SETARA
JURNAL ILMU HUKUM

Volume 5, No. 2 (2024)
DOI: 10.59017/setara.v5i2.559
P-ISSN 2655-2264 | ISSN-L 2963-1297
Pascasarjana Universitas Bung Karno
Pegangsaan Timur No.17, Menteng, Jakarta, Indonesia

REFORMULASI KEBIJAKAN KRIMINAL DALAM PENANGGULANGAN KEJAHATAN BERBASIS TEKNOLOGI KECERDASAN BUATAN

Reformulating Criminal Policy in Combating Artificial Intelligence-Based Crime

Imam Subekti[1], Elly Kristiani Purwendah[2*], Heru Sukrisno[3], Sugeng Wahyudi[4]

[1,2,3,4] Fakultas Hukum, Universitas Wijayakusuma Purwokerto, Indonesia

[*]Email: ellykpurwendah@gmail.com

Abstract

The reformulation of criminal policy in combating artificial intelligence (AI)-based crime has become an urgent issue as technology develops rapidly. This study examines legal challenges related to digital crime, regulatory strengthening, and the role of law enforcement institutions in addressing these problems. The method used is a literature study with a qualitative approach. The study finds the need for AI-specific regulation, the establishment or strengthening of institutions competent in technology, and international cooperation in combating AI-based crime. Such policy reform is expected to create a legal system that is more responsive to digital threats.

Keywords: Criminal Policy; Artificial Intelligence; Digital Crime; AI Regulation; International Cooperation

Abstrak

Reformulasi kebijakan kriminal dalam penanggulangan kejahatan berbasis kecerdasan buatan (AI) menjadi isu mendesak seiring perkembangan teknologi yang pesat. Studi ini mengkaji tantangan hukum terkait kejahatan digital, penguatan regulasi, serta peran lembaga penegakan hukum dalam mengatasi masalah ini. Metode yang digunakan adalah studi literatur dengan pendekatan kualitatif. Hasil penelitian menunjukkan perlunya regulasi spesifik yang mengatur AI, pembentukan lembaga yang kompeten dalam teknologi, dan kerja sama internasional dalam penanggulangan kejahatan berbasis AI. Reformulasi kebijakan ini diharapkan dapat menciptakan sistem hukum yang lebih responsif terhadap ancaman digital.

Kata Kunci: Kebijakan Kriminal; Kecerdasan Buatan; Kejahatan Digital; Regulasi AI; Kerja Sama Internasional

1. Pendahuluan

Perkembangan kecerdasan buatan membawa perubahan besar dalam kehidupan sosial, ekonomi, dan hukum. Teknologi ini dapat digunakan untuk meningkatkan efisiensi layanan, mempercepat analisis data, membantu pengambilan keputusan, dan memperluas inovasi.[1] Namun pada saat yang sama, kecerdasan buatan juga dapat dipakai untuk melakukan atau mempermudah tindak kejahatan. Kemampuan sistem AI untuk

[1]Stuart Russell dan Peter Norvig, *Artificial intelligence: A modern approach*, 4th ed. (Harlow: Pearson, 2021).

menghasilkan teks, suara, gambar, video, prediksi perilaku, dan otomatisasi keputusan menimbulkan tantangan baru bagi hukum pidana.

Kejahatan berbasis teknologi kecerdasan buatan tidak selalu hadir sebagai jenis tindak pidana yang sepenuhnya baru. Sebagian merupakan perluasan dari kejahatan lama, seperti penipuan, pemerasan, pencemaran nama baik, penyalahgunaan data pribadi, manipulasi informasi, atau serangan siber.[2] Perbedaannya terletak pada skala, kecepatan, tingkat otomatisasi, dan kemampuan meniru identitas atau perilaku manusia. Dalam konteks inilah kebijakan kriminal yang ada perlu dievaluasi.

Kebijakan kriminal tidak dapat hanya bereaksi setelah kejahatan terjadi. Ia harus mampu mengantisipasi perubahan modus, menyesuaikan rumusan norma, meningkatkan kapasitas penegak hukum, dan membangun kerja sama lintas negara.[3] AI membuat batas yurisdiksi semakin kabur karena pelaku, korban, sistem, server, dan bukti elektronik dapat berada di wilayah yang berbeda. Tanpa reformulasi, sistem hukum akan selalu tertinggal dari teknologi.

