PERKARA
Jurnal Ilmu Hukum dan Politik

LPPM Universitas Sains dan Teknologi Komputer
Vol. 3 No. 1 Maret 2025, Hal. 750-768
E-ISSN: 2988-5213; P-ISSN: 2988-7747
https://journal.stekom.ac.id/index.php/PERKARA

Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi

Rafli Hukom*[1], Martinus Hukmu Setiadi[2]
[1]*Universitas Darussalam Ambon, Kota Ambon, Maluku, Indonesia, E-mail: rafli.hhkm@gmail.com*
[2]*Universitas Padjadjaran, Kota Bandung, Jawa Barat, Indonesia, E-mail: martinu.hukum@unpad.ac.id*

Article Info
Keywords:
Cybercrime
Social Media
Digital Fraud
Law Enforcement
Regulatory Framework

Abstract
The rapid development of social media has transformed digital crime patterns, enabling financial fraud, exploitation, and radicalization to spread more efficiently. In Indonesia, cybercrime cases have increased by 60% over the past five years, yet law enforcement remains ineffective due to the complexity of digital crime and limited regulatory enforcement. This study aims to analyze how social media facilitates cybercrime, the evolving modus operandi of criminals, and the effectiveness of existing legal frameworks. This research employs a netnographic approach, combining qualitative content analysis of online interactions with secondary data from law enforcement reports. Findings indicate that digital fraud cases have risen by 85% in the past three years, with cryptocurrency-related scams causing losses of IDR 5.2 trillion. Cyberbullying and defamation cases have surged by 60% since 2018, while only 22% of reported cybercrimes have been legally processed, with a conviction rate of just 6%. These figures highlight significant gaps in digital forensic capabilities and cross-sector collaboration. This study contributes to understanding the role of social media in shaping cybercrime and provides policy recommendations to enhance crime prevention strategies. Strengthening legal frameworks, improving law enforcement technology, and fostering cooperation between stakeholders are essential to addressing cybercrime in the digital era. Future research should focus on comparative legal studies and the role of artificial intelligence in cybercrime detection.

DOI: 10.51903/perkara.v3i1.2353
Submitted: January 2025, Reviwed: January 2025, Accepted: February 2025
**Corresponding Author*

I. INTRODUCTION

Dalam beberapa dekade terakhir, perkembangan media sosial telah mengubah lanskap komunikasi global. Platform seperti Facebook, Instagram, Twitter, dan TikTok tidak hanya menjadi ruang interaksi sosial tetapi juga menciptakan ekosistem digital yang memengaruhi berbagai aspek kehidupan, termasuk keamanan dan kejahatan. Laporan dari Statista (2023) menunjukkan bahwa terdapat lebih dari 4,8 miliar pengguna media sosial di seluruh dunia, dengan peningkatan signifikan di Asia Tenggara, termasuk Indonesia. Seiring dengan pertumbuhan ini, laporan dari Interpol (2022) mencatat lonjakan kasus kejahatan digital berbasis media sosial, termasuk penipuan daring, eksploitasi anak, radikalisasi digital, dan pencemaran nama baik. Di Indonesia, Bareskrim Polri melaporkan peningkatan kejahatan siber berbasis media sosial hingga 60% dalam lima tahun terakhir, dengan modus operandi yang semakin

kompleks. Kasus penipuan investasi melalui Instagram dan WhatsApp, serta eksploitasi anak melalui TikTok, menunjukkan bahwa media sosial telah menjadi medan baru bagi berbagai jenis kejahatan yang berkembang seiring dengan digitalisasi masyarakat.

Permasalahan utama dalam penelitian ini adalah bagaimana media sosial berkontribusi terhadap munculnya pola baru dalam kejahatan digital serta bagaimana dinamika interaksi daring memfasilitasi modus operandi pelaku kejahatan. Berbagai penelitian telah mengungkapkan bahwa media sosial memiliki peran signifikan dalam meningkatkan jumlah dan kompleksitas kejahatan digital. Menurut (Mughaid et al., 2023), lebih dari 70% kasus penipuan daring yang dilaporkan di Amerika Serikat dalam lima tahun terakhir terkait dengan aktivitas di platform media sosial, terutama Facebook dan Instagram. Sementara itu, penelitian oleh (Li & Li, 2023) menemukan bahwa 40% kasus eksploitasi anak secara daring terjadi melalui aplikasi pesan instan yang terintegrasi dengan media sosial, memfasilitasi pelaku dalam membangun kepercayaan dengan korban. Di Indonesia, laporan dari Bareskrim Polri (2023) menunjukkan bahwa kasus scam cryptocurrency berbasis media sosial meningkat sebesar 85% dalam tiga tahun terakhir, dengan total kerugian mencapai Rp5,2 triliun. Selain itu, pencemaran nama baik dan ujaran kebencian yang dilakukan melalui media sosial mengalami lonjakan sebesar 60% sejak 2018, mengindikasikan bahwa media sosial tidak hanya menjadi alat komunikasi tetapi juga medium untuk melakukan kejahatan siber. Data ini menunjukkan bahwa meskipun media sosial memberikan manfaat bagi interaksi sosial, ia juga menjadi ekosistem yang kondusif bagi kejahatan digital yang berkembang pesat, menuntut pemahaman lebih dalam mengenai modus operandi pelaku serta strategi mitigasi yang efektif.

Beberapa penelitian terkait dengan pengaruh media sosial terhadap pola kejahatan digital menunjukkan bahwa platform digital telah menjadi alat utama dalam memfasilitasi berbagai bentuk kriminalitas siber. (Izzah et al., 2024) menemukan bahwa anonimitas dalam media sosial memungkinkan pelaku untuk lebih mudah menghindari deteksi, terutama dalam kasus penipuan dan pencemaran nama baik. (Diaz Ruiz & Nilsson, 2023) menunjukkan bahwa penyebaran ujaran kebencian dan disinformasi meningkat secara signifikan melalui algoritma media sosial yang memperkuat konten kontroversial. (Karpova et al., 2022) meneliti bagaimana kelompok ekstremis memanfaatkan media sosial untuk perekrutan anggota baru, menggunakan teknik manipulasi psikologis dan propaganda digital. (Faraz et al., 2024) menemukan bahwa peningkatan eksploitasi anak secara daring berhubungan langsung dengan pertumbuhan aplikasi pesan instan yang memungkinkan komunikasi tanpa pengawasan. (Klopp et al., 2022) membahas bahwa kurangnya regulasi yang ketat di beberapa negara berkembang memperburuk situasi, karena penegakan hukum sulit menjangkau pelaku kejahatan lintas batas.

Penelitian lain juga menunjukkan bahwa perkembangan kejahatan digital di media sosial terus mengalami evolusi seiring dengan meningkatnya keterlibatan pengguna dalam ekosistem digital. (Andriyanto, 2022) mengidentifikasi bahwa modus operandi kejahatan berbasis media sosial semakin kompleks, dengan pelaku yang memanfaatkan identitas palsu dan teknik rekayasa sosial untuk menipu

korban. (Krishnan et al., 2023) meneliti bagaimana penjahat siber menggunakan bot dan akun palsu untuk menyebarkan penipuan investasi, terutama dalam sektor mata uang kripto. (Jain & Gupta, 2022) menemukan bahwa modus phishing di media sosial telah berkembang dengan memanfaatkan fitur iklan berbayar dan tautan yang mengarahkan pengguna ke situs berbahaya. (Moore, 2024) mengungkapkan bahwa praktik perdagangan manusia kini juga difasilitasi oleh media sosial, di mana pelaku merekrut korban melalui iklan pekerjaan palsu. (Jungert et al., 2025) menunjukkan bahwa tren cyberbullying dan doxxing meningkat seiring dengan maraknya penggunaan platform berbasis komunitas, yang sering kali tidak memiliki mekanisme moderasi yang kuat.

