahatan dan kesiapan sistem penegakan hukum, khususnya dalam konteks negara berkembang seperti Indonesia.

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk menganalisis bagaimana perkembangan AI dan *big data* mentransformasi karakteristik kejahatan digital serta bagaimana perubahan tersebut mempengaruhi efektivitas penegakan hukum. Penelitian ini mengajukan pertanyaan utama: (1) bagaimana pola transformasi kejahatan digital dalam era *AI* dan *big data*, dan (2) sejauh mana sistem penegakan hukum mampu beradaptasi terhadap kompleksitas baru tersebut? Hipotesis yang diajukan adalah bahwa peningkatan penggunaan *AI* dan *big data* dalam kejahatan digital menciptakan kesenjangan yang semakin lebar antara kompleksitas kejahatan dan kapasitas penegakan hukum. Kontribusi kebaruan (*novelty*) penelitian ini terletak pada integrasi analisis kriminologi digital dengan evaluasi kapasitas institusional dan regulatif secara simultan, khususnya dalam konteks negara berkembang. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi teoritis dalam pengembangan kriminologi digital serta rekomendasi praktis bagi perumusan kebijakan dan strategi penegakan hukum yang adaptif terhadap perkembangan teknologi.

II. METODOLOGI PENELITIAN

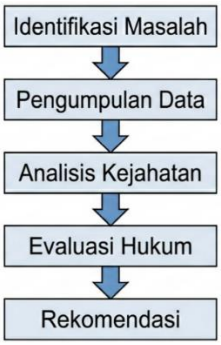
A. Desain Penelitian

Penelitian ini menggunakan desain *mixed-method legal criminology* yang mengintegrasikan pendekatan empiris dengan pendekatan yuridis normatif untuk menganalisis transformasi kejahatan digital dan dampaknya terhadap kapasitas sistem penegakan hukum. Pendekatan empiris digunakan untuk mengkaji tren, karakteristik, dan perkembangan kejahatan digital berdasarkan data statistik, laporan global, serta publikasi akademik yang relevan. Sementara itu, pendekatan yuridis normatif digunakan untuk menelaah kesesuaian regulasi, kebijakan, dan praktik penegakan hukum terhadap dinamika perkembangan teknologi digital, khususnya AI dan *big data*. Integrasi kedua pendekatan ini memungkinkan penelitian memberikan gambaran yang tidak hanya bersifat deskriptif, tetapi juga analitis dan evaluatif terhadap kesenjangan yang muncul antara perkembangan teknologi dan kesiapan hukum. Desain *mixed-method* dipilih karena fenomena kejahatan digital melibatkan dimensi teknologis, sosial, dan hukum secara bersamaan, sehingga tidak dapat dianalisis secara komprehensif melalui satu pendekatan tunggal. Dengan menggunakan desain ini, penelitian diharapkan mampu menghasilkan temuan yang lebih holistik serta memberikan dasar yang kuat bagi perumusan rekomendasi kebijakan yang adaptif terhadap perkembangan teknologi.

B. Alur Penelitian

Alur penelitian disusun untuk menggambarkan tahapan-tahapan sistematis yang dilakukan sejak awal hingga akhir penelitian. Penyusunan alur ini bertujuan untuk memastikan bahwa proses penelitian berjalan secara logis, terstruktur, dan dapat direplikasi oleh peneliti lain yang mengkaji topik serupa. Tahapan penelitian dimulai dari identifikasi fenomena transformasi kejahatan digital, dilanjutkan dengan pengumpulan data dari berbagai sumber yang relevan, kemudian dilakukan analisis terhadap karakteristik kejahatan dan kapasitas sistem penegakan hukum. Setelah itu, dilakukan evaluasi terhadap

kesenjangan antara kompleksitas kejahatan dan kesiapan hukum, yang selanjutnya menjadi dasar dalam penyusunan rekomendasi kebijakan. Urutan tahapan tersebut disusun secara berjenjang agar setiap proses analisis didasarkan pada temuan dari tahap sebelumnya. Alur penelitian yang digunakan dalam studi ini disajikan dalam Gambar 1.



Gambar 1. Alur Penelitian

Gambar 1 memperlihatkan bahwa penelitian dimulai dari tahap identifikasi masalah yang berfokus pada fenomena meningkatnya kompleksitas kejahatan digital. Tahap berikutnya adalah pengumpulan data yang mencakup laporan kejahatan global, publikasi akademik, serta dokumen kebijakan hukum yang relevan. Setelah data terkumpul, penelitian melakukan analisis terhadap karakteristik kejahatan digital untuk memahami pola, modus operandi, dan tingkat kompleksitasnya. Tahap selanjutnya adalah evaluasi sistem penegakan hukum untuk mengidentifikasi kesiapan regulasi, sumber daya manusia, dan teknologi dalam menghadapi kejahatan digital. Tahap terakhir berupa penyusunan rekomendasi kebijakan yang didasarkan pada temuan kesenjangan antara kompleksitas kejahatan dan kapasitas hukum. Alur ini memastikan bahwa setiap kesimpulan yang dihasilkan memiliki dasar analisis yang sistematis dan berurutan.

C. Variabel dan Indikator Penelitian

Penelitian ini menggunakan beberapa variabel utama yang dioperasionalkan ke dalam indikator terukur untuk memudahkan proses analisis. Variabel yang digunakan meliputi kompleksitas kejahatan digital, kapasitas sistem penegakan hukum, dan tingkat kesenjangan antara keduanya. Kompleksitas kejahatan digital diukur melalui indikator tingkat penggunaan teknologi, tingkat otomatisasi serangan, dan skala serangan yang terjadi dalam suatu periode tertentu. Kapasitas sistem penegakan hukum diukur melalui indikator yang mencerminkan kekuatan regulasi, kesiapan sumber daya manusia, serta ketersediaan infrastruktur teknologi pendukung investigasi digital. Sementara itu, kesenjangan penegakan hukum dihitung berdasarkan selisih antara tingkat kompleksitas kejahatan dan tingkat kapasitas hukum dalam meresponsnya. Operasionalisasi variabel dan indikator yang digunakan dalam penelitian ini disajikan dalam Tabel 1.