Artikel ini membahas reformulasi kebijakan kriminal dalam penanggulangan kejahatan berbasis teknologi kecerdasan buatan. Fokusnya meliputi tantangan hukum kejahatan digital, kebutuhan regulasi spesifik AI, pembentukan kelembagaan yang kompeten secara teknologi, dan kerja sama internasional.

1.1 Kontribusi Artikel

Kontribusi utama artikel ini adalah menawarkan kerangka reformulasi kebijakan kriminal berbasis empat pilar: regulasi adaptif, kapasitas kelembagaan, tata kelola bukti digital, dan kerja sama internasional. Kerangka ini penting karena banyak pembahasan AI dalam hukum pidana masih berhenti pada kekhawatiran umum. Artikel ini mengarahkan pembahasan pada desain kebijakan yang dapat digunakan untuk memperkuat sistem hukum.

Kontribusi kedua adalah membedakan antara AI sebagai alat, AI sebagai lingkungan kejahatan, dan AI sebagai objek pengaturan. Sebagai alat, AI digunakan pelaku untuk mempercepat atau menyamarkan kejahatan. Sebagai lingkungan, AI menciptakan ruang baru tempat data, identitas digital, dan sistem otomatis saling berinteraksi. Sebagai objek pengaturan, AI memerlukan standar tanggung jawab, transparansi, keamanan, dan pengawasan. Pembedaan ini membantu pembentuk undang-undang agar tidak merumuskan norma secara terlalu umum.

Kontribusi ketiga adalah menekankan bahwa penanggulangan kejahatan AI tidak cukup dilakukan melalui kriminalisasi. Kebijakan kriminal yang baik harus memadukan hukum pidana, pencegahan administratif, penguatan literasi digital, audit teknologi, perlindungan data pribadi, dan koordinasi internasional. Dengan demikian, artikel ini menawarkan pendekatan yang lebih komprehensif dibandingkan respons pidana yang semata-mata represif.

2. Metode Penelitian

Penelitian ini menggunakan studi literatur dengan pendekatan kualitatif. Literatur yang dikaji mencakup peraturan perundang-undangan terkait kejahatan digital, perlindungan

[2]Susan W. Brenner, *Cybercrime: Criminal threats from cyberspace* (Santa Barbara: Praeger, 2010).
[3]Barda Nawawi Arief, *Bunga rampai kebijakan hukum pidana* (Jakarta: Kencana, 2011).

data pribadi, hukum pidana, serta literatur mengenai AI governance, cybercrime, dan kebijakan kriminal.[4] Pendekatan kualitatif digunakan untuk membaca kecenderungan perkembangan teknologi dan menilai kecukupan kebijakan hukum yang tersedia.

Analisis dilakukan melalui tiga tahap. Pertama, mengidentifikasi bentuk tantangan hukum yang muncul dari penggunaan AI dalam kejahatan digital. Kedua, menilai kebutuhan pembaruan regulasi dan kelembagaan. Ketiga, merumuskan arah kebijakan kriminal yang responsif terhadap ancaman digital tanpa mengabaikan hak asasi manusia, kepastian hukum, dan prinsip proporsionalitas.

3. Hasil dan Pembahasan

3.1 Tantangan Hukum Kejahatan Digital Berbasis AI

Kejahatan berbasis AI menimbulkan tantangan hukum karena teknologi tersebut dapat memperbesar kemampuan pelaku. AI dapat digunakan untuk membuat pesan penipuan yang sangat meyakinkan, meniru suara atau wajah seseorang, mengotomatisasi serangan terhadap sistem, dan memanipulasi informasi publik.[5] Dalam situasi seperti ini, korban dapat kesulitan membedakan komunikasi asli dan palsu. Penegak hukum juga menghadapi kesulitan karena jejak digital dapat dibuat secara masif dan tersebar.

Tantangan pertama adalah persoalan atribusi. Dalam kejahatan konvensional, hubungan antara pelaku dan perbuatan sering lebih mudah ditelusuri. Dalam kejahatan berbasis AI, pelaku dapat menggunakan sistem otomatis, identitas palsu, perangkat perantara, dan infrastruktur lintas negara. Pertanyaan tentang siapa yang bertanggung jawab menjadi lebih rumit, terutama ketika teknologi digunakan oleh banyak pihak atau ketika sistem bekerja secara semiotonom.

