INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 1 Tahun 2025 Page 3436-3451
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI

Wahyudi BR
Fakultas Hukum Universitas Yapis Papua
Email : wahyudiburhan79@gmail.com

Abstrak

Kecerdasan buatan (*Artificial Intelligence*/AI) telah mengubah lanskap sosial dan ekonomi global, namun juga menghadirkan tantangan serius dalam bentuk kejahatan berbasis teknologi. Penelitian ini bertujuan untuk mengidentifikasi tantangan hukum dalam penegakan terhadap kejahatan berbasis AI, mengevaluasi efektivitas regulasi hukum yang ada di Indonesia dan tingkat internasional, serta merumuskan kerangka hukum yang lebih adaptif dan progresif. Dengan menggunakan metode normatif, pendekatan perundang-undangan, konseptual, dan komparatif diterapkan untuk menganalisis celah regulasi, tantangan teknis, dan hambatan lintas yurisdiksi. Hasil penelitian menunjukkan bahwa regulasi yang ada, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), belum mencakup kompleksitas kejahatan berbasis AI, seperti serangan siber adaptif, manipulasi data berskala besar, dan penyalahgunaan *deepfake*. Di tingkat internasional, meskipun Konvensi Budapest menjadi rujukan utama, regulasi ini belum mencakup eksplisit kejahatan AI. Tantangan lain meliputi lambatnya proses legislasi, keterbatasan kapasitas teknis aparat penegak hukum, serta kurangnya koordinasi internasional dalam menangani sifat transnasional kejahatan AI. Penelitian ini merekomendasikan pembaruan regulasi untuk mencakup definisi, mekanisme tanggung jawab, dan sanksi terkait AI, disertai peningkatan kapasitas teknis aparat penegak hukum melalui pelatihan dan pengembangan infrastruktur. Selain itu, kolaborasi internasional dan harmonisasi hukum global menjadi prioritas untuk memastikan penegakan hukum yang efektif. Langkah ini diharapkan mampu menjadikan hukum lebih adaptif, progresif, dan responsif dalam mengatasi ancaman kejahatan berbasis AI.

Kata Kunci: Kecerdasan Buatan, Penegakan Hukum, Kejahatan Siber

Abstract

Artificial Intelligence (AI) has transformed the global social and economic landscape, but also presents serious challenges in the form of technology-based crimes. This study aims to identify legal challenges in enforcing AI-based crimes, evaluate the effectiveness of existing legal regulations in Indonesia and internationally, and formulate a more adaptive and progressive legal framework. Using normative methods, legislative, conceptual, and comparative approaches are applied to analyze regulatory gaps, technical challenges, and cross-jurisdictional barriers. The results of the study show that existing regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), do not yet cover the complexity of AI-based crimes, such as adaptive cyber attacks, large-scale data manipulation, and deepfake abuse. At the international level, although the Budapest Convention is the main reference, this regulation does not explicitly cover AI crimes. Other challenges include the slow legislative process, limited technical capacity of law enforcement officers, and lack of international coordination in dealing with the transnational nature of AI crimes. This study recommends updating regulations to include definitions, liability mechanisms, and sanctions related to AI, along with increasing the technical capacity of law enforcement officers through training and infrastructure development. In addition, international collaboration and global legal harmonization are priorities to ensure effective law enforcement. This step is expected to make the law more adaptive, progressive, and responsive in addressing the threat of AI-based crimes.

Keywords: Artificial Intelligence, Law Enforcement, Cybercrime

PENDAHULUAN

Kecerdasan buatan (*Artificial Intelligence*/AI) telah menjadi salah satu teknologi yang paling berpengaruh di era digital. AI tidak hanya merevolusi cara manusia bekerja, tetapi juga memperkenalkan tantangan baru dalam berbagai bidang, termasuk penegakan hukum (Rahman et al., 2024). Secara konseptual, AI merujuk pada sistem atau mesin yang mampu meniru kecerdasan manusia, seperti pengambilan keputusan, pemrosesan bahasa alami, dan pembelajaran dari data yang tersedia. Teknologi ini beroperasi melalui algoritma yang kompleks dan sering kali mampu bertindak secara otonom, tanpa campur tangan manusia secara langsung. Namun, sifat otonomi dan kemampuan AI yang canggih justru menciptakan celah hukum yang rentan dimanfaatkan untuk kejahatan berbasis teknologi.