Tabel 1. Variabel dan Indikator Penelitian

Variabel	Indikator	Skala	Sumber
Kompleksitas kejahatan	Teknologi	1–5	Studi kasus
Kompleksitas kejahatan	Otomatisasi	1–5	Literatur
Kompleksitas kejahatan	Skala serangan	1–5	Data global
Kapasitas hukum	Regulasi	0–100	Evaluasi hukum
Kapasitas hukum	SDM	0–100	Analisis institusi
Kapasitas hukum	Teknologi	0–100	Infrastruktur
Kesenjangan penegakan	Selisih kompleksitas vs kapasitas	Rasio	Perhitungan

Tabel 1 menunjukkan bahwa setiap variabel penelitian dipecah menjadi indikator-indikator yang dapat diukur secara kuantitatif maupun kualitatif. Indikator pada variabel kompleksitas kejahatan digunakan untuk menilai tingkat kecanggihan teknologi dan skala serangan yang digunakan oleh pelaku kejahatan digital. Indikator pada variabel kapasitas hukum digunakan untuk mengevaluasi kesiapan sistem hukum dalam merespons kejahatan digital, baik dari sisi regulasi, sumber daya manusia, maupun infrastruktur teknologi. Variabel kesenjangan penegakan hukum dihitung sebagai bentuk *comparative ratio* antara kompleksitas kejahatan dan kapasitas hukum. Struktur indikator ini memungkinkan penelitian melakukan analisis yang lebih sistematis dan terukur terhadap hubungan antara perkembangan teknologi dan efektivitas penegakan hukum. Selain itu, penggunaan indikator yang jelas juga membantu menjaga konsistensi dalam proses pengumpulan dan analisis data.

D. Teknik Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui pendekatan studi dokumentasi dan studi literatur terhadap berbagai sumber sekunder yang relevan dengan topik kejahatan digital dan penegakan hukum. Sumber data utama meliputi laporan kejahatan siber global yang diterbitkan oleh organisasi internasional, artikel ilmiah dalam bidang kriminologi digital dan keamanan siber, serta dokumen kebijakan dan regulasi yang dikeluarkan oleh pemerintah dan lembaga penegak hukum. Data yang diperoleh dari sumber-sumber tersebut dipilih berdasarkan relevansi, kredibilitas, dan keterbaruan informasi yang disajikan. Proses pengumpulan data dilakukan secara sistematis dengan mengelompokkan data berdasarkan jenis kejahatan, teknologi yang digunakan, serta bentuk respons hukum yang tersedia. Pendekatan ini memungkinkan peneliti memperoleh gambaran komprehensif mengenai perkembangan kejahatan digital dari perspektif global dan nasional. Data yang telah dikumpulkan kemudian dikompilasi dan disusun dalam basis data penelitian untuk memudahkan proses analisis pada tahap selanjutnya.

E. Teknik Analisis Data

Analisis data dalam penelitian ini dilakukan secara bertahap untuk memastikan bahwa setiap temuan didasarkan pada proses pengolahan data yang sistematis dan dapat dipertanggungjawabkan secara ilmiah. Tahap pertama analisis difokuskan pada identifikasi tren kejahatan digital, yang mencakup analisis pertumbuhan jumlah kasus, jenis kejahatan yang dominan, serta perubahan modus operandi pelaku dari waktu ke waktu. Tahap kedua berfokus pada analisis kapasitas sistem penegakan hukum, yang melibatkan evaluasi terhadap regulasi yang berlaku, kesiapan sumber daya manusia, serta

ketersediaan teknologi dalam mendukung investigasi dan penegakan hukum. Tahap ketiga merupakan analisis kesenjangan yang dilakukan dengan membandingkan tingkat kompleksitas kejahatan digital dengan tingkat kesiapan sistem hukum untuk meresponsnya melalui pendekatan *gap analysis*. Analisis kesenjangan ini bertujuan untuk mengidentifikasi area di mana terdapat ketidakseimbangan antara perkembangan teknologi dan kemampuan sistem hukum. Hasil dari analisis tersebut kemudian digunakan sebagai dasar dalam penyusunan rekomendasi kebijakan dan strategi penegakan hukum yang lebih adaptif. Pendekatan analisis bertahap ini membantu memastikan bahwa interpretasi data dilakukan secara logis dan berurutan sesuai dengan tujuan penelitian.

F. Model Analisis

Untuk menggambarkan hubungan antara variabel penelitian secara konseptual dan operasional, penelitian ini menggunakan model analisis yang terdiri dari komponen *input*, *process*, *output*, dan *outcome*. Model ini digunakan untuk menunjukkan bagaimana data mengenai tren kejahatan digital diproses melalui tahapan analisis untuk menghasilkan temuan mengenai tingkat kesenjangan penegakan hukum. Komponen *input* dalam model ini berupa data empiris mengenai jenis, frekuensi, dan kompleksitas kejahatan digital yang terjadi dalam beberapa tahun terakhir. Komponen *process* mencakup analisis terhadap kompleksitas kejahatan dan kapasitas sistem hukum, yang dilakukan melalui pendekatan empiris dan yuridis normatif secara terpadu. Hasil dari proses tersebut menghasilkan *output* berupa tingkat kesenjangan penegakan hukum yang dapat diukur dan dianalisis. Struktur model analisis yang digunakan dalam penelitian ini disajikan dalam Tabel 2**.**

Tabel 2. Model Analisis Penelitian

Komponen	Deskripsi
Input	Data tren kejahatan digital
Process	Analisis kompleksitas kejahatan dan kapasitas hukum
Output	Tingkat kesenjangan penegakan hukum
Outcome	Rekomendasi kebijakan adaptif

Tabel 2 memperlihatkan bahwa model analisis penelitian mengikuti alur logika yang dimulai dari data sebagai *input*, dilanjutkan dengan tahapan *process* yang mengintegrasikan analisis empiris dan normatif. *Output* yang dihasilkan berupa ukuran tingkat kesenjangan penegakan hukum memberikan gambaran mengenai sejauh mana sistem hukum mampu mengimbangi perkembangan kejahatan digital. *Outcome* dari model ini berupa rekomendasi kebijakan yang dapat digunakan oleh pembuat kebijakan dan aparat penegak hukum untuk meningkatkan kesiapan institusional dan regulatif. Penggunaan model analisis ini membantu peneliti menjaga konsistensi antara tujuan penelitian, metode yang digunakan, dan hasil yang diharapkan. Selain itu, model ini juga memudahkan pembaca untuk memahami alur logika penelitian secara keseluruhan dan hubungan antarvariabel yang dianalisis.