Beberapa studi juga telah menyoroti tantangan dalam penegakan hukum terkait kejahatan berbasis media sosial. (Prabhu Kavin et al., 2022) mengungkapkan bahwa meskipun terdapat peningkatan dalam kebijakan keamanan digital, banyak platform media sosial masih gagal dalam mendeteksi dan menindak akun-akun berbahaya secara efektif. (Lusthaus et al., 2023) membahas bahwa kerja sama antara pemerintah dan penyedia layanan media sosial masih terbatas dalam hal pertukaran data untuk investigasi kejahatan digital. (Button et al., 2025) menunjukkan bahwa proses hukum dalam menangani kasus kejahatan media sosial sering kali terhambat oleh kendala yurisdiksi, terutama dalam kasus yang melibatkan aktor lintas negara. (Mensah et al., 2023) meneliti bagaimana banyak korban kejahatan digital tidak melaporkan kasus mereka karena kurangnya kesadaran akan mekanisme hukum yang tersedia. (Pawlicka et al., 2023) membahas bahwa meskipun ada upaya peningkatan literasi digital, masih banyak pengguna media sosial yang tidak memiliki pemahaman cukup mengenai risiko keamanan siber yang dapat mengancam mereka.

Meskipun penelitian sebelumnya telah menyoroti bagaimana media sosial berkontribusi terhadap kejahatan digital, masih terdapat kesenjangan dalam memahami bagaimana pola interaksi daring membentuk modus operandi pelaku kejahatan secara spesifik. (Cross & Layt, 2022) menunjukkan bahwa anonimitas di media sosial mempermudah pelaku dalam melakukan penipuan daring, tetapi penelitian ini belum mengeksplorasi bagaimana interaksi antar pengguna berperan dalam menciptakan pola kejahatan baru. (Mehta & Passi, 2022) mengidentifikasi bahwa algoritma media sosial memperkuat penyebaran ujaran kebencian, namun masih sedikit studi yang menganalisis bagaimana faktor ini berkorelasi dengan peningkatan kejahatan berbasis ideologi radikal. (Hollewell & Longpré, 2021) membahas penggunaan media sosial dalam perekrutan kelompok ekstremis, tetapi tidak menguraikan bagaimana teknik komunikasi daring digunakan untuk membangun jaringan kejahatan yang lebih luas. (Rindestig et al., 2025) menunjukkan bahwa eksploitasi anak berbasis media sosial meningkat, namun masih terbatas penelitian yang membahas bagaimana pola komunikasi daring memfasilitasi pelaku dalam menargetkan korban. (Harkin & Whelan, 2022) meneliti kurangnya regulasi yang efektif terhadap kejahatan digital, tetapi belum membahas sejauh mana pendekatan hukum yang ada mampu menghambat evolusi pola kejahatan di media sosial.

Selain itu, minimnya penelitian yang secara khusus menggunakan pendekatan netnografi dalam menganalisis pola kejahatan berbasis media sosial menjadi kesenjangan utama dalam literatur yang ada. (Langlois et al., 2022) menyoroti kompleksitas modus operandi kejahatan digital, tetapi pendekatan yang digunakan lebih berfokus pada analisis kasus tanpa mempertimbangkan aspek interaksi daring yang terjadi secara real-time. (Su et al., 2024) mengkaji penggunaan akun palsu dalam penipuan investasi, tetapi penelitian ini tidak membahas bagaimana dinamika interaksi antar akun tersebut memengaruhi keputusan korban. (Carroll et al., 2022) menunjukkan bahwa phishing semakin canggih melalui iklan media sosial, namun tidak banyak studi yang meneliti bagaimana pola percakapan daring antara pelaku dan korban berkembang sebelum aksi kejahatan terjadi. (Schroeder et al., 2022) mengungkapkan bahwa media sosial kini digunakan dalam perdagangan manusia, tetapi penelitian ini belum menguraikan secara rinci bagaimana strategi manipulatif digunakan dalam komunikasi daring. (Bacaj et al., 2024) menunjukkan bahwa tren cyberbullying meningkat dengan adanya platform berbasis komunitas, tetapi belum ada analisis yang menghubungkan pola percakapan daring dengan eskalasi kejahatan di dunia nyata. Oleh karena itu, penelitian ini bertujuan untuk menganalisis bagaimana media sosial membentuk pola baru dalam kejahatan digital, memahami modus operandi pelaku dalam memanfaatkan interaksi daring, serta mengevaluasi efektivitas regulasi dalam menangani kejahatan berbasis media sosial menggunakan pendekatan netnografi.

Penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai bagaimana media sosial membentuk pola kejahatan digital serta bagaimana interaksi daring digunakan oleh pelaku dalam menjalankan modus operandi mereka. Dengan menggunakan pendekatan netnografi, penelitian ini akan mengeksplorasi dinamika komunikasi di berbagai platform untuk mengidentifikasi pola perilaku yang berkontribusi terhadap kejahatan berbasis media sosial. Hipotesis utama dalam penelitian ini adalah bahwa semakin tinggi tingkat interaksi dan anonimitas dalam media sosial, semakin besar kemungkinan platform tersebut dimanfaatkan untuk aktivitas kriminal. Selain itu, penelitian ini juga bertujuan untuk mengevaluasi efektivitas regulasi yang ada dalam menangani kejahatan digital, serta mengidentifikasi celah hukum yang masih perlu diperbaiki. Pertanyaan penelitian yang menjadi fokus utama adalah bagaimana pola interaksi daring memfasilitasi kejahatan digital, bagaimana penegakan hukum merespons fenomena ini, serta strategi apa yang dapat diterapkan untuk mengurangi risiko kejahatan berbasis media sosial. Hasil penelitian ini diharapkan dapat memberikan rekomendasi kebijakan yang lebih efektif dalam mengatasi kejahatan digital, sekaligus meningkatkan kesadaran publik terhadap ancaman yang ditimbulkan oleh penyalahgunaan media sosial.

II. METHODOLOGY

A. Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode netnografi, yang berfokus pada analisis interaksi daring dalam media sosial guna memahami pola kejahatan digital yang berkembang. Pendekatan ini memungkinkan peneliti untuk mengamati, mendokumentasikan, dan menganalisis

komunikasi serta perilaku yang terjadi di berbagai platform media sosial, seperti Facebook, Instagram, Twitter, dan TikTok. Studi ini menggabungkan analisis konten digital dan wawancara mendalam untuk mendapatkan pemahaman yang lebih luas tentang bagaimana media sosial digunakan sebagai alat dalam berbagai bentuk kejahatan. Penggunaan metode netnografi memberikan wawasan lebih dalam mengenai bagaimana individu dan kelompok tertentu beroperasi dalam ruang digital untuk menjalankan berbagai bentuk kejahatan, seperti penipuan daring, eksploitasi anak, ujaran kebencian, dan radikalisasi. Selain itu, metode ini memungkinkan penelitian untuk mengidentifikasi pola komunikasi yang digunakan oleh pelaku dalam membangun jaringan kejahatan serta strategi mereka dalam menyamarkan identitas guna menghindari deteksi oleh aparat penegak hukum. Analisis ini dilakukan dengan mengamati interaksi dalam grup diskusi daring, forum komunitas, serta unggahan yang mengindikasikan keterlibatan dalam aktivitas ilegal, sehingga memungkinkan pemetaan pola kejahatan digital yang lebih komprehensif.

B. Populasi dan Sampel

Populasi dalam penelitian ini mencakup konten media sosial yang berkaitan dengan aktivitas kriminal digital, laporan kepolisian terkait kejahatan siber, serta regulasi yang mengatur penggunaan media sosial dalam konteks hukum di Indonesia. Pemilihan populasi ini bertujuan untuk mencakup berbagai sumber informasi yang dapat memberikan gambaran menyeluruh mengenai bagaimana kejahatan digital berkembang di ruang daring. Selain itu, penelitian ini juga mempertimbangkan data dari lembaga yang berwenang, seperti Bareskrim Polri dan Kementerian Komunikasi dan Informatika (Kominfo), yang memiliki rekam jejak dalam menangani kasus kejahatan digital. Sampel penelitian dipilih menggunakan purposive sampling, yang memungkinkan peneliti untuk menyeleksi data yang paling relevan dengan tujuan penelitian. Sampel yang digunakan mencakup konten media sosial yang mengandung unsur kriminal, studi kasus kejahatan digital yang terjadi di Indonesia dalam lima tahun terakhir, wawancara dengan berbagai pihak terkait, serta regulasi yang mengatur penggunaan media sosial dalam perspektif hukum. Kriteria pemilihan sampel ini dirinci dalam Tabel 1, yang mengelompokkan berbagai sumber data yang digunakan dalam penelitian ini.

