

**ARTIFICIAL INTELLIGENCE SEBAGAI SARANA BARU
KEJAHATAN TELEMATIKA: TANTANGAN PENEGAKAN HUKUM PIDANA DI INDONESIA**

Ali Mukti Nur Hidayat, Muchamad Iksan

Program Studi Magister Ilmu Hukum, Universitas Muhammadiyah Surakarta

alimuktinurh@gmail.com

ABSTRAK

Perkembangan Artificial Intelligence (AI) telah mengubah pola interaksi manusia dengan teknologi digital. Di satu sisi AI memberikan manfaat besar bagi produktivitas, analisis data, otomatisasi, dan inovasi; di sisi lain, kemampuan AI dapat disalahgunakan sebagai sarana baru untuk melakukan kejahatan telematika, antara lain penipuan berbasis impersonasi, pembuatan konten palsu atau deepfake, manipulasi informasi, rekayasa sosial, penyalahgunaan data pribadi, serta pengembangan serangan digital yang lebih adaptif. Persoalan hukum muncul karena teknologi berkembang lebih cepat daripada kemampuan hukum pidana untuk merumuskan dan membuktikan perbuatan yang dilakukan dengan bantuan AI. Penelitian ini bertujuan menganalisis bentuk penyalahgunaan AI sebagai sarana kejahatan telematika, kerangka hukum pidana yang dapat digunakan di Indonesia, serta tantangan penegakan hukum terhadap pelaku, termasuk persoalan atribusi, alat bukti elektronik, yurisdiksi, dan pertanggungjawaban pidana. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual serta diperkuat studi kepustakaan. Pembahasan juga mengacu pada penelitian Sudaryono, M. Iksan, dan Kuswardani mengenai penyelesaian perkara pidana oleh kepolisian, khususnya gagasan bahwa penegakan hukum tidak cukup hanya berorientasi pada prosedur formal, tetapi perlu memperhatikan manusia, pengalaman, efektivitas, dan keadilan substantif. Hasil penelitian menunjukkan bahwa AI pada dasarnya bukan subjek kejahatan, melainkan sarana atau medium yang digunakan manusia. Oleh karena itu, fokus pertanggungjawaban tetap diarahkan kepada manusia yang secara sadar menggunakan, mengendalikan, atau memanfaatkan AI untuk melakukan tindak pidana. Penegakan hukum ke depan memerlukan penguatan kapasitas penyidik, forensik digital, mekanisme preservasi bukti, kerja sama lintas negara, dan regulasi AI yang lebih komprehensif.

Kata Kunci: Artificial Intelligence, kejahatan telematika, cybercrime, penegakan hukum pidana, deepfake, bukti elektronik.

ABSTRACT

Article History

Received: September 2026

Reviewed: Oktober 2026

Published: Oktober 2026

Copyright : Author

Publish by : CAUSA



This work is licensed
under a [Creative
Commons Attribution-
NonCommercial 4.0
International License](https://creativecommons.org/licenses/by-nc/4.0/).

The development of Artificial Intelligence (AI) has transformed human interaction with digital technology. While AI provides significant benefits, it may also be misused as a new means of committing telematic crimes, including impersonation fraud, deepfake content, information manipulation, social engineering, personal-data abuse, and adaptive digital attacks. This article examines the misuse of AI as a means of telematic crime, the Indonesian criminal-law framework applicable to such conduct, and the challenges of attribution, electronic evidence, jurisdiction, and criminal responsibility. The research employs normative juridical methods with statutory and conceptual approaches. The discussion also uses the study by Sudaryono, M. Iksan, and Kuswardani concerning criminal-case resolution by the police, particularly its emphasis that law enforcement should not be understood merely as formal implementation of rules but also requires attention to human factors, experience, effectiveness, and substantive justice. The article argues that AI is not itself the criminal subject; rather, it is a technological means used by human actors. Criminal responsibility therefore remains focused on persons who intentionally control or exploit AI to commit criminal conduct. Future enforcement requires stronger digital-forensic capacity, evidence preservation, cross-border cooperation, and a more comprehensive AI governance framework.