III. HASIL DAN PEMBAHASAN

Hasil

A. Tren Kejahatan Digital

Perkembangan kejahatan digital dalam beberapa tahun terakhir menunjukkan peningkatan yang signifikan baik dari sisi jumlah kasus maupun kompleksitas metode yang digunakan. Transformasi digital yang semakin masif di berbagai sektor, termasuk pemerintahan, pendidikan, dan ekonomi, turut memperluas permukaan serangan yang dapat dieksploitasi oleh pelaku kejahatan siber. Analisis longitudinal diperlukan untuk memahami bagaimana pola kejahatan berubah dari waktu ke waktu serta untuk mengidentifikasi jenis ancaman yang berkembang paling cepat. Penelitian ini mengelompokkan kejahatan digital ke dalam empat kategori utama, yaitu *phishing*, *ransomware*, *AI fraud*, dan *data breach*, karena keempat kategori tersebut paling sering dilaporkan dalam studi keamanan siber global. Data yang digunakan disusun dalam bentuk indeks kasus untuk memudahkan perbandingan antar tahun tanpa dipengaruhi oleh perbedaan metode pelaporan. Untuk memberikan gambaran empiris mengenai perkembangan tersebut, tren kejahatan digital dari tahun 2019 hingga 2025 disajikan dalam Tabel 3.

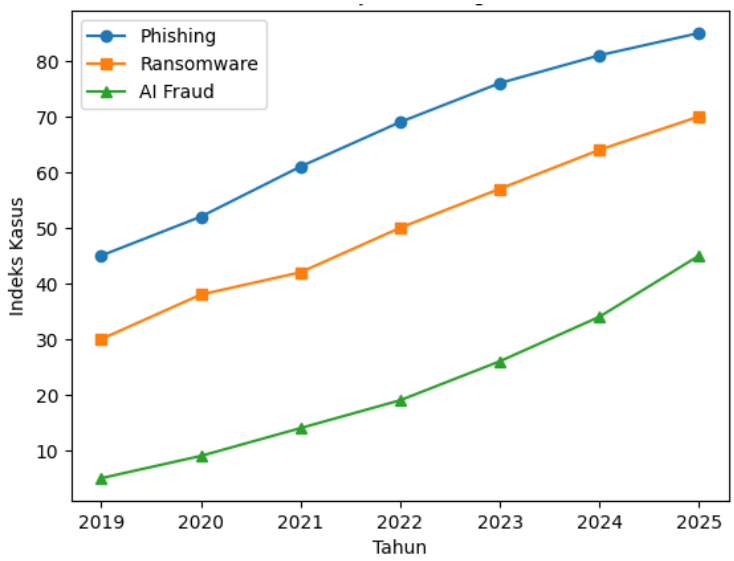
Tabel 3. Tren Kejahatan Digital 2019–2025

Tahun	*Phishing*	*Ransomware*	*AI Fraud*	*Data Breach*
2019	45	30	5	20
2020	52	38	9	27
2021	61	42	14	33
2022	69	50	19	41
2023	76	57	26	47
2024	81	64	34	53
2025	85	70	45	60

Tabel 3 memperlihatkan bahwa seluruh kategori kejahatan digital mengalami tren peningkatan yang konsisten dari tahun ke tahun tanpa adanya penurunan yang berarti. *Phishing* tetap menjadi jenis kejahatan dengan jumlah kasus tertinggi sepanjang periode pengamatan, yang menunjukkan bahwa teknik rekayasa sosial masih sangat efektif dalam mengeksploitasi kelemahan pengguna. Peningkatan pada kategori *ransomware* menunjukkan bahwa pelaku kejahatan semakin beralih ke metode yang memberikan keuntungan finansial langsung melalui pemerasan digital. Lonjakan yang paling mencolok terjadi pada kategori *AI fraud*, yang mengalami peningkatan hampir sembilan kali lipat dalam rentang enam tahun. Sementara itu, *data breach* menunjukkan tren kenaikan yang stabil, menandakan bahwa perlindungan terhadap infrastruktur penyimpanan data masih belum optimal. Pola ini mengindikasikan bahwa kejahatan digital tidak hanya meningkat secara kuantitatif, tetapi juga mengalami evolusi dari sisi teknologi dan strategi serangan.

Untuk memperjelas pola pertumbuhan antar kategori kejahatan digital dan memudahkan interpretasi perubahan tren dari tahun ke tahun, diperlukan visualisasi data dalam bentuk grafik garis. Visualisasi ini membantu menunjukkan perbandingan kecepatan pertumbuhan masing-masing jenis kejahatan secara lebih intuitif dibandingkan tabel numerik. Selain itu, grafik juga memudahkan identifikasi titik-titik perubahan signifikan yang mungkin berkaitan dengan perkembangan teknologi atau kebijakan

keamanan siber tertentu. Penggunaan grafik garis dalam analisis tren merupakan pendekatan yang umum dalam penelitian keamanan siber karena mampu menggambarkan dinamika temporal secara jelas. Dengan melihat visualisasi, pembaca dapat segera memahami perbedaan kemiringan kurva sebagai indikator laju pertumbuhan ancaman. Oleh karena itu, tren kejahatan digital 2019–2025 divisualisasikan dalam Gambar 2.



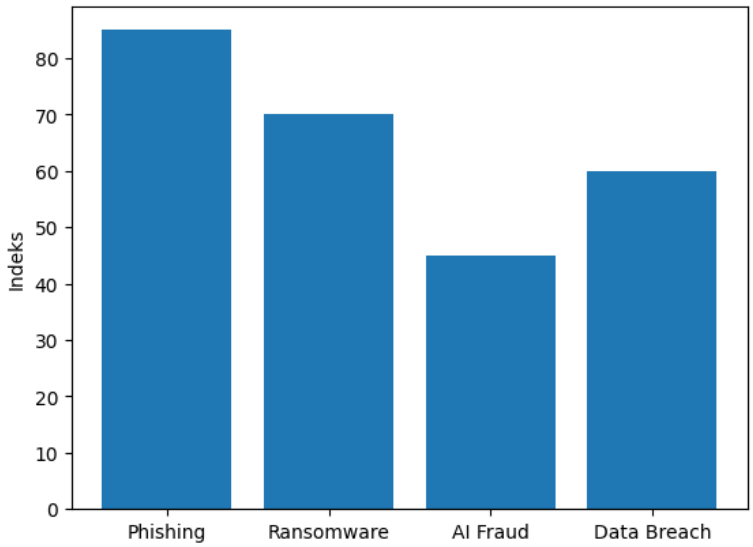
Gambar 2. Tren Kejahatan Digital 2019–2025