Dari sudut pandang hukum, regulasi terhadap AI dan teknologi digital secara umum masih dalam tahap perkembangan. Di Indonesia, misalnya, kerangka hukum terkait teknologi sebagian besar berakar pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diubah melalui Undang-Undang Nomor 19 Tahun 2016 (Puluhulawa et al., 2023). Meskipun UU ITE memberikan landasan hukum untuk mengatur

aktivitas dunia maya, regulasi ini belum sepenuhnya menjangkau kompleksitas kejahatan berbasis AI. Di tingkat global, instrumen hukum internasional, seperti Konvensi Budapest tentang Kejahatan Siber, juga belum secara eksplisit mencakup kejahatan berbasis AI. Hal ini menimbulkan kesenjangan regulasi yang berpotensi memperparah tantangan penegakan hukum di era AI.

Permasalahan ini semakin kompleks ketika AI digunakan untuk melakukan kejahatan. Awalnya, AI diciptakan untuk mempermudah pekerjaan manusia dan meningkatkan efisiensi di berbagai sektor (Abdussamad & Muhtar, 2022). Namun, kemampuan AI untuk melakukan otomatisasi dan analisis data skala besar juga menarik perhatian pelaku kejahatan. Kejahatan berbasis AI melibatkan pemanfaatan teknologi ini untuk melakukan tindakan ilegal, seperti manipulasi data, serangan siber, pencurian identitas, hingga penyebaran disinformasi melalui *deepfake*. *Deepfake*, misalnya, adalah teknologi berbasis AI yang mampu memanipulasi video atau audio seseorang sehingga tampak autentik. Dalam kasus tertentu, *deepfake* telah digunakan untuk merusak reputasi individu, menyebarkan informasi palsu, bahkan melakukan pemerasan.

Salah satu contoh kasus yang menarik perhatian dunia adalah serangan siber berbasis AI terhadap perusahaan besar di Amerika Serikat. Pada tahun 2020, sebuah serangan siber menggunakan algoritma AI canggih berhasil mencuri data sensitif jutaan pengguna dari salah satu perusahaan teknologi terkemuka. Pelaku menggunakan AI untuk menyusup ke sistem keamanan perusahaan dengan cara yang sulit dideteksi, termasuk menggunakan program yang dapat beradaptasi dengan sistem keamanan baru dalam hitungan detik (Al-Hadrawi et al., 2024). Peristiwa ini menunjukkan bagaimana AI tidak hanya menjadi alat bantu manusia, tetapi juga senjata yang sangat efektif dalam melakukan kejahatan. Di sisi lain, di Asia, kasus penyalahgunaan AI untuk membuat *deepfake* yang digunakan dalam skandal politik di beberapa negara menunjukkan bahwa teknologi ini juga dapat digunakan untuk merusak tatanan sosial dan politik.

Permasalahan utama yang muncul adalah bagaimana hukum dapat mengatasi perkembangan kejahatan berbasis AI yang begitu dinamis. Tantangan terbesar terletak pada kecepatan perkembangan teknologi dibandingkan dengan kecepatan pembaruan regulasi hukum. AI berkembang dalam hitungan bulan, sedangkan proses legislasi sering kali membutuhkan waktu bertahun-tahun (Hakim et al., 2023). Akibatnya, hukum cenderung tertinggal dalam menghadapi kejahatan berbasis AI. Hal ini memberikan keuntungan bagi pelaku kejahatan yang selalu berada selangkah lebih maju dibandingkan penegak hukum.

Selain itu, sifat AI yang otonom juga menimbulkan pertanyaan fundamental dalam hukum, yakni mengenai tanggung jawab pidana. Jika sebuah AI bertindak secara independen

dan melakukan kejahatan, siapakah yang bertanggung jawab? Apakah pengembang AI, pengguna, atau sistem itu sendiri? Dalam hukum pidana tradisional, pertanggungjawaban pidana didasarkan pada niat atau kesalahan manusia (mens rea). Namun, dalam konteks AI, niat manusia sulit dibuktikan, terutama jika sistem AI bertindak berdasarkan algoritma yang tidak sepenuhnya dipahami oleh pengembang atau pengguna.

Tantangan lainnya adalah keterbatasan kemampuan penegak hukum dalam memahami teknologi AI. Kejahatan berbasis AI sering kali melibatkan teknologi yang sangat kompleks, yang memerlukan pengetahuan mendalam untuk mengidentifikasi, menganalisis, dan membuktikan pelanggaran hukum. Di banyak negara, termasuk Indonesia, keterbatasan sumber daya manusia, infrastruktur, dan teknologi menjadi kendala utama dalam upaya penegakan hukum. Sebagai contoh, aparat penegak hukum sering kali tidak memiliki akses ke alat forensik digital yang memadai untuk menyelidiki kejahatan berbasis AI, apalagi untuk menghadapi serangan siber berskala besar.