Keywords: Artificial Intelligence, telematic crime, cybercrime, criminal law enforcement, deepfake, electronic evidence.

I. PENDAHULUAN

Transformasi digital telah menghasilkan perubahan mendasar dalam kehidupan sosial, ekonomi, pemerintahan, dan penegakan hukum. Perubahan tersebut semakin kuat dengan hadirnya Artificial Intelligence (AI) yang mampu melakukan pemrosesan data, mengenali pola, menghasilkan teks, gambar, suara, dan video, serta membantu pengambilan keputusan. Dalam konteks Indonesia, pemerintah telah mengeluarkan Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial sebagai pedoman etika bagi pelaku usaha dan penyelenggara sistem elektronik. Surat edaran tersebut menekankan nilai inklusivitas, kemanusiaan, keamanan, aksesibilitas, transparansi, kredibilitas dan akuntabilitas, perlindungan data pribadi, keberlanjutan, serta kekayaan intelektual.

Kemajuan AI juga menghadirkan dimensi baru dalam kejahatan telematika. Pelaku tidak selalu membutuhkan kemampuan teknis yang sangat tinggi untuk menghasilkan konten manipulatif. AI dapat digunakan untuk meniru gaya komunikasi seseorang, menghasilkan pesan persuasif, membuat suara atau gambar sintetis, serta mengotomatisasi penyebaran informasi palsu. Dengan demikian, AI dapat menurunkan

hambatan teknis bagi pelaku kejahatan sekaligus meningkatkan skala dan kecepatan serangan.

Fenomena tersebut menimbulkan pertanyaan penting dalam hukum pidana. Apakah ketentuan pidana yang berlaku telah cukup untuk menjangkau perbuatan yang dilakukan dengan bantuan AI? Bagaimana menentukan siapa yang harus bertanggung jawab apabila suatu konten dibuat melalui sistem AI? Bagaimana penyidik membuktikan hubungan antara pelaku dengan sistem, akun, perangkat, dan data yang digunakan? Persoalan menjadi lebih kompleks ketika pelaku, korban, penyedia layanan AI, dan server berada di negara berbeda.

Dalam hukum pidana Indonesia, prinsip pertanggungjawaban pidana tetap menempatkan manusia sebagai subjek yang dapat dimintai pertanggungjawaban. Karena itu, AI tidak dapat diposisikan secara sederhana sebagai 'pelaku' dalam pengertian hukum pidana. AI lebih tepat dipahami sebagai alat, sarana, atau medium yang dapat dipakai untuk mewujudkan tindak pidana yang telah dirumuskan dalam peraturan perundang-undangan.

Artikel ini penting karena perkembangan kejahatan telematika tidak hanya menuntut pembaruan norma, tetapi juga pembaruan cara berpikir aparat penegak hukum. Penegakan hukum terhadap kejahatan berbasis AI memerlukan kemampuan teknis, pemahaman terhadap algoritma dan bukti digital, serta kemampuan menghubungkan fakta teknologi dengan unsur tindak pidana. Dengan kata lain, tantangannya bukan sekadar menemukan pasal, tetapi membuktikan perbuatan, pelaku, kesalahan, akibat, dan hubungan kausalnya.

Rumusan Masalah

1. Bagaimana Artificial Intelligence dapat menjadi sarana baru dalam kejahatan telematika?
2. Bagaimana kerangka hukum pidana Indonesia dapat digunakan untuk menanggulangi penyalahgunaan AI?
3. Apa saja tantangan penegakan hukum pidana terhadap kejahatan telematika berbasis AI dan bagaimana arah penguatannya?