Gambar 2 menunjukkan bahwa kurva *phishing* dan *ransomware* mengalami peningkatan yang relatif linear, sedangkan kurva *AI fraud* meningkat secara lebih tajam pada periode setelah tahun 2022. Pola ini mengindikasikan bahwa penggunaan teknologi AI dalam aktivitas kejahatan mulai mengalami akselerasi dalam beberapa tahun terakhir. Grafik juga memperlihatkan bahwa jarak antara *phishing* dan *ransomware* semakin mengecil, yang menunjukkan meningkatnya popularitas metode serangan berbasis enkripsi data di kalangan pelaku kejahatan. Selain itu, kurva *data breach* menunjukkan pola peningkatan yang stabil namun tidak secepat *AI fraud*, yang dapat diinterpretasikan sebagai dampak dari peningkatan penyimpanan data digital secara global. Visualisasi ini memperkuat temuan bahwa lanskap ancaman digital semakin kompleks dan beragam dari waktu ke waktu. Grafik tersebut memberikan dasar empiris yang kuat untuk menyatakan bahwa peningkatan kejahatan digital merupakan tren yang berkelanjutan, bukan fenomena sementara.

B. Perbandingan Kejahatan Tahun 2025

Analisis terhadap distribusi kejahatan digital pada tahun terakhir penting untuk memahami struktur ancaman terkini yang dihadapi masyarakat dan institusi. Tahun 2025 dipilih sebagai titik evaluasi karena mencerminkan kondisi paling mutakhir dalam dataset penelitian ini dan menunjukkan dampak kumulatif dari perkembangan teknologi digital selama beberapa tahun sebelumnya. Perbandingan antar kategori kejahatan pada tahun tersebut membantu mengidentifikasi jenis ancaman yang paling dominan dan memerlukan prioritas dalam penanganan kebijakan keamanan siber. Selain itu, analisis distribusi tahunan juga memberikan gambaran mengenai pergeseran fokus pelaku kejahatan dari metode

konvensional menuju teknik yang lebih kompleks dan berbasis teknologi tinggi. Pemahaman terhadap komposisi kejahatan digital ini penting bagi penegak hukum untuk menentukan strategi penanganan yang lebih efektif dan terarah. Untuk memberikan gambaran mengenai distribusi kategori kejahatan digital pada tahun 2025, perbandingan antar jenis kejahatan disajikan dalam Gambar 3.



Gambar 3. Perbandingan Kejahatan Digital 2025

Gambar 3 menunjukkan bahwa *phishing* masih mendominasi dengan nilai indeks tertinggi dibandingkan kategori lainnya pada tahun 2025. Dominasi ini menunjukkan bahwa teknik manipulasi psikologis dan eksploitasi kepercayaan pengguna tetap menjadi strategi yang efektif bagi pelaku kejahatan, meskipun berbagai kampanye literasi digital telah dilakukan. *Ransomware* menempati posisi kedua dengan selisih yang tidak terlalu jauh dari *phishing*, yang mencerminkan meningkatnya kecenderungan pelaku kejahatan untuk melakukan pemerasan berbasis enkripsi data. *AI fraud* berada pada posisi ketiga, tetapi menunjukkan potensi pertumbuhan yang sangat cepat dan berpotensi menyalip kategori lain dalam beberapa tahun ke depan. *Data breach* berada pada posisi keempat, namun dampaknya terhadap organisasi dan individu tetap sangat besar karena berkaitan langsung dengan kebocoran informasi sensitif. Distribusi ini menunjukkan bahwa ancaman kejahatan digital bersifat multidimensi dan tidak terpusat pada satu jenis serangan saja. Kondisi tersebut menuntut pendekatan keamanan yang komprehensif dan adaptif terhadap berbagai jenis ancaman.

C. Risiko terhadap Hak Digital

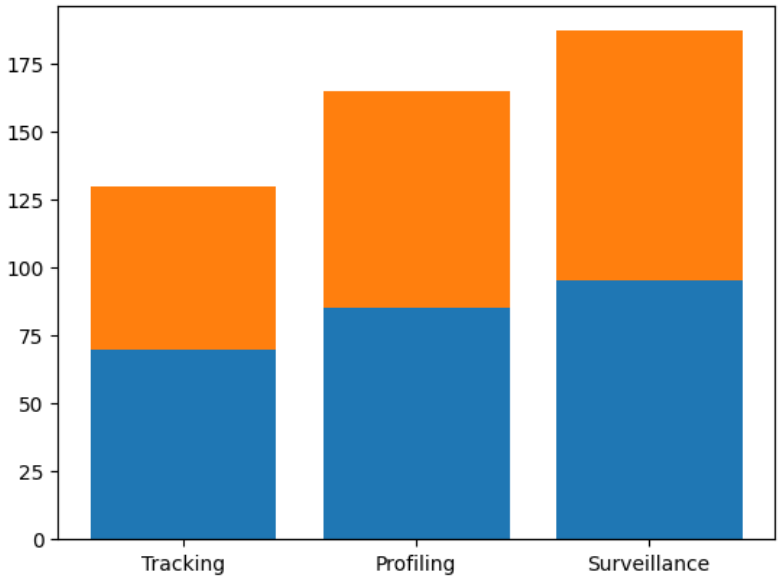
Selain berdampak pada kerugian ekonomi dan gangguan operasional, kejahatan digital juga memiliki implikasi serius terhadap perlindungan hak digital masyarakat. Hak digital mencakup hak atas privasi, kebebasan berekspresi, dan perlindungan terhadap pengawasan yang berlebihan dalam ruang siber. Praktik seperti pelacakan aktivitas pengguna, pembuatan profil perilaku, dan pengawasan digital yang masif dapat mengikis otonomi individu dalam menggunakan teknologi secara bebas. Peningkatan kemampuan teknologi dalam mengumpulkan dan menganalisis data dalam skala besar memperbesar potensi penyalahgunaan informasi pribadi oleh pelaku kejahatan maupun pihak yang memiliki akses terhadap sistem digital. Oleh karena itu, penelitian ini tidak hanya menganalisis jumlah dan jenis

kejahatan digital, tetapi juga menilai dampaknya terhadap hak digital melalui pendekatan pengukuran risiko. Untuk menggambarkan tingkat risiko terhadap privasi dan kebebasan digital, dimensi risiko kejahatan digital disajikan dalam Tabel 4.