Tantangan kedua adalah kecepatan dan skala. AI dapat memperbanyak konten, pesan, atau serangan dalam jumlah besar dengan biaya rendah. Kejahatan yang dulu membutuhkan banyak tenaga manusia kini dapat dilakukan melalui otomatisasi. Hal ini menuntut penegak hukum memiliki kemampuan deteksi yang juga cepat dan berbasis teknologi.

Tantangan ketiga adalah pembuktian. Bukti digital dalam perkara AI dapat berupa data pelatihan, log sistem, metadata, model, prompt, keluaran sistem, atau jejak transaksi. Tidak semua penegak hukum memiliki kapasitas untuk membaca dan mengamankan jenis bukti tersebut. Jika prosedur pengamanan bukti tidak tepat, bukti dapat diragukan keasliannya.

3.2 AI sebagai Alat, Lingkungan, dan Objek Pengaturan

Reformulasi kebijakan kriminal perlu dimulai dengan pemetaan posisi AI. Pertama, AI sebagai alat kejahatan. Dalam posisi ini, pelaku menggunakan AI untuk melakukan kejahatan yang sudah dikenal hukum, misalnya penipuan digital, pemalsuan identitas, penyebaran konten manipulatif, atau pemerasan. Norma pidana yang ada dapat dipakai, tetapi sering perlu diperkuat agar mampu menjangkau modus yang lebih kompleks.

Kedua, AI sebagai lingkungan kejahatan. Dalam posisi ini, AI tidak hanya menjadi alat, tetapi menjadi bagian dari ekosistem digital tempat interaksi berlangsung. Platform,

[4]Peter Mahmud Marzuki, *Penelitian hukum* (Jakarta: Kencana, 2017); Soerjono Soekanto dan Sri Mamudji, *Penelitian hukum normatif: Suatu tinjauan singkat* (Jakarta: RajaGrafindo Persada, 2015).
[5]Ian Goodfellow, Yoshua Bengio, dan Aaron Courville, *Deep learning* (Cambridge: MIT Press, 2016).

algoritma rekomendasi, sistem verifikasi, dan basis data saling terhubung. Kejahatan dapat terjadi karena celah dalam desain sistem, lemahnya pengawasan, atau penyalahgunaan data. Kebijakan kriminal harus mampu membaca ekosistem ini, bukan hanya tindakan individual pelaku.

Ketiga, AI sebagai objek pengaturan. Dalam posisi ini, negara perlu menentukan standar pengembangan dan penggunaan AI. Standar tersebut dapat mencakup keamanan, akuntabilitas, perlindungan data, transparansi, audit risiko, dan kewajiban pelaporan insiden. Tanpa standar, penegakan hukum hanya bekerja setelah kerugian terjadi.

3.3 Penguatan Regulasi, Kelembagaan, dan Kerja Sama Internasional

Regulasi yang ada belum sepenuhnya dirancang untuk menghadapi kompleksitas AI. Undang-undang terkait informasi elektronik, perlindungan data pribadi, dan hukum pidana dapat digunakan untuk sebagian perbuatan, tetapi belum tentu cukup untuk mengatur risiko khusus seperti deepfake, keputusan otomatis yang merugikan, manipulasi algoritmik, atau penyalahgunaan model generatif.[6] Karena itu, regulasi spesifik AI diperlukan.

Regulasi spesifik tidak harus selalu berarti undang-undang pidana baru yang memperbanyak ancaman hukuman. Regulasi dapat berupa standar tata kelola, kewajiban uji risiko, kewajiban transparansi pada penggunaan AI tertentu, serta sanksi administratif dan pidana untuk pelanggaran serius. Dengan model ini, hukum tidak hanya menghukum pelaku, tetapi juga mencegah desain dan penggunaan AI yang berbahaya.