Tujuan Penelitian

1. Menganalisis bentuk penyalahgunaan AI sebagai sarana kejahatan telematika.
2. Menganalisis relevansi hukum pidana dan hukum siber Indonesia terhadap perbuatan tersebut.
3. Merumuskan gagasan penguatan penegakan hukum pidana terhadap kejahatan berbasis AI.

II. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (yuridis normatif) dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Bahan hukum primer yang digunakan meliputi Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana beserta penyesuaiannya, serta Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. Bahan hukum sekunder berupa buku, artikel ilmiah, dan penelitian terdahulu, termasuk

artikel Sudaryono, M. Iksan, dan Kuswardani yang dilampirkan dalam penelitian ini. Analisis dilakukan secara kualitatif dengan menghubungkan norma hukum dengan karakteristik kejahatan telematika berbasis AI.

III. HASIL DAN PEMBAHASAN

A. Artificial Intelligence dan Transformasi Kejahatan Telematika

Artificial Intelligence dapat dipahami sebagai teknologi yang memungkinkan sistem komputer melakukan pemrosesan atau pengolahan data untuk menghasilkan keluaran yang sebelumnya membutuhkan kemampuan manusia. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 mendefinisikan kecerdasan artifisial dan mengatur nilai serta prinsip etika dalam penyelenggaraannya. Instrumen tersebut menunjukkan bahwa negara telah mengakui AI sebagai teknologi yang memiliki manfaat sekaligus potensi risiko.

Dalam konteks kejahatan telematika, AI mengubah dua hal sekaligus. Pertama, AI dapat menjadi alat untuk melakukan kejahatan yang sebelumnya telah dikenal, seperti penipuan, pemerasan, pencurian data, pemalsuan, atau penyebaran informasi palsu. Kedua, AI dapat mengubah karakter serangan menjadi lebih cepat, personal, otomatis, dan sulit dibedakan dari komunikasi manusia.

Salah satu contoh yang relevan adalah penipuan berbasis impersonasi. Pelaku dapat menggunakan teknologi sintetis untuk membuat komunikasi seolah-olah berasal dari seseorang yang dikenal korban. Dalam perspektif hukum pidana, teknologi tersebut tidak menghapus sifat melawan hukum dari perbuatan utama. Yang perlu dibuktikan adalah siapa yang menggunakan sarana tersebut, untuk tujuan apa, dengan kesengajaan seperti apa, dan kerugian atau akibat apa yang ditimbulkan.

Contoh lain adalah deepfake. Konten audio-visual yang dibuat atau dimanipulasi AI dapat digunakan untuk merusak reputasi, menipu korban, memengaruhi transaksi, memeras, atau menyebarkan informasi yang menyesatkan. Tantangan hukumnya terletak pada pemisahan antara penggunaan AI yang sah dan penggunaan AI sebagai instrumen tindak pidana.

B. Bentuk-Bentuk Penyalahgunaan AI sebagai Sarana Kejahatan Telematika

Bentuk	Karakteristik	Isu Hukum
Impersonasi dan penipuan	AI digunakan untuk menghasilkan komunikasi yang menyerupai identitas/gaya seseorang.	Pembuktian pelaku, niat, tipu muslihat, kerugian, dan hubungan dengan akun/perangkat.
Deepfake	Pembuatan atau manipulasi audio, gambar, atau video secara sintetis.	Pemalsuan, pencemaran nama baik, penipuan, pemerasan, perlindungan korban, dan pembuktian keaslian konten.
Rekayasa sosial berbasis AI	Pesan dibuat lebih personal dan persuasif berdasarkan data korban.	Penyalahgunaan data pribadi, penipuan, akses tanpa hak, dan atribusi pelaku.
Penyalahgunaan data pribadi	Data dikumpulkan, diproses, atau digunakan untuk membuat profil dan serangan.	Kepatuhan UU PDP, dasar pemrosesan data, keamanan, dan pertanggungjawaban.