Tabel 1. Kriteria Sampel Penelitian

Kategori	Keterangan
Konten Media Sosial	Postingan, komentar, atau pesan yang mengandung unsur kejahatan digital
Kasus Kejahatan Digital	Studi kasus kejahatan berbasis media sosial di Indonesia (2018–2023)
Responden Wawancara	Korban, pelaku, pakar kriminologi, dan aparat penegak hukum
Regulasi yang Dikaji	UU ITE, KUHP, serta regulasi internasional tentang kejahatan digital

C. Prosedur Pengumpulan Data

Data dikumpulkan melalui dua sumber utama, yaitu data primer dan data sekunder. Data primer diperoleh melalui berbagai metode yang memungkinkan pengumpulan informasi secara langsung dari sumber yang memiliki relevansi dengan penelitian ini. Salah satu metode utama yang digunakan adalah observasi netnografi terhadap aktivitas kriminal di media sosial, yang mencakup pemantauan interaksi

dalam grup atau forum daring yang memiliki keterkaitan dengan berbagai bentuk kejahatan digital. Observasi ini dilakukan dengan mengamati bagaimana pola komunikasi berkembang dalam komunitas daring yang sering digunakan oleh pelaku kejahatan, termasuk cara mereka merekrut korban, menyebarkan informasi ilegal, atau menyamarkan identitas mereka untuk menghindari deteksi. Selain observasi, data primer juga dikumpulkan melalui wawancara mendalam dengan berbagai pihak yang memiliki keterlibatan langsung maupun tidak langsung dalam kasus kejahatan digital. Wawancara dilakukan dengan korban kejahatan digital untuk memahami pengalaman mereka, dengan pelaku (jika memungkinkan) untuk mengidentifikasi strategi yang mereka gunakan, serta dengan pakar kriminologi dan penyidik siber untuk memperoleh perspektif akademik dan praktis mengenai tren kejahatan di ruang digital. Pendekatan ini memungkinkan penelitian untuk mendapatkan pemahaman yang lebih komprehensif mengenai dinamika interaksi dalam kejahatan digital serta faktor-faktor yang memengaruhi perkembangannya.

Data sekunder diperoleh melalui berbagai sumber yang dapat memberikan informasi tambahan untuk melengkapi hasil yang didapatkan dari data primer. Salah satu sumber utama adalah analisis laporan kepolisian yang mencatat tren kejahatan berbasis media sosial dari tahun 2018 hingga 2023, yang memungkinkan penelitian untuk mengidentifikasi pola peningkatan atau perubahan modus operandi dalam kejahatan digital. Selain laporan kepolisian, penelitian ini juga menggunakan kajian terhadap dokumen hukum yang berkaitan dengan regulasi kejahatan digital, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta berbagai regulasi internasional yang mengatur penggunaan media sosial dan keamanan siber. Kajian terhadap regulasi ini bertujuan untuk menilai efektivitas hukum dalam menanggulangi kejahatan digital serta mengidentifikasi potensi kelemahan dalam sistem hukum yang berlaku. Data sekunder ini juga mencakup laporan dari organisasi non-pemerintah dan lembaga internasional yang menyoroti perkembangan kejahatan digital di berbagai negara, sehingga memungkinkan penelitian untuk melakukan perbandingan terhadap tren global dan melihat bagaimana regulasi di negara lain dapat memberikan wawasan bagi kebijakan di Indonesia. Tabel 2 merangkum berbagai sumber data yang digunakan dalam penelitian ini, memberikan gambaran yang lebih sistematis mengenai jenis informasi yang dikumpulkan dan bagaimana relevansinya terhadap penelitian ini.

Tabel 2. Sumber Data dalam Penelitian

Kategori	Sumber Data
Observasi Netnografi	Konten media sosial, grup diskusi daring
Wawancara	Korban, pelaku, pakar, dan penyidik siber
Dokumen Hukum	UU ITE, KUHP, regulasi internasional
Laporan Kejahatan	Data dari kepolisian, Kominfo, dan NGO

D. Instrumen Penelitian

Instrumen penelitian yang digunakan dalam penelitian ini dirancang untuk mengumpulkan data yang komprehensif terkait dengan dinamika interaksi daring dan kejahatan digital. Salah satu instrumen

utama yang diterapkan adalah pedoman observasi netnografi, yang memungkinkan peneliti untuk menganalisis secara mendalam pola interaksi dan jenis kejahatan yang terjadi di berbagai platform media sosial. Instrumen ini disusun dengan merinci aspek-aspek yang berhubungan dengan perilaku pelaku dan korban dalam konteks kejahatan digital. Selain itu, pedoman wawancara semi-terstruktur digunakan untuk menggali pengalaman korban, memahami modus operandi pelaku, serta mengevaluasi efektivitas penegakan hukum dari sudut pandang praktis dan teoretis. Instrumen wawancara tersebut disusun dengan pertanyaan-pertanyaan yang mampu mengungkap gambaran rinci mengenai pengalaman individu yang terdampak dan memberikan penjelasan mendalam tentang strategi penegakan hukum. Instrumen ketiga, yaitu checklist analisis regulasi, difokuskan pada penilaian kebijakan yang ada dalam mengatasi kejahatan digital berbasis media sosial guna memperoleh evaluasi menyeluruh terhadap efektivitas regulasi yang diterapkan.

E. Prosedur Analisis Data

Prosedur analisis data dalam penelitian ini menggabungkan pendekatan analisis tematik dan perbandingan regulasi untuk mengidentifikasi pola interaksi daring yang berkontribusi terhadap kejahatan digital. Pendekatan analisis tematik digunakan untuk mengelompokkan hasil observasi netnografi ke dalam kategori modus operandi kejahatan digital, sehingga memungkinkan peneliti mengidentifikasi pola komunikasi antara pelaku dan korban secara detail. Proses analisis ini dilakukan dengan menguraikan setiap aspek interaksi yang diamati untuk mengungkap kecenderungan dan tren yang muncul dalam aktivitas kejahatan digital. Selanjutnya, perbandingan regulasi dilaksanakan dengan membandingkan kebijakan dan peraturan terkait kejahatan digital di Indonesia dengan negara lain seperti Amerika Serikat dan Uni Eropa, yang memberikan gambaran tentang praktik terbaik yang telah diterapkan di berbagai yurisdiksi. Pendekatan ini menyediakan kerangka kerja yang komprehensif untuk memahami kelebihan dan kekurangan sistem regulasi yang ada. Tabel 3 disajikan untuk memvisualisasikan perbandingan regulasi kejahatan digital secara rinci, sehingga memberikan gambaran yang jelas mengenai perbedaan dan persamaan antara sistem hukum di berbagai negara.

Tabel 3. Sumber Data dalam Penelitian

Aspek	Indonesia	Amerika Serikat	Uni Eropa
Penegakan Hukum	UU ITE, KUHP	CFAA (Computer Fraud and Abuse Act)	GDPR & ePrivacy Regulation
Sanksi	Denda, penjara	Hukuman berat untuk cybercrime	Regulasi ketat terhadap platform daring
Peran Media Sosial	Moderasi terbatas	Wajib melaporkan kejahatan digital	Wajib menghapus konten ilegal dalam 24 jam

F. Langkah-Langkah Pelaksanaan

Penelitian ini dilaksanakan melalui serangkaian tahap yang terstruktur dengan cermat untuk memperoleh hasil yang komprehensif. Tahap awal melibatkan persiapan penelitian, yang mencakup penyusunan proposal serta pengumpulan literatur yang relevan guna membangun dasar teoretis dan

metodologis yang kuat. Observasi netnografi dilaksanakan untuk mengamati interaksi daring yang berpotensi menjadi bagian dari kejahatan digital, di mana setiap pola komunikasi dianalisis secara mendetail. Proses wawancara mendalam kemudian dilakukan dengan korban, pelaku, dan pakar terkait, yang memungkinkan pengumpulan data kualitatif yang kaya mengenai dinamika kejahatan digital. Selanjutnya, data yang telah dikumpulkan dianalisis menggunakan metode tematik dan perbandingan regulasi untuk menguraikan perbedaan serta persamaan yang muncul di antara kasus-kasus kejahatan digital. Tahap akhir merupakan penyusunan laporan penelitian secara menyeluruh, yang mendokumentasikan temuan-temuan secara sistematis dan mendetail untuk mendukung pengembangan strategi penanggulangan kejahatan digital.