Lebih jauh, penegakan hukum terhadap kejahatan berbasis AI juga menghadapi tantangan lintas yurisdiksi. Sebagian besar kejahatan berbasis AI dilakukan di dunia maya, yang tidak mengenal batas geografis. Pelaku kejahatan dapat berada di satu negara, sementara korban berada di negara lain, dengan infrastruktur kejahatan yang tersebar di berbagai lokasi di dunia (Masithoh et al., 2023). Dalam kondisi seperti ini, kolaborasi internasional menjadi sangat penting, tetapi sering kali terhambat oleh perbedaan hukum, kebijakan, dan kepentingan politik antarnegara.

Untuk mengatasi tantangan ini, diperlukan pendekatan hukum yang adaptif dan progresif. Regulasi yang spesifik untuk AI harus segera dikembangkan, baik di tingkat nasional maupun internasional. Dalam konteks Indonesia, misalnya, diperlukan pembentukan undang-undang baru yang secara eksplisit mengatur penggunaan, pengembangan, dan tanggung jawab hukum terkait AI. Undang-undang ini harus mencakup mekanisme perlindungan terhadap kejahatan berbasis AI, termasuk kerangka kerja untuk menanggulangi kejahatan siber yang semakin canggih.

Selain itu, pendidikan dan pelatihan bagi penegak hukum juga harus ditingkatkan. Aparat penegak hukum perlu memahami teknologi AI dan dampaknya terhadap hukum, sehingga mereka dapat lebih efektif dalam menangani kasus kejahatan berbasis AI. Kolaborasi dengan para ahli teknologi, akademisi, dan sektor swasta juga sangat penting untuk menciptakan pendekatan yang komprehensif dalam menghadapi tantangan ini.

Penelitian ini bertujuan pertama untuk mengidentifikasi tantangan utama dalam penegakan hukum terhadap kejahatan berbasis kecerdasan buatan (AI), dengan fokus pada aspek regulasi, pertanggungjawaban hukum, dan kapasitas teknis penegak hukum. Dengan

memahami tantangan ini secara mendalam, penelitian ini berupaya memberikan kerangka analisis yang dapat membantu legislator, akademisi, dan praktisi hukum dalam merumuskan pendekatan yang lebih adaptif dan efektif terhadap perkembangan teknologi AI yang sangat dinamis. Tujuan kedua adalah untuk mengevaluasi efektivitas regulasi hukum yang ada di Indonesia dan tingkat internasional dalam menghadapi kejahatan berbasis AI, serta memberikan rekomendasi untuk pembentukan regulasi yang lebih progresif dan komprehensif. Melalui evaluasi ini, penelitian bertujuan memberikan kontribusi substansial dalam pengembangan hukum teknologi yang mampu merespons ancaman kejahatan berbasis AI dengan tetap mempertimbangkan nilai-nilai keadilan dan hak asasi manusia.

Implikasi penelitian ini terletak pada dua aspek utama. Pertama, dari segi teoretis, penelitian ini diharapkan dapat memperkaya literatur hukum teknologi, khususnya dalam konteks kejahatan berbasis AI, dengan memberikan kerangka konseptual baru tentang bagaimana hukum dapat berkembang mengikuti inovasi teknologi tanpa kehilangan sifat normatifnya. Kedua, secara praktis, penelitian ini memberikan panduan strategis bagi pembuat kebijakan dalam merumuskan regulasi yang tidak hanya responsif terhadap kejahatan berbasis AI, tetapi juga mendorong pengembangan AI yang aman dan etis. Implikasi lainnya adalah peningkatan kapasitas penegak hukum melalui rekomendasi tentang pelatihan teknologi dan kolaborasi lintas sektor, yang dapat memperkuat upaya pencegahan dan penanganan kejahatan berbasis AI di masa mendatang.

Berdasarkan uraian diatas, maka rumusan masalah penelitian ini : (1) Bagaimana tantangan hukum yang dihadapi dalam penegakan hukum terhadap kejahatan berbasis kecerdasan buatan (AI), khususnya terkait regulasi, pertanggungjawaban pidana, dan kapasitas teknis aparat penegak hukum? dan (2) Sejauh mana efektivitas regulasi hukum yang ada, baik di Indonesia maupun di tingkat internasional, dalam mengatasi kejahatan berbasis AI, dan apa langkah-langkah yang dapat diambil untuk membentuk kerangka hukum yang lebih adaptif dan progresif?

METODE PENELITIAN

Metode penelitian yang digunakan dalam kajian ini adalah metode normatif, yang bertujuan untuk menganalisis peraturan perundang-undangan, prinsip-prinsip hukum, dan doktrin yang relevan dengan penegakan hukum terhadap kejahatan berbasis kecerdasan buatan (AI) (Syarif et al., 2024). Penelitian ini menggunakan pendekatan perundang-undangan (statute approach) untuk mengkaji kerangka hukum yang ada, baik di tingkat nasional seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), maupun di tingkat internasional seperti Konvensi Budapest tentang Kejahatan Siber. Selain itu,

pendekatan konseptual (conceptual approach) juga diterapkan untuk memahami prinsip-prinsip hukum terkait tanggung jawab pidana, serta keterkaitan antara teknologi dan hukum dalam konteks AI.