Otomatisasi serangan digital	AI membantu menghasilkan atau mengadaptasi konten serangan dalam skala besar.	Atribusi, bukti digital, kesengajaan, dan keterkaitan antara operator dengan sistem.
------------------------------	---	--

Kelima bentuk tersebut menunjukkan bahwa AI bukan selalu menciptakan delik baru. Dalam banyak keadaan, AI justru memperkuat cara melakukan tindak pidana yang telah dikenal. Karena itu, pendekatan hukum pidana perlu membedakan antara 'teknologi yang digunakan' dan 'perbuatan pidana yang dilakukan'. Perbedaan ini penting agar hukum tidak terjebak pada teknologi, melainkan tetap berfokus pada perbuatan dan unsur deliknya.

C. Kerangka Hukum Pidana Indonesia terhadap Kejahatan Berbasis AI

1. Undang-Undang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 1 Tahun 2024 merupakan perubahan kedua atas UU ITE. UU ini tetap menjadi salah satu instrumen utama dalam menangani perbuatan pidana di ruang digital. Dalam kasus AI, ketentuan mengenai akses tanpa hak, intersepsi, manipulasi atau pemindahan informasi elektronik, gangguan terhadap sistem, serta ketentuan pidana terkait informasi elektronik dapat menjadi relevan bergantung pada konstruksi perbuatan dan unsur yang terbukti.
2. Undang-Undang Pelindungan Data Pribadi. UU Nomor 27 Tahun 2022 penting ketika AI digunakan untuk memproses atau mengeksploitasi data pribadi. Penyalahgunaan data untuk membuat profil korban, melakukan impersonasi, atau mengembangkan konten sintetis dapat menimbulkan persoalan pelindungan data, khususnya apabila pemrosesan dilakukan tanpa dasar yang sah atau dengan mengabaikan kewajiban keamanan dan hak subjek data.
3. Kitab Undang-Undang Hukum Pidana Nasional. UU Nomor 1 Tahun 2023 tentang KUHP telah berlaku sejak 2 Januari 2026. Keberlakuan KUHP nasional menandai perubahan sistem hukum pidana Indonesia dan menuntut harmonisasi dengan berbagai undang-undang pidana di luar KUHP. Dalam perkara berbasis AI, konstruksi pertanggungjawaban tetap harus dibangun berdasarkan asas dan unsur tindak pidana yang berlaku, sementara UU khusus tetap relevan sepanjang mengatur perbuatan tertentu.
4. Etika Kecerdasan Artifisial. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 bukan pengganti hukum pidana, tetapi dapat menjadi rujukan tata kelola dan pencegahan penyalahgunaan AI. Prinsip keamanan, transparansi, akuntabilitas, pelindungan data pribadi, dan manajemen risiko penting untuk membangun ekosistem AI yang dapat diawasi.

D. Pertanggungjawaban Pidana: AI Bukan Pelaku, Manusia yang Bertanggung Jawab

Pertanggungjawaban pidana terhadap penyalahgunaan AI perlu dimulai dari prinsip bahwa AI tidak memiliki kesadaran hukum dan tidak dapat diperlakukan sebagai subjek pertanggungjawaban pidana seperti manusia. Sistem AI dapat menghasilkan keluaran yang kompleks, tetapi penggunaan sistem tersebut dalam tindak pidana pada prinsipnya tetap harus ditelusuri kepada manusia yang mengoperasikan, mengarahkan, mengendalikan, atau dengan sengaja memanfaatkan sistem tersebut.

Persoalan menjadi sulit ketika pelaku menggunakan layanan pihak ketiga dan tidak berinteraksi langsung dengan korban. Dalam kondisi demikian, penyidik perlu membangun rangkaian bukti yang menunjukkan hubungan antara pelaku dan perbuatan: akun, perangkat, identitas pembayaran, alamat jaringan, riwayat komunikasi, file, metadata, log, serta bukti lain yang sah. Tidak satu pun bukti tersebut boleh dinilai

secara terpisah; semuanya perlu dirangkai untuk menjelaskan siapa yang mengendalikan aktivitas.