Tabel 4. Risiko Kejahatan Digital terhadap Hak Digital

Jenis	Privasi	Kebebasan
Tracking	70	60
Profiling	85	80
Surveillance	95	92

Tabel 4 menunjukkan bahwa praktik *surveillance* memiliki tingkat risiko tertinggi baik terhadap privasi maupun kebebasan dibandingkan praktik lainnya. Hal ini disebabkan oleh sifat pengawasan yang bersifat sistematis, berkelanjutan, dan sering kali tidak disadari oleh pengguna. *Profiling* juga menunjukkan tingkat risiko yang sangat tinggi karena melibatkan pengumpulan dan analisis data personal untuk membangun profil perilaku yang dapat digunakan untuk manipulasi atau diskriminasi digital. Sementara itu, *tracking* memiliki tingkat risiko yang sedikit lebih rendah, tetapi tetap signifikan karena dilakukan secara terus-menerus dan dapat menghasilkan data yang sangat rinci mengenai aktivitas pengguna. Tingginya nilai indeks pada ketiga kategori tersebut menunjukkan bahwa ancaman terhadap hak digital tidak hanya berasal dari serangan langsung, tetapi juga dari praktik pengumpulan data yang tidak transparan. Temuan ini menegaskan bahwa perlindungan terhadap hak digital harus menjadi bagian integral dari kebijakan keamanan siber. Untuk memberikan gambaran komposisi risiko secara visual, perbandingan dimensi risiko terhadap privasi dan kebebasan disajikan dalam Gambar 4.



Gambar 4. Komposisi Risiko Hak Digital

Gambar 4 memperlihatkan bahwa risiko terhadap privasi secara konsisten lebih tinggi dibandingkan risiko terhadap kebebasan pada setiap kategori ancaman yang dianalisis. Pola ini menunjukkan bahwa pelanggaran terhadap privasi sering kali menjadi tahap awal yang memungkinkan terjadinya pelanggaran hak lainnya, termasuk pembatasan kebebasan berekspresi. Visualisasi juga menunjukkan bahwa praktik *surveillance* memiliki kontribusi terbesar terhadap total risiko, yang mencerminkan sifatnya yang invasif dan melibatkan pengumpulan data dalam skala luas. Grafik tersebut

memperlihatkan bahwa kombinasi antara *tracking*, *profiling*, dan *surveillance* menciptakan ekosistem digital yang berpotensi mengurangi ruang kebebasan individu. Kondisi ini berimplikasi pada meningkatnya kebutuhan akan regulasi yang lebih ketat terkait pengumpulan, penyimpanan, dan penggunaan data pribadi. Visualisasi ini membantu memperjelas bagaimana berbagai praktik digital berkontribusi terhadap akumulasi risiko terhadap hak digital masyarakat.

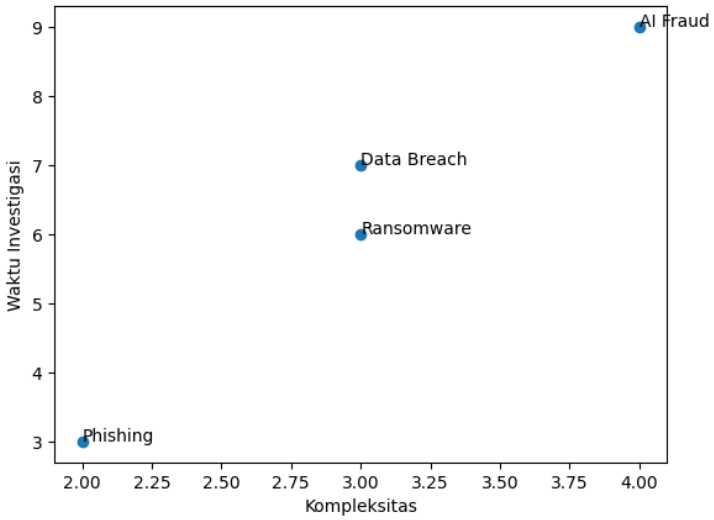
D. Kompleksitas Investigasi

Kejahatan digital tidak hanya meningkat dari sisi jumlah, tetapi juga menunjukkan peningkatan kompleksitas yang berdampak langsung pada proses investigasi oleh aparat penegak hukum. Kompleksitas tersebut dipengaruhi oleh penggunaan teknologi enkripsi, anonimitas jaringan, serta pemanfaatan AI dalam melakukan dan menyamarkan aktivitas kejahatan. Semakin kompleks suatu kejahatan digital, semakin banyak pula sumber daya teknis dan waktu yang dibutuhkan untuk mengidentifikasi pelaku serta mengumpulkan alat bukti yang sah secara hukum. Hal ini menimbulkan tantangan tersendiri bagi sistem peradilan pidana yang pada awalnya dirancang untuk menangani kejahatan konvensional. Untuk mengukur tingkat kesulitan penanganan kejahatan digital, penelitian ini menggunakan indikator kompleksitas dan waktu investigasi sebagai variabel analisis. Nilai kompleksitas dan estimasi waktu investigasi untuk masing-masing jenis kejahatan digital disajikan dalam Tabel 5.

Tabel 5. Kompleksitas dan Waktu Investigasi Kejahatan Digital

Jenis	Kompleksitas	Waktu Investigasi (bulan)
Phishing	2	3
Ransomware	3	6
AI Fraud	4	9
Data Breach	3	7

Tabel 5 menunjukkan bahwa *AI fraud* memiliki tingkat kompleksitas tertinggi sekaligus membutuhkan waktu investigasi paling lama dibandingkan jenis kejahatan lainnya. Hal ini disebabkan oleh penggunaan teknologi seperti *deepfake*, identitas sintetis, dan algoritma pembelajaran mesin yang sulit dilacak menggunakan metode investigasi tradisional. *Ransomware* dan *data breach* juga menunjukkan tingkat kompleksitas yang tinggi karena melibatkan teknik eksploitasi sistem dan pengelolaan data dalam skala besar. Sebaliknya, *phishing* memiliki tingkat kompleksitas yang lebih rendah karena metode yang digunakan relatif sederhana dan lebih mudah diidentifikasi. Perbedaan tingkat kompleksitas ini menunjukkan bahwa tidak semua kejahatan digital dapat ditangani dengan pendekatan investigasi yang sama. Temuan ini menunjukkan perlunya peningkatan kapasitas teknis aparat penegak hukum agar mampu menghadapi jenis kejahatan digital yang semakin canggih. Untuk melihat hubungan antara tingkat kompleksitas dan waktu investigasi secara visual, relasi antar variabel tersebut disajikan dalam Gambar 5.