G. Pertimbangan Etis

Penelitian ini mengutamakan pertimbangan etis untuk memastikan seluruh proses pengumpulan dan analisis data dilakukan sesuai standar integritas akademik. Setiap partisipan yang terlibat diberikan informasi lengkap mengenai tujuan serta prosedur penelitian sebelum mengikuti wawancara, dengan pemberian persetujuan informasi secara tertulis sebagai bagian dari proses awal. Perlindungan privasi menjadi prioritas utama, di mana identitas partisipan disamarkan untuk menjaga kerahasiaan data yang diperoleh. Penerapan prinsip etis juga meliputi kepatuhan terhadap kode etik penelitian, khususnya dalam pengelolaan data sensitif yang berkaitan dengan kejahatan digital. Langkah-langkah tersebut diterapkan secara konsisten untuk menjaga keabsahan dan kualitas data yang dikumpulkan sepanjang penelitian. Setiap aspek etis yang dijalankan dalam penelitian ini diuraikan secara mendetail dan direfleksikan melalui penyusunan Tabel 3, yang menyajikan perbandingan regulasi kejahatan digital sebagai salah satu acuan dalam analisis.

III. RESULT AND DISCUSSION

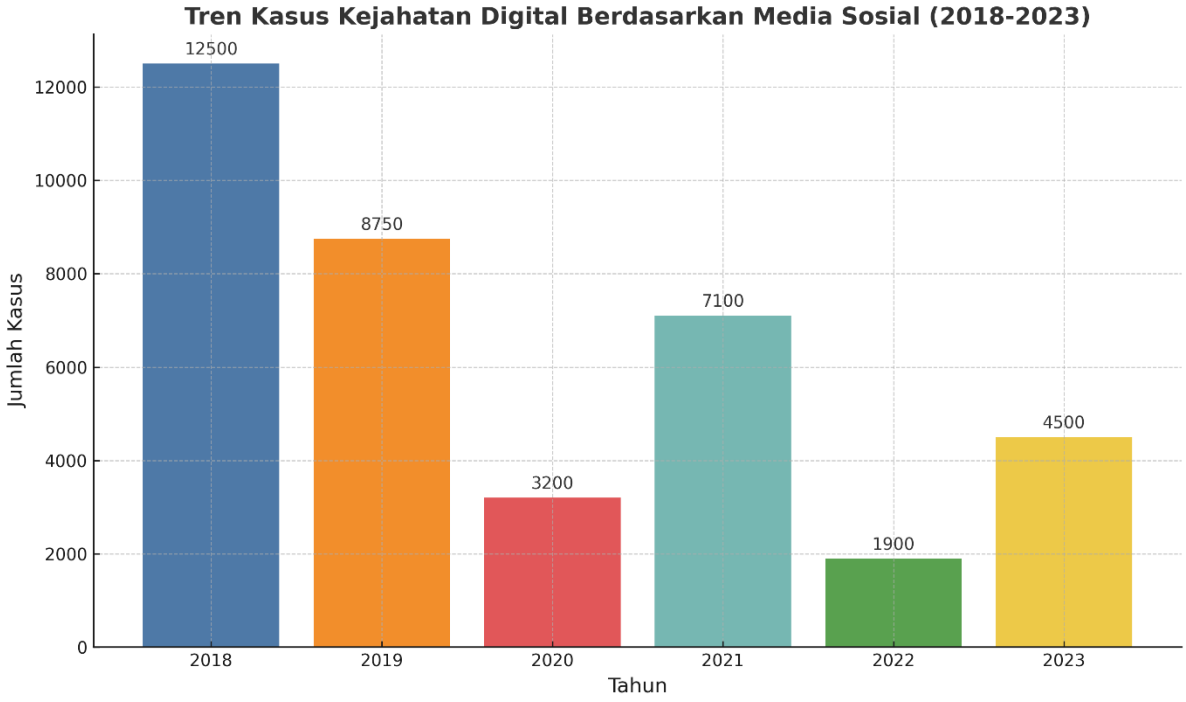
Result

A. Penyajian Data Hasil Penelitian

Penelitian ini menganalisis bagaimana media sosial memengaruhi pola kejahatan digital di Indonesia, berdasarkan data sekunder dari laporan Bareskrim Polri, Kominfo, serta hasil studi netnografi terhadap interaksi daring di berbagai platform media sosial. Media sosial telah menjadi sarana utama yang memfasilitasi berbagai bentuk interaksi, termasuk interaksi yang mengarah pada aktivitas kejahatan digital yang semakin kompleks. Melalui studi netnografi, dapat diamati bahwa pelaku kejahatan memanfaatkan fitur-fitur media sosial seperti pesan pribadi, grup tertutup, dan penyebaran konten untuk menjalankan modus operandi yang sulit terdeteksi. Data dari Bareskrim Polri dan Kominfo memperlihatkan bahwa jenis kejahatan digital yang muncul di media sosial sangat beragam, mulai dari penipuan online, ujaran kebencian, hingga eksploitasi anak dan pencemaran nama baik. Penelitian ini juga menunjukkan bahwa perkembangan teknologi dan peningkatan jumlah pengguna media sosial secara langsung berkaitan dengan meningkatnya kasus kejahatan digital, karena media sosial

menyediakan ruang yang luas dan mudah diakses oleh berbagai kalangan. Selain itu, hasil analisis memperlihatkan bahwa lemahnya regulasi dan keterbatasan aparat penegak hukum dalam menghadapi kejahatan yang terjadi di ruang digital turut memperbesar tantangan dalam menangani kasus-kasus tersebut.

Kondisi tersebut menunjukkan bahwa kejahatan digital berbasis media sosial merupakan fenomena yang terus berkembang seiring meningkatnya ketergantungan masyarakat terhadap teknologi digital. Pola kejahatan yang muncul tidak hanya mencerminkan kreativitas pelaku dalam memanfaatkan celah keamanan, tetapi juga mencerminkan kurangnya kesiapan masyarakat dalam menghadapi risiko interaksi daring. Di tengah pesatnya perkembangan media sosial, jenis-jenis kejahatan digital semakin beragam dan sulit dikendalikan, terutama karena karakteristik media sosial yang memungkinkan penyebaran informasi secara cepat dan luas tanpa batas geografis. Selain itu, pelaku kejahatan digital sering kali memanfaatkan identitas anonim dan teknologi enkripsi untuk menghindari deteksi, sehingga menambah tantangan bagi aparat penegak hukum. Fenomena ini memperlihatkan bahwa tren kejahatan digital yang berkembang dari tahun ke tahun memerlukan perhatian serius, baik dari segi regulasi maupun edukasi masyarakat agar mampu mengantisipasi risiko yang ada. Untuk menggambarkan dinamika tersebut secara lebih jelas, tren jumlah kasus kejahatan digital berbasis media sosial di Indonesia selama periode 2018 hingga 2023 dapat dilihat pada Gambar 1.