Kelembagaan menjadi pilar kedua. Penegak hukum memerlukan unit yang memahami teknologi AI, forensik digital, pelacakan data, dan analisis pola. Tanpa kapasitas tersebut, norma hukum yang baik tidak akan efektif. Lembaga penegak hukum juga perlu bekerja sama dengan penyelenggara sistem elektronik, ahli teknologi, lembaga perlindungan data, dan otoritas keamanan siber.

Kerja sama internasional menjadi pilar ketiga karena kejahatan berbasis AI sering melintasi batas negara. Pelaku dapat beroperasi dari satu negara, menggunakan layanan di negara lain, dan menyerang korban di negara berbeda. Proses permintaan data, ekstradisi, bantuan hukum timbal balik, dan pertukaran informasi harus diperkuat. Jika kerja sama internasional lambat, pelaku dapat memanfaatkan perbedaan yurisdiksi untuk menghindari penegakan hukum.

3.4 Reformulasi Kebijakan Kriminal

Reformulasi kebijakan kriminal harus dilakukan secara bertahap. Tahap pertama adalah pemetaan risiko. Negara perlu mengidentifikasi bentuk penggunaan AI yang paling berpotensi menimbulkan kerugian hukum, seperti pemalsuan identitas digital, manipulasi informasi publik, serangan siber otomatis, penyalahgunaan data pribadi, dan eksploitasi kelompok rentan.[7] Pemetaan risiko membantu menentukan prioritas regulasi.

Tahap kedua adalah pembaruan norma. Norma pidana harus cukup jelas agar

[6] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

[7] Badan Pengkajian dan Penerapan Teknologi, *Strategi nasional kecerdasan artifisial Indonesia 2020–2045* (Jakarta: BPPT, 2020).

tidak menimbulkan ketidakpastian hukum, tetapi cukup adaptif agar tidak cepat usang. Rumusan yang terlalu teknis dapat tertinggal ketika teknologi berubah. Sebaliknya, rumusan yang terlalu umum dapat mengancam kebebasan berekspresi dan inovasi. Karena itu, pembaruan norma perlu menggabungkan unsur perbuatan, akibat, kesengajaan, dan tingkat risiko.

Tahap ketiga adalah penguatan pencegahan. Kebijakan kriminal modern tidak boleh hanya mengandalkan pemidanaan. Pencegahan dapat dilakukan melalui literasi digital, kewajiban keamanan sistem, audit teknologi, dan mekanisme pelaporan cepat. Dalam konteks AI, pencegahan menjadi sangat penting karena kerugian dapat menyebar dalam waktu singkat.

Tahap keempat adalah peningkatan kapasitas penegakan hukum. Penyidik, jaksa, hakim, dan lembaga pendukung harus memahami karakter bukti digital dan teknologi AI. Pelatihan tidak boleh hanya bersifat umum, tetapi harus mencakup simulasi kasus, standar forensik, teknik pelacakan, dan etika penggunaan teknologi oleh penegak hukum.

3.5 Prinsip Hak Asasi Manusia dan Proporsionalitas

Reformulasi kebijakan kriminal AI harus memperhatikan hak asasi manusia. Kekhawatiran terhadap kejahatan digital tidak boleh menjadi alasan untuk membangun pengawasan yang berlebihan. Negara perlu menjaga keseimbangan antara keamanan, privasi, kebebasan berekspresi, dan inovasi.[8] Kebijakan yang terlalu represif dapat menghambat perkembangan teknologi yang bermanfaat.

Prinsip proporsionalitas penting dalam menentukan sanksi. Tidak semua pelanggaran terkait AI harus dipidana berat. Pelanggaran administratif atau kelalaian teknis dapat diselesaikan dengan sanksi administratif, perintah perbaikan, atau denda. Hukum pidana sebaiknya digunakan untuk perbuatan yang menimbulkan kerugian serius, dilakukan dengan kesengajaan, atau mengancam kepentingan publik secara signifikan.

Selain itu, penggunaan AI oleh penegak hukum juga harus diawasi. AI dapat membantu analisis data dan deteksi pola, tetapi tidak boleh menggantikan penilaian manusia dalam keputusan yang membatasi hak seseorang. Transparansi, audit, dan mekanisme keberatan harus tersedia agar teknologi tidak menimbulkan ketidakadilan baru.