Di sinilah konsep mens rea atau kesalahan menjadi penting. Penggunaan AI secara otomatis tidak dengan sendirinya membuktikan kesengajaan. Penegak hukum perlu membuktikan bahwa manusia di balik penggunaan AI mengetahui dan menghendaki perbuatan yang dilarang atau setidaknya memenuhi bentuk kesalahan yang disyaratkan oleh delik yang diterapkan.

E. Pembuktian Digital dalam Kejahatan Berbasis AI

Bukti elektronik merupakan bagian sentral dalam perkara kejahatan telematika. Namun, AI menimbulkan tantangan tambahan karena konten digital dapat dibuat, diubah, diproduksi ulang, atau diproses secara sintetis. Oleh sebab itu, pemeriksaan bukti tidak cukup hanya dengan melihat tampilan sebuah gambar, suara, video, atau percakapan.

Penyidik perlu memperhatikan rantai penguasaan barang bukti (chain of custody), metode akuisisi data, integritas file, waktu pembuatan dan perubahan, sumber data, hubungan antarperangkat, serta hasil pemeriksaan forensik. Dalam perkara deepfake, misalnya, pertanyaan penting bukan hanya apakah konten tersebut palsu, tetapi siapa yang membuat atau menyebarkannya, dengan perangkat apa, dengan akun siapa, untuk tujuan apa, dan apakah pelaku mengetahui sifat manipulatif konten tersebut.

Tantangan lain adalah ketergantungan pada penyedia platform dan layanan AI. Data yang dibutuhkan penyidik mungkin berada pada server di luar Indonesia. Hal ini membuat kerja sama internasional, mekanisme permintaan data, dan kemampuan penyidik melakukan forensik lintas platform menjadi semakin penting.

Artikel Sudaryono, M. Iksan, dan Kuswardani berjudul “Model Penyelesaian Secara Alternatif dalam Peradilan Pidana (Studi Khusus terhadap Model Penyelesaian Perkara Pidana oleh Lembaga Kepolisian)” membahas bagaimana kepolisian menangani perkara pidana dan tantangan penerapan model penyelesaian alternatif. Penelitian tersebut menggunakan pendekatan yuridis-sosiologis dengan data primer dan sekunder serta analisis kualitatif. Dalam penelitian itu, Polresta Surakarta pada Januari-Mei 2011 dicatat menangani 33 jenis tindak pidana, yang dibagi menjadi kejahatan konvensional dan inkonvensional/transnasional. Pada tabel perkara inkonvensional juga telah tercatat adanya “kejahatan komputer”, menunjukkan bahwa pada periode tersebut kejahatan berbasis teknologi telah menjadi bagian dari perhatian penegak hukum (Sudaryono, Iksan, & Kuswardani, 2012). Yang paling relevan untuk konteks AI adalah gagasan penulis mengenai penegakan hukum yang tidak boleh berhenti pada prosedur formal. Penulis mengutip pandangan Satjipto Rahardjo bahwa penegakan hukum harus bersifat progresif dan hukum tidak hanya dilihat dari aspek peraturan, tetapi juga dari aspek manusianya. Artikel tersebut juga menegaskan bahwa logika peraturan perlu disempurnakan dengan logika pengalaman. Gagasan ini penting ketika berhadapan dengan AI karena teknologi bergerak lebih cepat daripada perubahan norma hukum. *“Hukum tidak dapat hanya dilihat dari aspek peraturan (rule), tetapi juga dari aspek manusianya (People, man).”*

— Sudaryono, M. Iksan, & Kuswardani, 2012, Jurnal Penelitian Humaniora, Vol. 13, No. 1, hlm. 65.