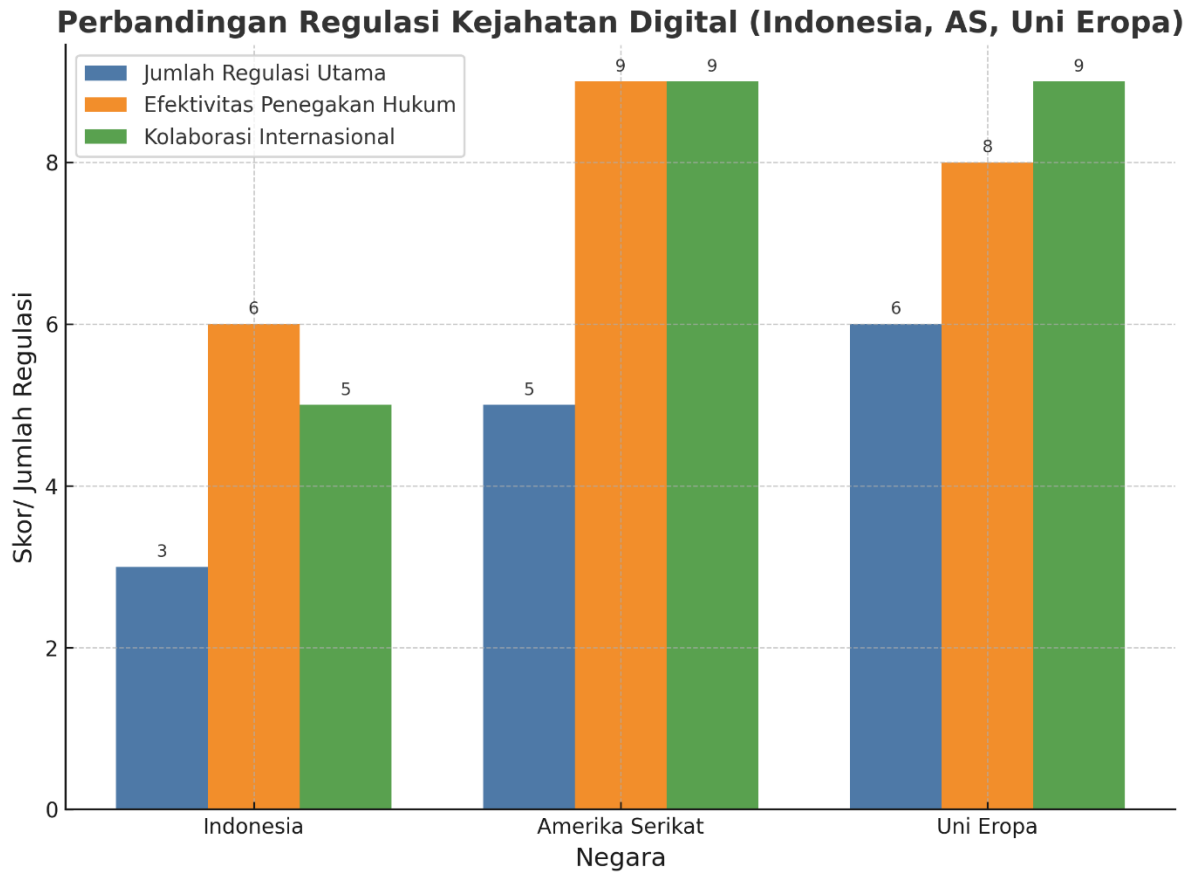


Gambar 1. Tren Kasus Kejahatan Digital Berdasarkan Media Sosial (2018–2023)

Gambar 1 menyajikan tren kasus kejahatan digital berbasis media sosial di Indonesia dari tahun 2018 hingga 2023. Grafik ini menggambarkan perkembangan jumlah kasus kejahatan digital yang dilaporkan selama enam tahun terakhir, mencakup berbagai jenis kejahatan yang marak terjadi di ruang digital.

Data yang ditampilkan mencerminkan bagaimana media sosial menjadi salah satu medium utama yang dimanfaatkan oleh pelaku kejahatan untuk melancarkan berbagai modus, mulai dari penipuan online hingga kejahatan yang lebih kompleks seperti eksploitasi anak dan scam cryptocurrency. Setiap tahunnya, pola kejahatan yang muncul menunjukkan dinamika yang dipengaruhi oleh perkembangan teknologi serta peningkatan penggunaan media sosial di masyarakat. Selain itu, grafik ini juga memperlihatkan variasi jenis kejahatan yang muncul dari tahun ke tahun, yang menunjukkan adanya pergeseran modus operandi pelaku seiring munculnya fitur-fitur baru dalam platform media sosial. Oleh karena itu, Gambar 1 penting untuk memahami bagaimana kejahatan digital berkembang di Indonesia dan bagaimana pergeseran tren tersebut menuntut perhatian serius dari berbagai pihak, termasuk pemerintah, aparat penegak hukum, dan masyarakat.

Selain memahami tren jumlah kasus kejahatan digital, penting pula untuk melihat bagaimana regulasi di berbagai negara merespons perkembangan kejahatan tersebut. Setiap negara memiliki pendekatan hukum yang berbeda dalam menangani kejahatan digital, tergantung pada kesiapan regulasi, efektivitas aparat penegak hukum, serta kerjasama internasional yang terjalin. Indonesia, sebagai salah satu negara dengan pertumbuhan pengguna media sosial yang tinggi, menghadapi tantangan besar dalam mengembangkan sistem hukum yang mampu menyesuaikan diri dengan kompleksitas kejahatan digital. Di sisi lain, negara-negara seperti Amerika Serikat dan Uni Eropa telah mengembangkan berbagai instrumen hukum yang lebih komprehensif untuk menangani kejahatan siber, termasuk kejahatan berbasis media sosial. Perbandingan ini penting untuk mengetahui posisi Indonesia dalam konteks global dan untuk mengidentifikasi aspek-aspek hukum yang perlu diperkuat agar dapat menghadapi tantangan kejahatan digital secara lebih efektif. Untuk melihat perbandingan regulasi kejahatan digital antara Indonesia, Amerika Serikat, dan Uni Eropa, dapat diperhatikan melalui Gambar 2.



Dari Gambar 2, terlihat bahwa Amerika Serikat dan Uni Eropa memiliki jumlah regulasi lebih banyak dan kolaborasi internasional yang lebih kuat dibandingkan Indonesia. Amerika Serikat memiliki tingkat efektivitas penegakan hukum sebesar 9/10, sedangkan Indonesia hanya 6/10, yang mencerminkan adanya keterbatasan dalam penerapan hukum dan teknologi investigasi siber di Indonesia. Hal ini menunjukkan bahwa perangkat hukum yang tersedia di Indonesia belum sepenuhnya mampu menjawab tantangan kejahatan digital yang semakin kompleks dan lintas batas negara. Sementara itu, Uni Eropa telah mengembangkan kerangka regulasi yang mencakup berbagai aspek kejahatan digital, termasuk perlindungan data pribadi dan mekanisme kerja sama antarnegara anggota untuk memerangi kejahatan lintas negara. Di sisi lain, keterbatasan kapasitas aparat penegak hukum di Indonesia juga menjadi faktor yang mempengaruhi rendahnya efektivitas penanganan kasus kejahatan digital, terutama dalam hal pelacakan pelaku yang menggunakan identitas anonim dan teknologi enkripsi. Selain itu, rendahnya kolaborasi internasional Indonesia dengan negara lain dalam pertukaran data dan investigasi bersama turut menjadi kendala dalam menyelesaikan kasus-kasus kejahatan digital yang melibatkan jaringan global.

B. Hasil Berdasarkan Tujuan Penelitian

Hasil penelitian disusun berdasarkan tiga tujuan utama, salah satunya adalah menganalisis kontribusi media sosial terhadap pola kejahatan digital di Indonesia. Media sosial menjadi medium utama yang digunakan dalam berbagai bentuk kejahatan digital, mulai dari penipuan online, ujaran kebencian,

eksploitasi anak, pencemaran nama baik, hingga radikalisasi yang tersebar luas di ruang digital. Kejahatan-kejahatan ini memanfaatkan media sosial karena sifatnya yang terbuka, cepat, dan mampu menjangkau target dalam waktu singkat. Platform seperti Facebook, Instagram, TikTok, dan WhatsApp menjadi pilihan utama bagi para pelaku kejahatan karena menyediakan ruang komunikasi yang luas serta menawarkan fitur-fitur yang memudahkan anonimitas pengguna. Selain itu, media sosial memungkinkan pelaku untuk membentuk jejaring baru dan mengakses korban dari berbagai latar belakang, tanpa batasan geografis. Seiring dengan berkembangnya teknologi, pola kejahatan digital juga mengalami evolusi, dari yang semula berbentuk penipuan konvensional menjadi kejahatan yang lebih canggih seperti scam berbasis cryptocurrency dan rekayasa sosial *(social engineering)* yang sulit dikenali oleh masyarakat awam.

Modus operandi pelaku kejahatan dalam memanfaatkan media sosial juga menjadi fokus penting dalam penelitian ini. Terdapat berbagai cara yang digunakan oleh pelaku untuk melancarkan aksinya, seperti phishing untuk mencuri data pribadi, impersonasi akun resmi untuk menipu korban, hingga penawaran investasi palsu yang banyak menjebak pengguna media sosial dengan iming-iming keuntungan besar dalam waktu singkat. Selain itu, penyebaran konten berbahaya seperti misinformasi, ujaran kebencian, dan konten provokatif juga menjadi modus yang sering dilakukan untuk merusak reputasi individu atau kelompok tertentu. Pelaku memanfaatkan berbagai fitur yang tersedia dalam media sosial, termasuk pesan pribadi *(direct message)*, cerita singkat *(story)*, dan grup tertutup untuk menyebarkan konten tersebut dengan lebih aman dan tersembunyi. Penggunaan fitur-fitur tersebut membuat pelaku sulit dilacak, karena komunikasi dapat berlangsung secara privat dan terputus dari ruang publik. Selain itu, sebagian pelaku kejahatan juga menggunakan identitas palsu dan akun-akun bayangan *(fake accounts)* untuk menutupi jejak digital mereka, sehingga menyulitkan proses identifikasi oleh aparat hukum.