3.6 Model Kebijakan yang Diusulkan

Artikel ini mengusulkan model kebijakan kriminal berbasis ekosistem. Model ini terdiri dari lima unsur. Pertama, regulasi AI yang membedakan tingkat risiko penggunaan. Kedua, penyesuaian hukum pidana untuk menjerat penggunaan AI dalam kejahatan serius. Ketiga, penguatan perlindungan data pribadi sebagai fondasi pencegahan. Keempat, pembentukan atau penguatan lembaga teknis yang kompeten dalam AI dan forensik digital. Kelima, kerja sama internasional yang cepat dan operasional.

Model berbasis ekosistem penting karena kejahatan AI tidak dapat ditangani oleh satu instrumen. Jika hanya mengandalkan hukum pidana, negara akan selalu tertinggal. Jika hanya mengandalkan regulasi administratif, pelaku serius tidak akan memperoleh efek jera yang memadai. Jika hanya mengandalkan teknologi, hak warga

[8] UNESCO, *Recommendation on the ethics of artificial intelligence* (Paris: UNESCO, 2021); Organisation for Economic Co-operation and Development, *OECD principles on artificial intelligence* (Paris: OECD, 2019).

dapat terabaikan. Oleh karena itu, kebijakan kriminal harus memadukan instrumen hukum, teknologi, kelembagaan, dan kerja sama.

Dengan model tersebut, sistem hukum dapat bergerak dari pola reaktif menuju pola antisipatif. Tujuannya bukan menghambat inovasi AI, melainkan memastikan teknologi tersebut berkembang dalam koridor yang aman, akuntabel, dan menghormati hukum.

3.7 Kebutuhan Kapasitas Forensik Digital

Salah satu titik lemah dalam penanggulangan kejahatan berbasis AI adalah kapasitas forensik digital. Kejahatan yang memanfaatkan AI sering meninggalkan jejak yang tidak mudah dibaca dengan metode pemeriksaan biasa. Penegak hukum perlu memahami metadata, sumber data, pola otomatisasi, jejak akses, perubahan file, dan kemungkinan manipulasi konten. Tanpa kapasitas ini, pembuktian dapat berhenti pada dugaan.

Forensik digital dalam perkara AI juga harus mampu membedakan konten asli, konten hasil manipulasi, dan konten hasil generasi sistem. Perbedaan ini penting karena konsekuensi hukumnya berbeda. Misalnya, penyebaran video palsu yang menyerupai seseorang dapat melibatkan pemalsuan, pencemaran nama baik, pelanggaran data pribadi, atau pemerasan. Untuk membuktikan perbuatan tersebut, penyidik memerlukan metode teknis yang dapat diterima di pengadilan.

Kapasitas forensik tidak hanya dibutuhkan oleh penyidik. Jaksa perlu memahami karakter bukti agar dapat menyusun dakwaan dan pembuktian secara tepat. Hakim juga perlu memahami batas kemampuan teknologi agar dapat menilai keterangan ahli secara kritis. Jika hakim hanya menerima istilah teknis tanpa pemahaman dasar, putusan dapat terlalu bergantung pada ahli tertentu. Karena itu, pelatihan lintas lembaga menjadi kebutuhan mendesak.

3.8 Tanggung Jawab Penyelenggara Sistem dan Pengembang AI

Kebijakan kriminal AI tidak boleh hanya menargetkan pelaku akhir. Penyelenggara sistem elektronik, pengembang AI, dan penyedia platform memiliki peran dalam mencegah penyalahgunaan. Mereka tidak selalu dapat dipidana atas setiap penyalahgunaan oleh pengguna, tetapi mereka harus memiliki kewajiban pencegahan yang wajar. Kewajiban tersebut dapat berupa desain keamanan, pembatasan penggunaan berbahaya, mekanisme pelaporan, dan respons cepat terhadap insiden.

Tanggung jawab ini harus dirumuskan secara proporsional. Jika terlalu berat, inovasi dapat terhambat dan pelaku usaha kecil sulit berkembang. Jika terlalu ringan, platform dapat menghindar dari tanggung jawab meskipun sistemnya jelas memfasilitasi penyalahgunaan. Oleh karena itu, pendekatan berbasis risiko menjadi penting. Sistem AI dengan risiko tinggi harus memiliki kewajiban lebih ketat dibandingkan aplikasi berisiko rendah.