Dalam konteks kejahatan berbasis AI, gagasan tersebut dapat diterjemahkan menjadi kebutuhan untuk meningkatkan kualitas sumber daya manusia penegak hukum. Polisi, jaksa, dan hakim perlu memahami bukan hanya teks undang-undang, tetapi juga karakteristik teknologi AI, mekanisme bukti elektronik, risiko manipulasi konten, dan cara menilai hubungan antara manusia dengan sistem. Artikel Sudaryono dkk. juga memperlihatkan persoalan klasik penegakan hukum: kepolisian dapat memahami kebutuhan terhadap pendekatan baru, tetapi pelaksanaannya membutuhkan landasan hukum yang jelas. Dalam penelitian tersebut, penerapan ADR pernah diupayakan tetapi ditanggguhkan karena dipandang membutuhkan payung hukum yang kuat. Pelajaran ini relevan untuk AI: inovasi penegakan hukum harus berjalan dalam batas kewenangan yang sah, tetapi hukum juga harus adaptif terhadap perkembangan teknologi.

Penelitian tersebut juga mencatat bahwa penyelesaian perkara pidana oleh kepolisian pada saat itu masih sangat berorientasi pada prosedur tetap dan ketentuan hukum acara. Bagi kejahatan telematika berbasis AI, kepatuhan prosedural tetap merupakan keharusan, tetapi perlu dilengkapi kapasitas teknis dan metode pembuktian yang mampu menjangkau karakter bukti digital. Dengan demikian, pendekatan progresif tidak berarti mengabaikan hukum, melainkan menerjemahkan hukum secara cermat agar mampu memberikan perlindungan nyata terhadap korban dan kepastian hukum bagi semua pihak.

F. Tantangan Penegakan Hukum Pidana terhadap Kejahatan AI

Tantangan	Uraian
Atribusi pelaku	Sulit menentukan manusia yang berada di balik akun, perangkat, atau layanan AI yang digunakan.
Keaslian bukti	Konten sintetis membuat perbedaan antara bukti asli dan manipulasi menjadi lebih kompleks.
Yurisdiksi	Pelaku, korban, platform, dan server dapat berada di negara yang berbeda.
Kesenjangan teknologi	Kemampuan pelaku dapat berkembang lebih cepat daripada kapasitas penyidik dan laboratorium forensik.
Kekosongan/ketidakjelasan norma	Tidak semua modus AI memiliki rumusan pidana yang secara eksplisit menyebut teknologi AI.
Perlindungan korban	Konten palsu dapat menyebar sangat cepat dan menimbulkan kerugian reputasi, ekonomi, maupun psikologis.
Platform dan data	Akses terhadap log, metadata, dan informasi akun sering bergantung pada kebijakan penyedia layanan dan mekanisme hukum.

G. Strategi Penguatan Penegakan Hukum

- Pertama, peningkatan kapasitas penyidik dan aparat penegak hukum. Pendidikan dan pelatihan harus mencakup AI, forensik digital, analisis metadata, autentikasi konten, serta teknik penelusuran bukti elektronik.
- Kedua, penguatan laboratorium forensik digital. Pemeriksaan konten sintetis membutuhkan kemampuan untuk menganalisis karakter file, pola manipulasi, sumber data, dan hubungan antarartefak digital. Hasil pemeriksaan juga harus dapat dipertanggungjawabkan secara ilmiah dan prosedural di pengadilan.

- c. Ketiga, penguatan kerja sama dengan penyedia platform. Mekanisme permintaan data yang cepat, sah, terdokumentasi, dan menghormati hak pengguna diperlukan untuk mencegah hilangnya bukti digital.
- d. Keempat, penguatan kerja sama internasional. Karena kejahatan telematika dapat bersifat lintas batas, penegakan hukum perlu mengoptimalkan mutual legal assistance, kerja sama kepolisian, dan mekanisme pertukaran informasi yang sah.
- e. Kelima, harmonisasi regulasi. Indonesia memerlukan kebijakan AI yang komprehensif yang menghubungkan tata kelola AI, perlindungan data, keamanan siber, tanggung jawab penyelenggara, dan hukum pidana tanpa menghambat inovasi.
- f. Keenam, penguatan perlindungan korban. Penanganan perkara tidak boleh hanya berfokus pada pelaku. Negara perlu memperkuat mekanisme pelaporan, preservasi bukti, penghapusan atau pembatasan penyebaran konten ilegal sesuai kewenangan hukum, serta pemulihan kerugian korban.
- g. Ketujuh, penerapan penegakan hukum yang proporsional dan berbasis risiko. Tidak setiap penggunaan AI yang menghasilkan informasi yang keliru merupakan tindak pidana. Penegak hukum harus membedakan antara kesalahan, penggunaan yang sah, pelanggaran administratif, dan tindak pidana berdasarkan unsur hukum yang berlaku.