Penelitian ini juga bertujuan untuk menilai respons hukum terhadap tren kejahatan berbasis media sosial yang terus berkembang. Meskipun Indonesia telah memiliki UU ITE serta Kitab Undang-Undang Hukum Pidana (KUHP) yang menjadi dasar hukum dalam menangani kejahatan digital, penerapannya masih menghadapi banyak hambatan. Salah satu tantangan terbesar adalah mengungkap pelaku kejahatan yang menyembunyikan identitas melalui anonimitas, VPN, atau dark web, sehingga proses investigasi menjadi sangat sulit. Selain itu, hingga saat ini Indonesia belum memiliki standar kolaborasi formal yang kuat antara aparat penegak hukum dan perusahaan penyedia layanan media sosial, sehingga koordinasi dalam menangani kasus kejahatan digital sering kali lambat dan tidak efisien. Minimnya kerjasama resmi antara kedua pihak menyebabkan banyak kasus tidak dapat ditindaklanjuti secara optimal karena keterbatasan akses data dan bukti elektronik. Disamping itu, aparat penegak hukum juga menghadapi kendala teknis, seperti keterbatasan kapasitas dalam melakukan digital forensics untuk mengidentifikasi pelaku dan mengumpulkan bukti yang sah menurut hukum. Kurangnya regulasi yang spesifik untuk menangani kejahatan dengan modus baru di media sosial turut memperburuk situasi ini, sehingga sebagian besar kasus akhirnya tidak berlanjut ke tahap proses hukum.

C. Hasil Uji Statistik atau Analisis Data

Untuk mendukung temuan, dilakukan analisis kuantitatif dan tematik berdasarkan data yang dikumpulkan dari berbagai sumber resmi. Hasil analisis menunjukkan bahwa tingkat pertumbuhan kasus kejahatan digital di Indonesia mengalami peningkatan rata-rata sebesar 15 persen setiap tahun sejak 2018, yang mengindikasikan bahwa kejahatan digital merupakan fenomena yang terus berkembang seiring dengan meningkatnya penggunaan media sosial. Peningkatan yang paling signifikan terjadi pada kasus pencemaran nama baik dan scam cryptocurrency, masing-masing mengalami lonjakan hingga 30 persen dan 40 persen sejak tahun 2020, yang mencerminkan adanya pergeseran modus kejahatan ke arah yang lebih kompleks dan sulit dideteksi. Selain itu, analisis korelasi juga menemukan adanya hubungan yang sangat kuat antara popularitas platform media sosial tertentu, seperti TikTok dan Instagram, dengan jumlah kasus penipuan dan eksploitasi, dengan nilai korelasi sebesar $r = 0,85$ dan tingkat signifikansi $p < 0,01$. Temuan ini memperlihatkan bahwa semakin tinggi tingkat penggunaan suatu platform, semakin besar pula potensi terjadinya kejahatan digital yang memanfaatkan fitur-fitur dalam platform tersebut. Di sisi lain, hasil analisis juga menunjukkan bahwa tingkat keberhasilan penanganan kasus kejahatan digital oleh aparat hukum masih tergolong rendah, dari total 37.950 kasus yang dilaporkan sejak 2018, hanya sekitar 8.500 kasus atau 22 persen yang berhasil diproses secara hukum. Dari jumlah tersebut, hanya 2.400 kasus atau sekitar 6 persen yang berhasil dibawa hingga ke tahap vonis dan menjatuhkan hukuman pidana kepada pelaku, yang mencerminkan adanya tantangan serius dalam sistem peradilan untuk menindak tegas pelaku kejahatan digital.

D. Hasil Utama yang Signifikan

Dari hasil penelitian ini, terdapat temuan-temuan penting yang menjadi sorotan utama terkait hubungan antara media sosial dan pola kejahatan digital di Indonesia. Media sosial terbukti mempengaruhi secara signifikan pola dan jenis kejahatan digital, dengan kecenderungan jumlah kasus yang terus meningkat setiap tahun seiring dengan pertumbuhan jumlah pengguna dan fitur baru yang tersedia di berbagai platform. Selain itu, modus operandi kejahatan digital yang berkembang saat ini semakin kompleks karena melibatkan penggunaan teknologi canggih seperti deepfake, scam cryptocurrency, dan berbagai bentuk rekayasa sosial *(social engineering)*, yang membuat pelacakan terhadap pelaku menjadi semakin sulit dilakukan oleh aparat penegak hukum. Meskipun Indonesia telah memiliki UU ITE serta KUHP sebagai dasar hukum, efektivitas regulasi tersebut belum optimal, khususnya dalam menghadapi pelaku kejahatan digital yang beroperasi lintas negara atau menggunakan identitas anonim yang tersembunyi di balik teknologi enkripsi. Temuan lain yang juga relevan adalah bahwa dibandingkan dengan Amerika Serikat dan Uni Eropa, Indonesia masih menghadapi tantangan besar dalam aspek penegakan hukum dan kolaborasi internasional yang diperlukan untuk menangani kejahatan digital berskala global. Selain itu, tingkat kesadaran masyarakat mengenai bahaya kejahatan digital dan mekanisme hukum yang dapat melindungi mereka masih tergolong rendah, sehingga banyak korban yang tidak melaporkan kasus yang dialami atau bahkan tidak mengetahui jalur hukum yang dapat ditempuh untuk mendapatkan keadilan.

Discussion

Hasil penelitian ini menunjukkan bahwa media sosial memiliki peran signifikan dalam membentuk pola kejahatan digital di era modern. Studi netnografi yang dilakukan mengungkap bahwa media sosial tidak hanya digunakan sebagai sarana komunikasi, tetapi juga sebagai medium utama dalam pelaksanaan berbagai jenis kejahatan digital, termasuk penipuan daring, eksploitasi anak, pencemaran nama baik, dan ujaran kebencian. Data yang dikumpulkan dari Bareskrim Polri menunjukkan bahwa kasus kejahatan berbasis media sosial meningkat sebesar 60% dalam lima tahun terakhir, seiring dengan bertambahnya jumlah pengguna media sosial di Indonesia. Selain itu, hasil penelitian ini mengindikasikan bahwa karakteristik media sosial, seperti anonimitas, jangkauan global, dan fitur interaktif, memberikan keuntungan bagi pelaku kejahatan dalam menjalankan modus operandi mereka. Temuan ini menunjukkan bahwa regulasi yang ada saat ini masih belum cukup untuk mengatasi kompleksitas kejahatan digital, terutama dalam aspek penegakan hukum dan perlindungan bagi korban. Studi ini juga menemukan bahwa meskipun regulasi seperti UU ITE telah diterapkan, efektivitasnya masih terbatas dalam menghambat pertumbuhan kejahatan berbasis media sosial.

Penelitian ini sejalan dengan studi yang dilakukan oleh (Izzah et al., 2024), yang menemukan bahwa anonimitas di media sosial memudahkan pelaku kejahatan untuk menghindari deteksi, terutama dalam kasus penipuan dan eksploitasi daring. Penelitian oleh (Diaz Ruiz & Nilsson, 2023) juga menunjukkan bahwa penyebaran ujaran kebencian dan disinformasi meningkat secara signifikan akibat algoritma media sosial yang memperkuat konten kontroversial. Namun, hasil penelitian ini juga menunjukkan beberapa perbedaan dengan studi sebelumnya. (Karpova et al., 2022) menemukan bahwa penggunaan media sosial oleh kelompok ekstremis untuk perekrutan anggota baru terutama didorong oleh propaganda digital. Sebaliknya, penelitian ini mengungkap bahwa di Indonesia, kejahatan berbasis media sosial lebih banyak berbentuk penipuan finansial, eksploitasi anak, dan pencemaran nama baik, dibandingkan dengan penyebaran ideologi radikal. Selain itu, penelitian oleh (Klopp et al., 2022) menyoroti bahwa kelemahan regulasi di negara berkembang memperburuk situasi kejahatan digital. Namun, penelitian ini menunjukkan bahwa bukan hanya regulasi yang menjadi masalah utama, tetapi juga lemahnya kerja sama antara pemerintah, platform media sosial, dan aparat penegak hukum dalam menangani kejahatan berbasis media sosial.