Dalam konteks pidana, tanggung jawab korporasi dapat dipertimbangkan apabila penyelenggara sistem secara sengaja membiarkan atau mengambil keuntungan dari penyalahgunaan yang serius. Namun untuk kelalaian biasa, sanksi administratif, perintah perbaikan, dan denda dapat lebih tepat. Pembagian ini menunjukkan bahwa reformulasi kebijakan kriminal tidak identik dengan perluasan pemidanaan, tetapi dengan penem-

patan sanksi secara tepat.

3.9 Perlindungan Korban Kejahatan AI

Korban kejahatan berbasis AI sering menghadapi kerugian yang cepat menyebar. Konten palsu dapat tersebar luas dalam hitungan menit. Identitas digital dapat disalahgunakan berkali-kali. Data pribadi dapat berpindah ke banyak pihak. Karena itu, kebijakan kriminal harus memasukkan perlindungan korban sebagai bagian utama, bukan sekadar tambahan setelah pelaku dihukum.

Perlindungan korban dapat mencakup mekanisme penghapusan atau pembatasan akses terhadap konten berbahaya, pemulihan identitas digital, bantuan psikologis untuk korban manipulasi seksual atau pemerasan, serta kompensasi atas kerugian tertentu. Dalam perkara deepfake atau manipulasi identitas, pemulihan reputasi juga penting karena kerugian tidak hanya bersifat finansial.

Kebijakan perlindungan korban perlu melibatkan platform digital. Platform memiliki kemampuan teknis untuk menurunkan konten, membatasi penyebaran, dan menyimpan bukti. Namun tindakan platform harus tetap berada dalam kerangka hukum agar tidak menjadi sensor sewenang-wenang. Negara perlu membuat prosedur yang cepat, jelas, dan dapat diawasi.

3.10 Arah Pembaruan Hukum Pidana Nasional

Pembaruan hukum pidana nasional harus memperhatikan perkembangan teknologi AI. Rumusan tindak pidana yang berkaitan dengan pemalsuan, penipuan, akses ilegal, manipulasi data, dan penyebaran konten elektronik perlu ditafsirkan dan, bila perlu, diperbarui agar dapat menjangkau modus berbasis AI. Namun pembaruan itu harus tetap menjaga asas legalitas. Warga harus dapat mengetahui perbuatan apa yang dilarang dan ancaman apa yang dapat dikenakan.

Hukum pidana juga perlu mengatur faktor pemberatan. Penggunaan AI dapat menjadi faktor pemberatan apabila memperbesar skala korban, menyasar kelompok rentan, menimbulkan gangguan publik besar, atau dilakukan secara terorganisasi. Dengan cara ini, hukum tidak menghukum teknologi, tetapi menghukum penyalahgunaan teknologi yang meningkatkan bahaya sosial.

Di sisi lain, pembaruan hukum harus menghindari kriminalisasi berlebihan terhadap riset, eksperimen, atau penggunaan AI yang sah. Peneliti keamanan siber, akademisi, dan pengembang yang bekerja untuk tujuan sah tidak boleh diperlakukan sama dengan pelaku kejahatan. Oleh karena itu, norma pengecualian, pembelaan hukum, atau mekanisme perizinan penelitian dapat dipertimbangkan.

3.11 Literasi Digital sebagai Kebijakan Pencegahan

Literasi digital merupakan bagian penting dari kebijakan kriminal preventif. Masyarakat yang tidak memahami cara kerja manipulasi digital lebih mudah menjadi korban penipuan, pemalsuan identitas, atau penyebaran informasi palsu. Dalam konteks AI generatif, literasi digital harus mencakup kemampuan mengenali konten manipulatif, memverifikasi sumber informasi, menjaga data pribadi, dan melaporkan insiden secara tepat.

Pendidikan literasi digital tidak boleh hanya ditujukan kepada pengguna umum.

Aparatur pemerintah, pendidik, jurnalis, pelaku usaha, dan kelompok rentan juga membutuhkan program khusus. Setiap kelompok menghadapi risiko berbeda. Jurnalis menghadapi risiko disinformasi, pelaku usaha menghadapi penipuan berbasis identitas, sedangkan anak dan remaja menghadapi risiko manipulasi emosional melalui platform digital.