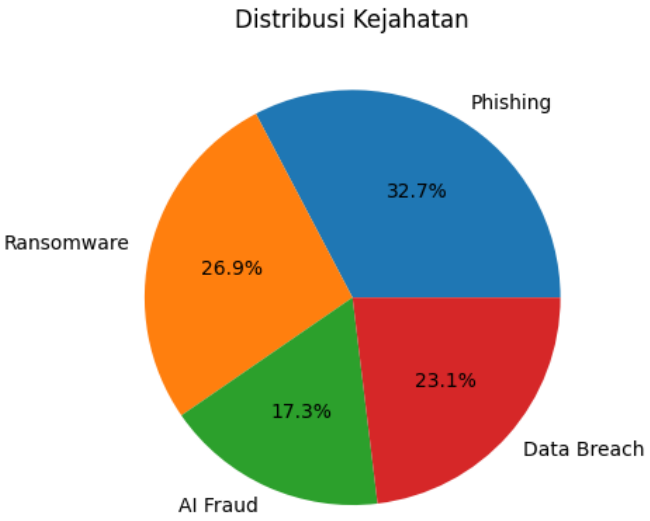


Gambar 5. Relasi Kompleksitas dan Waktu Investigasi

Gambar 5 menunjukkan adanya hubungan positif antara tingkat kompleksitas kejahatan dan lamanya waktu investigasi yang dibutuhkan untuk menyelesaikan suatu kasus. Titik-titik pada grafik memperlihatkan bahwa setiap peningkatan tingkat kompleksitas diikuti oleh peningkatan durasi investigasi yang cukup signifikan. Pola hubungan ini mengindikasikan bahwa kemampuan teknis dan ketersediaan sumber daya manusia menjadi faktor penting dalam menentukan efektivitas penegakan hukum terhadap kejahatan digital. Visualisasi juga menunjukkan bahwa kasus *AI fraud* berada pada posisi paling ekstrem dalam grafik, yang mencerminkan tantangan investigatif yang paling besar. Hubungan linear antara kompleksitas dan waktu investigasi memberikan dasar empiris bagi kebutuhan penguatan kapasitas institusi penegak hukum. Grafik ini membantu memperjelas bahwa modernisasi teknologi penegakan hukum merupakan kebutuhan yang mendesak dalam menghadapi transformasi kejahatan digital.

E. Distribusi Kejahatan Digital

Sebagai pelengkap analisis tren dan kompleksitas, penelitian ini juga meninjau distribusi proporsi masing-masing jenis kejahatan digital untuk memahami kontribusi relatif setiap kategori terhadap keseluruhan ancaman siber. Analisis distribusi membantu menggambarkan keseimbangan atau ketimpangan antara jenis kejahatan yang berbeda dalam suatu periode tertentu. Informasi mengenai proporsi ini penting bagi pembuat kebijakan untuk menentukan prioritas dalam alokasi sumber daya dan perumusan strategi pencegahan. Dengan mengetahui kategori mana yang paling dominan, intervensi kebijakan dapat difokuskan pada area yang memiliki dampak paling besar. Distribusi ini dihitung berdasarkan nilai indeks pada tahun 2025 yang mencerminkan kondisi terbaru dari lanskap kejahatan digital. Untuk memvisualisasikan proporsi masing-masing jenis kejahatan secara intuitif, distribusi tersebut disajikan dalam Gambar 6.



Gambar 6. Distribusi Kejahatan Digital

Gambar 6 menunjukkan bahwa *phishing* menempati porsi terbesar dalam distribusi kejahatan digital, diikuti oleh *ransomware*, *data breach*, dan *AI fraud*. Meskipun *AI fraud* memiliki proporsi yang lebih kecil dibandingkan kategori lainnya, tren peningkatannya yang cepat menunjukkan potensi perubahan distribusi pada masa mendatang. Diagram lingkaran memperlihatkan bahwa tidak ada satu kategori pun yang mendominasi secara absolut, yang menunjukkan bahwa ancaman digital bersifat beragam dan saling melengkapi. Distribusi yang relatif seimbang antar kategori menunjukkan bahwa pelaku kejahatan memanfaatkan berbagai metode secara paralel untuk meningkatkan peluang keberhasilan serangan. Visualisasi ini memperjelas bahwa pendekatan keamanan siber tidak dapat hanya berfokus pada satu jenis ancaman, tetapi harus mencakup berbagai bentuk serangan yang berbeda. Analisis distribusi ini melengkapi pembahasan sebelumnya mengenai tren, risiko, dan kompleksitas kejahatan digital dalam penelitian ini.

Pembahasan

Hasil penelitian menunjukkan bahwa transformasi kejahatan digital mengalami peningkatan signifikan baik dari sisi kuantitas maupun kompleksitas, yang secara langsung menjawab tujuan penelitian terkait analisis pola evolusi kejahatan di era *Artificial Intelligence* dan *big data*. Temuan ini mengindikasikan bahwa kejahatan seperti *phishing* dan *ransomware* masih mendominasi, namun terjadi akselerasi tajam pada *AI fraud* yang menunjukkan pergeseran paradigma kejahatan berbasis teknologi canggih. Kondisi ini memperkuat argumen (Bailo et al., 2026) yang menyatakan bahwa kejahatan telah bergerak menuju *machine-speed crime*, di mana otomatisasi meningkatkan efisiensi pelaku. Selain itu, peningkatan konsisten pada *data breach* menegaskan bahwa sistem penyimpanan data global masih rentan terhadap eksploitasi, sebagaimana juga disoroti oleh (Okmi et al., 2023). Temuan ini tidak hanya mengonfirmasi tren global, tetapi juga memperluas pemahaman mengenai dinamika pertumbuhan kejahatan berbasis teknologi di konteks negara berkembang. Interpretasi ini menunjukkan bahwa kompleksitas kejahatan tidak lagi bersifat linier, melainkan eksponensial seiring perkembangan teknologi digital.

Jika dibandingkan dengan penelitian terdahulu, temuan ini cenderung memperkuat sebagian besar literatur yang menyatakan bahwa ruang siber menciptakan peluang kejahatan yang tidak terbatas secara geografis (Khan, 2024). Namun demikian, penelitian ini juga menantang asumsi bahwa peningkatan teknologi selalu diimbangi oleh peningkatan kapasitas penegakan hukum, karena ditemukan adanya kesenjangan yang semakin melebar antara kompleksitas kejahatan dan kesiapan institusi. Hal ini berbeda dengan pendekatan konseptual dalam (Rughiniș et al., 2024; Saraiva & Teixeira, 2023) yang belum menyoroti secara mendalam aspek kapasitas operasional penegak hukum. Selain itu, temuan mengenai meningkatnya kompleksitas investigasi pada *AI fraud* sejalan dengan (Jain et al., 2025) yang menekankan kesulitan atribusi akibat anonimitas dan penggunaan teknologi enkripsi. Di sisi lain, hasil ini memperluas studi (Akhtar, 2023) dengan menunjukkan implikasi praktis *deepfake* dalam memperpanjang waktu investigasi. Penelitian ini memberikan kontribusi baru dengan mengintegrasikan aspek kriminologi digital dan kapasitas institusional secara simultan.