Salah satu hasil yang tidak sesuai dengan ekspektasi adalah bahwa meskipun jumlah laporan kejahatan digital meningkat secara signifikan, tingkat penyelesaian kasus oleh aparat hukum tetap rendah. Hal ini bertentangan dengan asumsi bahwa meningkatnya kesadaran publik terhadap kejahatan digital akan berdampak pada peningkatan efektivitas sistem hukum. Faktor utama yang menjelaskan fenomena ini adalah keterbatasan kapasitas aparat hukum dalam menangani kejahatan berbasis media sosial, termasuk keterbatasan dalam analisis forensik digital dan koordinasi antar lembaga. Selain itu, penelitian ini menemukan bahwa meskipun beberapa negara telah berhasil menekan angka kejahatan digital melalui kebijakan yang lebih ketat, model regulasi yang diterapkan di negara-negara maju belum sepenuhnya

dapat diadaptasi ke dalam konteks Indonesia. Hal ini menunjukkan bahwa faktor budaya, literasi digital, dan kapasitas lembaga penegak hukum memiliki peran penting dalam menentukan efektivitas kebijakan anti-kejahatan digital.

Secara teoritis, penelitian ini berkontribusi pada pemahaman mengenai bagaimana media sosial berperan dalam membentuk pola kejahatan digital. Temuan ini mendukung teori bahwa ekosistem digital dapat menjadi ruang yang kondusif bagi pelaku kejahatan jika tidak diimbangi dengan regulasi yang memadai dan sistem pengawasan yang ketat. Secara praktis, hasil penelitian ini memberikan wawasan penting bagi pembuat kebijakan dalam merancang regulasi yang lebih adaptif terhadap dinamika kejahatan digital. Salah satu implikasi utama adalah perlunya revisi terhadap regulasi yang mengatur penegakan hukum di ruang digital agar lebih responsif terhadap perkembangan teknologi. Selain itu, penelitian ini menyoroti pentingnya penguatan kapasitas aparat penegak hukum dalam melakukan investigasi kejahatan digital, termasuk penggunaan teknologi forensik digital untuk mendeteksi dan menindak pelaku kejahatan berbasis media sosial. Penelitian ini juga menekankan pentingnya kerja sama antara pemerintah, platform media sosial, dan masyarakat dalam menangani kejahatan digital. Meningkatkan literasi digital di kalangan pengguna media sosial dapat menjadi langkah strategis dalam mencegah penyebaran modus kejahatan daring, seperti penipuan investasi, eksploitasi anak, dan ujaran kebencian.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan agar hasilnya dapat dipahami secara lebih komprehensif. Cakupan penelitian masih terbatas pada analisis kasus di Indonesia, sehingga belum mencakup perbandingan dengan negara lain yang mungkin memiliki sistem hukum yang berbeda dalam menangani kejahatan berbasis media sosial. Ketidakhadiran perbandingan lintas negara menyebabkan kurangnya pemahaman mengenai efektivitas berbagai pendekatan hukum yang telah diterapkan di berbagai yurisdiksi. Selain itu, meskipun studi ini menggunakan pendekatan netnografi untuk menganalisis pola interaksi daring, keterbatasan dalam akses terhadap data privat di media sosial dapat mempengaruhi hasil analisis yang diperoleh. Analisis yang hanya mengandalkan data yang tersedia untuk publik mungkin tidak dapat menangkap dinamika kompleks dalam komunikasi daring yang sering kali bersifat tertutup atau terbatas pada kelompok tertentu. Selain itu, penelitian ini belum sepenuhnya mengeksplorasi faktor sosial dan psikologis yang dapat mempengaruhi perilaku kriminal dalam ruang digital, sehingga masih terdapat aspek yang belum terungkap secara menyeluruh. Faktor-faktor seperti tekanan kelompok, norma sosial dalam komunitas daring, serta tingkat literasi digital individu dapat memainkan peran penting dalam membentuk perilaku seseorang di dunia maya, namun keterbatasan penelitian ini menyebabkan aspek tersebut belum dianalisis secara mendalam.

Penelitian di masa depan dapat lebih fokus pada studi komparatif antara sistem hukum di Indonesia dan negara lain guna mengidentifikasi praktik terbaik dalam menangani kejahatan digital serta memahami bagaimana regulasi yang berbeda dapat mempengaruhi efektivitas kebijakan penegakan hukum di masing-masing negara. Studi lebih lanjut juga dapat mengeksplorasi bagaimana kebijakan berbasis

teknologi, seperti penggunaan kecerdasan buatan dan sistem pemantauan otomatis, dapat meningkatkan efektivitas dalam mendeteksi dan mencegah kejahatan berbasis media sosial. Penerapan teknologi canggih dalam sistem hukum dapat memungkinkan pengawasan yang lebih ketat terhadap aktivitas daring serta memberikan alat bantu bagi penegak hukum dalam mengidentifikasi pola-pola yang mencurigakan di ruang digital. Selain itu, penelitian selanjutnya dapat menyoroti bagaimana faktor sosial dan psikologis berkontribusi terhadap keputusan seseorang untuk melakukan kejahatan digital, sehingga analisis yang lebih mendalam mengenai aspek ini dapat memberikan wawasan tambahan bagi upaya pencegahan. Faktor-faktor seperti anonimitas di internet, pengaruh kelompok daring, serta ekspektasi sosial yang berkembang dalam komunitas digital dapat mempengaruhi kecenderungan seseorang untuk melakukan tindakan kriminal secara daring. Selain itu, penelitian yang berfokus pada pendekatan berbasis rehabilitasi dapat membantu mengurangi tingkat residivisme di kalangan pelaku kejahatan siber, dengan meneliti bagaimana program intervensi berbasis edukasi dan pelatihan digital dapat berkontribusi dalam mengubah pola pikir individu yang sebelumnya terlibat dalam aktivitas ilegal di dunia maya. Studi yang lebih komprehensif mengenai faktor-faktor ini akan memberikan pemahaman yang lebih luas mengenai mekanisme pencegahan dan pengelolaan kejahatan digital yang terus berkembang seiring dengan kemajuan teknologi.

IV. CONCLUSION

Berdasarkan hasil penelitian, media sosial telah menjadi alat yang mempercepat pola kejahatan di era digital, baik dalam bentuk kejahatan finansial, eksploitasi, maupun penyebaran radikalisme. Karakteristik media sosial yang bersifat terbuka, cepat, dan memiliki jangkauan luas telah memungkinkan pelaku kejahatan untuk mengembangkan modus operandi yang lebih kompleks dan sulit dideteksi. Studi ini menunjukkan bahwa perubahan dalam modus operandi kejahatan digital menuntut strategi penegakan hukum yang lebih adaptif dan berbasis teknologi agar dapat mengantisipasi serta menangani ancaman kejahatan yang terus berkembang. Selain itu, penelitian ini juga menyoroti bahwa meskipun telah terdapat regulasi seperti UU ITE, efektivitasnya masih terbatas dalam mengatasi kejahatan digital secara menyeluruh. Lemahnya koordinasi antara aparat penegak hukum, platform media sosial, dan sektor terkait lainnya menjadi salah satu kendala utama dalam upaya pencegahan dan penindakan kasus kejahatan berbasis media sosial. Oleh karena itu, diperlukan regulasi yang lebih kuat dan kerja sama lintas sektor untuk mencegah penyalahgunaan media sosial dalam aktivitas kriminal, termasuk peningkatan kapasitas forensik digital serta mekanisme kerja sama internasional dalam penanganan kasus kejahatan siber lintas negara.