Literasi digital memperkuat efektivitas hukum pidana karena mengurangi jumlah korban dan mempercepat pelaporan. Penegakan hukum akan selalu terbatas jika masyarakat tidak mampu mengenali ancaman sejak awal. Karena itu, reformulasi kebijakan kriminal AI harus memadukan norma, lembaga, teknologi, dan pendidikan publik.

3.12 Peta Jalan Implementasi Kebijakan

Reformulasi kebijakan kriminal berbasis AI memerlukan peta jalan implementasi. Tahap pertama adalah audit regulasi. Pemerintah perlu memetakan norma yang sudah ada dalam hukum pidana, hukum informasi elektronik, perlindungan data pribadi, dan keamanan siber. Audit ini menentukan bagian mana yang cukup ditafsirkan, bagian mana yang perlu diperbarui, dan bagian mana yang membutuhkan instrumen hukum baru.

Tahap kedua adalah penyusunan standar teknis. Standar teknis diperlukan agar penegak hukum, penyelenggara sistem, dan pengembang memiliki bahasa yang sama mengenai risiko AI. Standar tersebut dapat mencakup pelaporan insiden, penyimpanan log, pengamanan data, audit sistem, dan prosedur pembuktian. Tanpa standar teknis, norma hukum akan sulit dilaksanakan secara konsisten.

Tahap ketiga adalah pembentukan mekanisme koordinasi nasional. Kejahatan AI tidak dapat ditangani oleh satu lembaga. Kepolisian, kejaksaan, pengadilan, otoritas perlindungan data, lembaga keamanan siber, kementerian terkait, dan penyelenggara sistem elektronik harus memiliki kanal koordinasi yang jelas. Kanal ini perlu digunakan bukan hanya setelah perkara muncul, tetapi juga untuk pencegahan dan pertukaran informasi risiko.

Tahap keempat adalah evaluasi berkala. Teknologi AI berubah cepat sehingga kebijakan yang disusun hari ini dapat menjadi usang dalam beberapa tahun. Evaluasi berkala memungkinkan negara menyesuaikan aturan tanpa selalu menunggu krisis besar. Dengan peta jalan tersebut, reformulasi kebijakan kriminal tidak berhenti sebagai gagasan normatif, tetapi bergerak menjadi agenda kelembagaan yang dapat dijalankan.

4. Penutup

Kejahatan berbasis teknologi kecerdasan buatan menuntut reformulasi kebijakan kriminal karena karakter kejahatannya berbeda dari kejahatan digital konvensional. AI memperbesar skala, kecepatan, kerumitan atribusi, dan tantangan pembuktian. Oleh sebab itu, respons hukum tidak cukup hanya menggunakan norma yang ada tanpa penguatan.

Reformulasi kebijakan kriminal harus mencakup regulasi spesifik AI, penguatan kapasitas lembaga penegak hukum, tata kelola bukti digital, perlindungan data pribadi, dan kerja sama internasional. Kebijakan tersebut perlu disusun secara proporsional agar mampu melindungi masyarakat tanpa menghambat inovasi dan tanpa melanggar hak asasi manusia. Dengan pendekatan berbasis ekosistem, sistem hukum Indonesia dapat menjadi lebih responsif terhadap ancaman digital yang berkembang.

Daftar Pustaka

Buku dan Artikel Ilmiah

Barda Nawawi Arief. (2011). *Bunga rampai kebijakan hukum pidana.* Kencana.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace.* Praeger.

Floridi, L. (2019). Establishing the rules for building trustworthy AI. *Nature Machine Intelligence, 1*, 261–262.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning.* MIT Press.

Marzuki, P. M. (2017). *Penelitian hukum.* Kencana.

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Soekanto, S., & Mamudji, S. (2015). *Penelitian hukum normatif: Suatu tinjauan singkat.* RajaGrafindo Persada.

Dokumen Kebijakan dan Peraturan

Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Badan Pengkajian dan Penerapan Teknologi. (2020). *Strategi nasional kecerdasan artifisial Indonesia 2020–2045.*

Organisation for Economic Co-operation and Development. (2019). *OECD principles on artificial intelligence.*

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence.*