H. Konseptual Penegakan Hukum Kejahatan Telematika Berbasis AI

1. Identifikasi peristiwa digital →
2. Pengamanan dan preservasi bukti elektronik →
3. Pemeriksaan forensik dan autentikasi konten →
4. Identifikasi akun, perangkat, dan manusia pengendali →
5. Pemetaan perbuatan terhadap unsur delik →
6. Pembuktian kesalahan dan hubungan kausal →
7. Penentuan yurisdiksi dan mekanisme kerja sama bila lintas negara →
8. Penuntutan dan pemeriksaan di pengadilan →
9. Perlindungan/pemulihan korban serta evaluasi pencegahan.

Model tersebut menempatkan teknologi sebagai bagian dari alat bukti dan konteks perbuatan, bukan sebagai pusat pertanggungjawaban pidana. Dengan demikian, proses penegakan hukum dimulai dari fakta digital, tetapi berakhir pada penilaian yuridis terhadap perbuatan dan kesalahan manusia. Model ini juga selaras dengan kebutuhan penegakan hukum yang adaptif: prosedur tetap harus dipertahankan, tetapi kemampuan membaca perkembangan teknologi harus terus ditingkatkan.

IV. ANALISIS

Kehadiran AI memperlihatkan bahwa kejahatan telematika semakin bergeser dari serangan yang semata-mata bergantung pada keterampilan teknis menuju penyalahgunaan teknologi yang dapat meningkatkan kemampuan sosial dan manipulatif pelaku. Oleh karena itu, hukum pidana perlu memusatkan perhatian pada modus perbuatan, bukan semata-mata alat yang dipakai. Pendekatan ini menjaga agar hukum tidak selalu tertinggal setiap kali muncul teknologi baru.

Pada saat yang sama, pendekatan berbasis perbuatan tidak berarti bahwa kebutuhan regulasi AI dapat diabaikan. Ketika AI menjadi komponen penting dalam proses produksi konten, pengambilan keputusan, atau pemrosesan data, diperlukan tata kelola yang mampu mencegah risiko sebelum menjadi tindak pidana. Prinsip keamanan,

transparansi, akuntabilitas, dan perlindungan data dalam SE Menkominfo No. 9 Tahun 2023 dapat menjadi salah satu dasar kebijakan pencegahan.

Dari perspektif penegakan hukum, pelajaran dari penelitian Sudaryono dkk. menunjukkan pentingnya keseimbangan antara kepastian hukum dan kemampuan aparat menerjemahkan tujuan hukum dalam praktik. Pada kejahatan berbasis AI, keseimbangan tersebut semakin penting karena bukti dapat berubah dengan cepat dan teknologi dapat beroperasi lintas batas. Penegakan hukum harus tetap tunduk pada hukum acara dan kewenangan yang sah, namun aparat juga membutuhkan kapasitas untuk menghadapi teknologi baru.

Dengan demikian, tantangan utama Indonesia bukan semata-mata menciptakan 'pasal AI'. Tantangan yang lebih mendasar adalah membangun sistem hukum pidana yang mampu mengatribusikan perbuatan, menjaga integritas bukti, melindungi korban, dan menghubungkan fakta digital dengan unsur tindak pidana secara meyakinkan. Regulasi khusus dapat diperlukan untuk aspek tertentu, tetapi efektivitas penegakan hukum sangat bergantung pada kapasitas institusi dan kualitas sumber daya manusia.