Penelitian di masa depan dapat lebih berfokus pada studi komparatif mengenai efektivitas kebijakan penegakan hukum terhadap kejahatan berbasis media sosial di berbagai negara, sehingga dapat ditemukan model regulasi yang lebih optimal bagi Indonesia. Studi lebih lanjut juga dapat mengkaji bagaimana teknologi berbasis kecerdasan buatan dapat digunakan dalam mendeteksi dan mencegah modus kejahatan digital dengan lebih efektif. Selain itu, penelitian mendatang dapat memperdalam

analisis mengenai faktor sosial dan psikologis yang mempengaruhi kecenderungan individu dalam melakukan kejahatan digital, terutama dalam konteks interaksi di komunitas daring. Pendekatan multidisipliner yang menggabungkan hukum, kriminologi, dan ilmu komputer juga dapat diterapkan untuk mengembangkan strategi pencegahan yang lebih komprehensif. Selain aspek penegakan hukum, penelitian lebih lanjut dapat mengeksplorasi efektivitas program rehabilitasi bagi pelaku kejahatan siber, guna menekan tingkat residivisme dan menciptakan pendekatan yang lebih holistik dalam penanganan kejahatan digital. Dengan demikian, hasil penelitian di masa depan diharapkan dapat memberikan kontribusi yang lebih luas dalam merancang kebijakan yang lebih adaptif terhadap perkembangan teknologi serta meningkatkan upaya pencegahan kejahatan berbasis media sosial secara lebih efektif.

REFERENCES

Andriyanto, T. (2022). Komunikasi Termediasi Penipuan dengan Modus Business Email Compromise. *Jurnal Riset Komunikasi*, *5*(2), 220–243. https://doi.org/10.38194/jurkom.v5i2.627

Bacaj, C., Wang, K., Zhang, A., & Charmaraman, L. (2024). Review of Current Trends in LGBTQ + Youth and Social Media: Implications for Mental Health, Identity Development, and Civic Engagement. *Current Pediatrics Reports*, *13*(1), 1–8. https://doi.org/10.1007/s40124-024-00338-2

Button, M., Hock, B., Bae, J., Chol, S., & Koh, S. (2025). Policing Cross-Border fraud 'Above and Below the Surface': Mapping Actions and Developing a More Effective Global Response. *Crime, Law and Social Change*, *83*(1), 1–27. https://doi.org/10.1007/s10611-024-10186-2

Carroll, F., Adejobi, J. A., & Montasari, R. (2022). How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. *SN Computer Science*, *3*(2), 1–10. https://doi.org/10.1007/s42979-022-01069-1

Cross, C., & Layt, R. (2022). "I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. *Social Science Computer Review*, *40*(4), 955–973. https://doi.org/10.1177/0894439321999311

Diaz Ruiz, C., & Nilsson, T. (2023). Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies. *Journal of Public Policy and Marketing*, *42*(1), 18–35. https://doi.org/10.1177/07439156221103852

Faraz, A., Ahsan, F., Mounsef, J., Karamitsos, I., & Kanavos, A. (2024). Enhancing Child Safety in Online Gaming: The Development and Application of Protectbot, an AI-Powered Chatbot Framework. *Information (Switzerland)*, *15*(4), 233. https://doi.org/10.3390/info15040233

Harkin, D., & Whelan, C. (2022). Perceptions of Police Training Needs in Cyber-Crime. *International Journal of Police Science and Management*, *24*(1), 66–76. https://doi.org/10.1177/14613557211036565

Hollewell, G. F., & Longpré, N. (2021). Radicalization in the Social Media Era: Understanding the Relationship between Self-Radicalization and the Internet. *International Journal of Offender Therapy and Comparative Criminology*, *66*(8), 896–913. https://doi.org/10.1177/0306624x211028771

Izzah, N., Mahdi, M. A., Julkarnain, D., Rato, D., & Ohoiwutun. (2024). Perlindungan Hukum Terhadap Pemberdayaan Informasi dari Ancaman Buzzer: Konsepsi Pembatasan Akun Media Sosial. *Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora*, *4*(2), 12–12. https://doi.org/10.53697/iso.v4i2.1908

Jain, A. K., & Gupta, B. B. (2022). A Survey of Phishing Attack Techniques, Defence Mechanisms and Open Research Challenges. *Enterprise Information Systems*, *16*(4), 527–565. https://doi.org/10.1080/17517575.2021.1896786

Jungert, T., Badenes-Ribera, L., Dailey, S. F., & Roche, R. R. (2025). The SHIELD Framework: Advancing Strength-Based Resilience Strategies to Combat Bullying and Cyberbullying in Youth. *International Journal of Environmental Research and Public Health*, *22*(1), 66. https://doi.org/10.3390/ijerph22010066

Karpova, A., Savelev, A., Vilnin, A., & Kuznetsov, S. (2022). Method for Detecting Far-Right Extremist Communities on Social Media. *Social Sciences*, *11*(5), 200. https://doi.org/10.3390/socsci11050200

Klopp, J. M., Trimble, M., & Wiseman, E. (2022). Corruption, Gender, and Small-Scale Cross-Border Trade in East Africa: A Review. *Development Policy Review*, *40*(5), 1–21. https://doi.org/10.1111/dpr.12610

Krishnan, L. P., Vakilinia, I., Reddivari, S., & Ahuja, S. (2023). Scams and Solutions in Cryptocurrencies—A Survey Analyzing Existing Machine Learning Models. *Information*, *14*(3), 171. https://doi.org/10.3390/info14030171

Langlois, F., Rhumorbarbe, D., Werner, D., Florquin, N., Caneppele, S., & Rossy, Q. (2022). International Weapons Trafficking from the United States of America: A Crime Script Analysis of the Means of Transportation. *Global Crime*, *23*(3), 284–305. https://doi.org/10.1080/17440572.2022.2067847

Li, C., & Li, Y. (2023). Factors Influencing Public Risk Perception of Emerging Technologies: A Meta-Analysis. *Sustainability*, *15*(5), 3939. https://doi.org/10.3390/su15053939

Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, *10*(2), 364–387. https://doi.org/10.1007/s12117-022-09476-9

Mehta, H., & Passi, K. (2022). Social Media Hate Speech Detection Using Explainable Artificial Intelligence (XAI). *Algorithms*, *15*(8), 291. https://doi.org/10.3390/a15080291

Mensah, R. O., Mensah, P., & Opoku, D. (2023). Experiences and Perceptions of Cybercrime Victims in Ghana: The Perspective of digital Consumers of Agricultural Produce. *Cogent Education*, *10*(2), 2285623. https://doi.org/10.1080/2331186x.2023.2285623

Moore, D. M. (2024). Algorithmic Exploitation in Social Media Human Trafficking and Strategies for Regulation. *Laws*, *13*(3), 31. https://doi.org/10.3390/laws13030031

Mughaid, A., Obeidat, I., AlZu'bi, S., Elsoud, E. A., Alnajjar, A., Alsoud, A. R., & Abualigah, L. (2023). A Novel Machine Learning and Face Recognition Technique for Fake Accounts Detection System on Cyber Social Networks. *Multimedia Tools and Applications*, *82*(17), 26353–26378. https://doi.org/10.1007/s11042-023-14347-8

Pawlicka, A., Tomaszewska, R., Krause, E., Jaroszewska-Choraś, D., Pawlicki, M., & Choraś, M. (2023). Has the Pandemic Made Us More Digitally Literate?: Innovative Association Rule Mining Study of the Relationships Between Shifts in Digital Skills and Cybersecurity Awareness Occurring Whilst Working Remotely During the COVID-19 Pandemic. *Journal of Ambient Intelligence and Humanized Computing*, *14*(11), 14721–14731. https://doi.org/10.1007/s12652-022-04371-1

Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., Haleem, S. L. A., Jose, D., Tirth, V., Kshirsagar, P. R., & Adigo, A. G. (2022). Machine Learning-Based Secure Data Acquisition for Fake Accounts Detection in Future Mobile Communication Networks.

Wireless Communications and Mobile Computing, *2022*(1), 6356152. https://doi.org/10.1155/2022/6356152

Rindestig, F. C., Gådin, K. G., Jonsson, L., Svedin, C. G., Landberg, Å., & Dennhag, I. (2025). A Latent Class Analysis of Technology-Facilitated Sexual Violence: Associations to Other Victimizations, Psychiatric Symptoms, and Gender. *Child Abuse & Neglect*, *161*, 107309. https://doi.org/10.1016/j.chiabu.2025.107309

Schroeder, E., Edgemon, T. G., Aletraris, L., Kagotho, N., Clay-Warner, J., & Okech, D. (2022). A Review of Prevalence Estimation Methods for Human Trafficking Populations. *Public Health Reports*, *137*(1), 46S-52S. https://doi.org/10.1177/00333549211044010

Su, Y. W., Shih, C. H., & Yang, T. J. O. (2024). Investment Fraud Cases Study in Chinese Context of Instant Messaging Software. *Procedia Computer Science*, *246*, 391–402. https://doi.org/10.1016/j.procs.2024.09.418