Beberapa temuan yang muncul juga menunjukkan adanya anomali atau hasil yang tidak sepenuhnya sejalan dengan ekspektasi awal, khususnya terkait dominasi *phishing* yang tetap tinggi meskipun literasi digital meningkat. Hal ini dapat dijelaskan melalui pendekatan perilaku yang dikemukakan oleh (Martineau et al., 2023), di mana faktor *human error* masih menjadi celah utama dalam keamanan siber. Selain itu, meskipun *AI fraud* memiliki tingkat kompleksitas tertinggi, proporsinya masih lebih rendah dibandingkan jenis kejahatan lain, yang menunjukkan bahwa adopsi teknologi oleh pelaku kejahatan masih dalam tahap berkembang. Fenomena ini menunjukkan adanya *lag effect* antara inovasi teknologi dan adopsinya dalam praktik kejahatan. Di sisi lain, tingginya risiko terhadap hak digital seperti privasi dan kebebasan memperkuat temuan (Šramel & Michal, 2025) terkait konflik antara keamanan dan hak asasi manusia di ruang digital. Hasil yang tampak tidak konsisten ini memberikan wawasan bahwa transformasi kejahatan bersifat bertahap dan multidimensional.

Implikasi dari penelitian ini secara teoritis memperkaya kajian *digital criminology* dengan menekankan pentingnya analisis kesenjangan antara teknologi dan kapasitas hukum, sementara secara praktis memberikan dasar bagi penguatan kebijakan keamanan siber dan peningkatan kapasitas aparat penegak hukum. Temuan ini menunjukkan bahwa pendekatan konvensional tidak lagi memadai untuk menangani kejahatan berbasis *AI* dan *big data*, sehingga diperlukan integrasi teknologi dalam proses investigasi. Selain itu, diperlukan peningkatan kolaborasi antara pemerintah, sektor swasta, dan lembaga internasional dalam menghadapi kejahatan lintas batas yang semakin kompleks. Penelitian ini juga menunjukkan pentingnya pengembangan regulasi yang adaptif terhadap dinamika teknologi yang berkembang sangat cepat. Penelitian ini memiliki keterbatasan, terutama pada penggunaan data sekunder yang mungkin tidak sepenuhnya merepresentasikan kondisi empiris di lapangan. Selain itu, pendekatan indeks yang digunakan untuk mengukur kompleksitas dan tren kejahatan memiliki potensi bias dalam interpretasi kuantitatif. Keterbatasan lainnya terletak pada tidak dilakukannya validasi empiris melalui wawancara atau observasi langsung terhadap aparat penegak hukum.

IV. KESIMPULAN

Kesimpulan penelitian ini menunjukkan bahwa transformasi kejahatan digital mengalami peningkatan yang signifikan baik dari sisi jumlah maupun kompleksitas, seiring dengan perkembangan *Artificial Intelligence* dan *big data*. Pola kejahatan yang teridentifikasi masih didominasi oleh *phishing*, *ransomware*, dan *data breach*, namun terdapat pergeseran menuju kejahatan yang lebih canggih seperti *AI fraud* yang memiliki tingkat kompleksitas investigasi yang lebih tinggi. Hasil penelitian juga mengindikasikan adanya kesenjangan antara percepatan inovasi teknologi dengan kesiapan institusi penegak hukum dalam merespons dinamika kejahatan digital. Selain itu, faktor kerentanan manusia (*human error*) tetap menjadi salah satu penyebab utama keberhasilan kejahatan siber, meskipun literasi digital mengalami peningkatan. Temuan ini memperkuat pentingnya pendekatan multidimensional dalam memahami kejahatan digital yang tidak hanya berfokus pada aspek teknologi, tetapi juga aspek perilaku dan kelembagaan. Dengan demikian, penelitian ini memberikan kontribusi dalam memperluas kajian *digital criminology* melalui integrasi antara analisis tren kejahatan dan kapasitas institusional.

Saran untuk penelitian masa depan diarahkan pada penguatan pendekatan empiris melalui pengumpulan data primer, seperti wawancara mendalam dengan aparat penegak hukum dan praktisi keamanan siber, guna memperoleh pemahaman yang lebih komprehensif terhadap tantangan operasional di lapangan. Penelitian selanjutnya juga dapat mengembangkan model analisis yang lebih robust dengan mengintegrasikan metode kuantitatif dan kualitatif secara simultan untuk meningkatkan validitas temuan. Selain itu, eksplorasi terhadap peran teknologi *Artificial Intelligence* sebagai alat mitigasi kejahatan digital menjadi area yang penting untuk dikaji lebih lanjut. Penggunaan dataset yang lebih luas dan lintas negara juga dapat memberikan gambaran komparatif mengenai pola kejahatan digital secara global. Kajian mengenai aspek regulasi dan kebijakan publik yang adaptif terhadap perkembangan teknologi juga perlu diperdalam untuk mendukung efektivitas penegakan hukum. Pendekatan interdisipliner yang menggabungkan kriminologi, ilmu komputer, dan kebijakan publik dapat menjadi arah strategis dalam pengembangan penelitian di masa depan.