V. PENUTUP

A. Kesimpulan

Artificial Intelligence merupakan sarana baru yang dapat memperkuat dan memperluas kejahatan telematika. Bentuk penyalahgunaannya antara lain impersonasi, penipuan, deepfake, rekayasa sosial, penyalahgunaan data pribadi, dan otomatisasi aktivitas digital yang melanggar hukum. Kerangka hukum Indonesia telah menyediakan sejumlah instrumen yang dapat digunakan untuk menanggulangi penyalahgunaan AI, terutama UU ITE, UU Pelindungan Data Pribadi, KUHP nasional, serta kebijakan etika AI. Namun, penerapan norma tersebut harus disesuaikan dengan konstruksi perbuatan dan unsur delik yang terbukti.

Tantangan utama terletak pada atribusi pelaku, autentikasi bukti digital, yurisdiksi lintas negara, keterbatasan kapasitas forensik, ketergantungan pada penyedia platform, serta kecepatan perkembangan teknologi. Karena itu, penegakan hukum harus diperkuat melalui peningkatan kompetensi aparat, laboratorium forensik, kerja sama lintas negara, tata kelola AI, dan perlindungan korban. Penelitian Sudaryono, M. Iksan, dan Kuswardani memberikan pelajaran penting bahwa penegakan hukum tidak boleh berhenti pada pelaksanaan prosedur formal. Dalam menghadapi kejahatan berbasis AI, hukum perlu diterjemahkan melalui aparat yang memiliki kompetensi teknologi, pengalaman, integritas, dan orientasi pada keadilan substantif, dengan tetap berada dalam batas hukum yang sah.

B. Saran

Pemerintah perlu memperkuat regulasi dan kebijakan tata kelola AI yang terintegrasi dengan keamanan siber, perlindungan data pribadi, dan hukum pidana. Kepolisian, kejaksaan, dan pengadilan perlu meningkatkan kompetensi AI dan forensik digital serta membangun mekanisme kerja bersama untuk penanganan bukti elektronik. Diperlukan penguatan kerja sama dengan penyedia platform dan negara lain untuk memperoleh bukti digital yang berada di luar wilayah Indonesia. Perlindungan korban harus ditempatkan sebagai bagian penting dari penegakan hukum, termasuk mekanisme pelaporan dan preservasi bukti yang cepat. Pengembangan kebijakan hukum AI

sebaiknya tetap mendorong inovasi yang sah, sekaligus memberikan batas tegas terhadap penggunaan AI yang secara sengaja digunakan untuk melakukan kejahatan.

DAFTAR PUSTAKA

- Komdigi/Kementerian Komunikasi dan Informatika Republik Indonesia. 2023. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.
- Republik Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- Republik Indonesia. 2023. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- Republik Indonesia. 2024. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. 2026. Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.
- Sudaryono, M. Iksan, dan Kuswardani. 2012. "Model Penyelesaian Secara Alternatif dalam Peradilan Pidana (Studi Khusus terhadap Model Penyelesaian Perkara Pidana oleh Lembaga Kepolisian)." Jurnal Penelitian Humaniora, Vol. 13, No. 1, Februari 2012, hlm. 62-73.
- Rahardjo, Satjipto. 2002. Sosiologi Hukum (Perkembangan Metode dan Pilihan Masalah). Surakarta: Muhammadiyah University Press.
- Rahardjo, Satjipto. 1983. Masalah Penegakan Hukum (Suatu Tinjauan Sosiologis). Bandung: Sinar Baru.
- Sudarto. 1977. Hukum dan Hukum Pidana. Bandung: Alumni.
- Soekanto, Soerjono. 1979. Masalah Penegakan Hukum dan Kesadaran Hukum. Jakarta: Universitas Indonesia.