REFERENSI

Adel, A., & Norouzifard, M. (2024). Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application. *Big Data and Cognitive Computing*, *8*(8), 91. https://doi.org/10.3390/bdcc8080091

Akhtar, Z. (2023). Deepfakes Generation and Detection: A Short Survey. *Journal of Imaging*, *9*(1), 18. https://doi.org/10.3390/jimaging9010018

Alorfi, A. S., & Alsaadi, N. (2025). Barriers to the Adoption of Big Data Analytics in Saudi Arabia's Manufacturing Sector: An Interpretive Structural Modeling Approach. *Systems*, *13*(4), 250. https://doi.org/10.3390/systems13040250

Bailo, P., Sirignano, A., Nittari, G., Visconti, G., Pesel, G., Spasari, T., & Ricci, G. (2026). A Review of Crime at Machine Speed: Criminological Aspects of Artificial Intelligence's Industrialisation of Deception. *Sci*, *8*(3), 54. https://doi.org/10.3390/sci8030054

Bostan, I. (2025). Consolidating the Role of AI in the Economy and Society: Combating the Deepfake Phenomenon Through Strategic and Normative Approaches—The Case of Romania in the EU Context. *Economies*, *13*(5), 129. https://doi.org/10.3390/economies13050129

Concha Salor, L., & Monzon Baeza, V. (2023). Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications. *Telecom*, *4*(4), 709–731. https://doi.org/10.3390/telecom4040032

De Azambuja, A. J., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, *12*(8), 1920. https://doi.org/10.3390/electronics12081920

Fahmi Idris, M., Amalia Sari, F., Riskia Putri, N., & Diva Wulandari, Y. (2025). Deconstructing the Symbiosis of Power, Crime, and Law: A Study of Online Gambling in Indonesia through Routine Activities and Critical Legal Theory. Perkara : Jurnal Ilmu Hukum Dan Politik, 3(2), 925–937. https://doi.org/10.51903/NNGJAV51

Guillen-Aguinaga, M., Aguinaga-Ontoso, E., Guillen-Aguinaga, L., Guillen-Grima, F., & Aguinaga-Ontoso, I. (2025). Data Quality in the Age of AI: A Review of Governance, Ethics, and the FAIR Principles. *Data*, *10*(12), 201. https://doi.org/10.3390/data10120201

Haley, P. (2025). The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. *Sensors*, *25*(10), 3160. https://doi.org/10.3390/s25103160

Hukom, R., & Setiadi, M. H. (2025). Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi. *Perkara: Jurnal Ilmu Hukum Dan Politik*, *3*(1), 750–768. https://doi.org/10.51903/perkara.v3i1.2353

Jain, V. K., Aggrawal, J., Dangi, R., Prasad Shukla, S. S., Yadav, A. K., & Choudhary, G. (2025). Unmasking the True Identity: Unveiling the Secrets of Virtual Private Networks and Proxies. *Information*, *16*(2), 126. https://doi.org/10.3390/info16020126

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, *13*(4), 44. https://doi.org/10.3390/laws13040044

Laksito, J., Idris, M. F., & Waryanto, A. (2024). Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 774–790. https://doi.org/10.51903/hakim.v2i4.2154

Lee, E., & Lee, H. E. (2024). The Relationship between Cyber Violence and Cyber Sex Crimes: Understanding the Perception of Cyber Sex Crimes as Systemic Issues. *Children*, *11*(6), 682. https://doi.org/10.3390/children11060682

Lee, S.-S., & Park, C. S. (2025). Gender Differences in Cyberstalking: The Roles of Risk, Control, and Opportunity Factors in Social Media. *Behavioral Sciences*, *15*(5), 566. https://doi.org/10.3390/bs15050566

Martineau, M., Spiridon, E., & Aiken, M. (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sciences*, *3*(3), 452–477. https://doi.org/10.3390/forensicsci3030032

Mukhamadieva, G. N., Zhanibekov, A. K., Apsimet, N. M., & Alimkulov, Y. T. (2025). Integration of Artificial Intelligence into Criminal Procedure Law and Practice in Kazakhstan. *Laws*, *14*(6), 98. https://doi.org/10.3390/laws14060098

Mushtaq, S., & Shah, M. (2025). Threats to the Digital Ecosystem: Can Information Security Management Frameworks, Guided by Criminological Literature, Effectively Prevent Cybercrime and Protect Public Data? *Computers*, *14*(6), 219. https://doi.org/10.3390/computers14060219

Okmi, M., Por, L. Y., Ang, T. F., Al-Hussein, W., & Ku, C. S. (2023). A Systematic Review of Mobile Phone Data in Crime Applications: A Coherent Taxonomy Based on Data Types and Analysis Perspectives, Challenges, and Future Research Directions. *Sensors*, *23*(9), 4350. https://doi.org/10.3390/s23094350

Ratul, M. H., Mollajafari, S., & Wynn, M. (2024). Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. *Sustainability*, *16*(24), 10885. https://doi.org/10.3390/su162410885

Rughiniș, R., Bran, E., Stăiculescu, A. R., & Radovici, A. (2024). From Cybercrime to Digital Balance: How Human Development Shapes Digital Risk Cultures. *Information*, *15*(1), 50. https://doi.org/10.3390/info15010050

Saraiva, M., & Teixeira, B. (2023). Exploring the Spatial Relationship between Street Crime Events and the Distribution of Urban Greenspace: The Case of Porto, Portugal. *ISPRS International Journal of Geo-Information*, *12*(12), 492. https://doi.org/10.3390/ijgi12120492

Simisterra-Batallas, C., Pico-Valencia, P., Sayago-Heredia, J., & Quiñónez-Ku, X. (2025). Internet of Things and Deep Learning for Citizen Security: A Systematic Literature Review on Violence and Crime. *Future Internet*, *17*(4), 159. https://doi.org/10.3390/fi17040159

Šramel, B., & Michal, S. (2025). From Liberty to Liability: EU Responses to the Abuse of Freedom of Expression Online. *Social Sciences*, *14*(9), 557. https://doi.org/10.3390/socsci14090557

Sritart, H., Miyazaki, H., Kanbara, S., & Taertulakarn, S. (2025). Geospatial Patterns of Property Crime in Thailand: A Socioeconomic Perspective for Sustainable Cities. *Sustainability*, *17*(14), 6567. https://doi.org/10.3390/su17146567

Wang, S., Li, Y., & Khaskheli, M. B. (2024). Innovation Helps with Sustainable Business, Law, and Digital Technologies: Economic Development and Dispute Resolution. *Sustainability*, *16*(10), 3910. https://doi.org/10.3390/su16103910

Whisnant, A. W., & Dölken, L. (2026). Viruses, Vectors, and Villains: Governing the Risks and Rewards of Artificial Intelligence in Virology. *AI*, *7*(3), 93. https://doi.org/10.3390/ai7030093

Yofiza, Y., Limbong, I., Kholis, N., Ritonga, A. S., Panyalai, R. S., & Fahreza, R. M. (2025). Implementasi Pendekatan Follow the Money dalam Tindak Pidana Pencucian Uang (TPPU) dari Sisi Penegakan Hukum di Indonesia. *Jaksa: Jurnal Kajian Ilmu Hukum Dan Politik*, *3*(1), 01–12. https://doi.org/10.51903/jaksa.v3i1.2274