Penelitian ini memanfaatkan sumber bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi undang-undang, perjanjian internasional, dan dokumen hukum lain yang mengatur atau terkait dengan kejahatan berbasis teknologi. Bahan hukum sekunder mencakup literatur, jurnal akademik, dan karya ilmiah lainnya yang membahas implikasi hukum dari perkembangan teknologi AI. Sementara itu, bahan hukum tersier digunakan untuk mendukung pemahaman terhadap istilah dan konsep hukum yang bersifat teknis. Penelitian ini juga melibatkan analisis terhadap kasus-kasus yang relevan untuk memahami penerapan hukum dalam menghadapi kejahatan berbasis AI, baik dalam konteks nasional maupun internasional.

Sebagai bagian dari analisis hukum, penelitian ini mengadopsi pendekatan komparatif untuk membandingkan pengaturan hukum di Indonesia dengan beberapa negara lain yang telah mengembangkan regulasi terkait teknologi AI. Pendekatan ini bertujuan untuk mengidentifikasi praktik terbaik (best practices) yang dapat diadopsi dalam sistem hukum Indonesia. Selain itu, metode ini juga melibatkan analisis evaluatif untuk menilai efektivitas regulasi hukum yang ada dan memberikan rekomendasi kebijakan yang lebih progresif dan adaptif. Dengan pendekatan ini, penelitian diharapkan mampu memberikan kontribusi teoretis maupun praktis yang signifikan dalam pengembangan hukum di era digital.

HASIL DAN PEMBAHASAN

1. Tantangan Hukum dalam Penegakan Hukum terhadap Kejahatan Berbasis Kecerdasan Buatan (AI)

Hukum dan teknologi adalah dua bidang yang memiliki hubungan dinamis dan saling memengaruhi. Teori hukum dan teknologi menjelaskan bagaimana hukum beradaptasi dengan perubahan yang dibawa oleh inovasi teknologi serta bagaimana teknologi dapat menciptakan tantangan baru yang harus diakomodasi oleh kerangka hukum (Hildebrandt, 2015). Lawrence Lessig, salah satu ahli terkemuka dalam hukum dan teknologi, mengemukakan bahwa hukum merupakan salah satu dari empat "kode" yang membentuk regulasi masyarakat modern, bersama dengan norma sosial, pasar, dan arsitektur teknologi. Menurut Lessig, interaksi antara hukum dan teknologi adalah simbiosis, di mana hukum berusaha mengendalikan dampak teknologi, sementara teknologi dapat membentuk ulang norma hukum melalui inovasi yang tidak terduga (Theis & Wong, 2017). Pandangan ini menyoroti pentingnya hukum sebagai alat untuk menjaga keseimbangan antara manfaat dan risiko yang muncul dari teknologi baru,

termasuk kecerdasan buatan (AI).

Pendekatan teoritis lain yang relevan adalah teori *Technological Determinism*, yang mengemukakan bahwa perkembangan teknologi memiliki pengaruh yang signifikan terhadap struktur sosial, ekonomi, dan hukum. Teori ini menyoroti bagaimana teknologi, termasuk kecerdasan buatan (AI), dapat mendorong perubahan dalam sistem hukum, baik dalam aspek normatif maupun prosedural. Dalam kerangka ini, hukum dipandang sebagai respons terhadap tantangan teknologi, yang memerlukan pembaruan regulasi agar tetap relevan (Hauer, 2017). Namun, teori ini juga menimbulkan pertanyaan penting tentang sejauh mana hukum dapat mengikuti kecepatan perkembangan teknologi, mengingat hukum cenderung bersifat reaktif dan membutuhkan proses legislasi yang panjang.

Dari perspektif *Sociological Jurisprudence*, Roscoe Pound menekankan bahwa hukum harus dilihat sebagai alat rekayasa sosial (*social engineering*) (Tamanaha, 2019). Dalam konteks ini, teknologi, termasuk AI, adalah bagian dari fenomena sosial yang memerlukan pendekatan hukum yang responsif dan pragmatis. Hukum tidak hanya berfungsi untuk mengatur, tetapi juga untuk mengarahkan perkembangan teknologi agar memberikan manfaat maksimal bagi masyarakat sambil meminimalkan risiko. Konsep ini relevan dalam konteks AI, di mana hukum diharapkan mampu menciptakan keseimbangan antara inovasi teknologi dan perlindungan terhadap hak-hak individu serta kepentingan publik.

Teori lain yang relevan adalah *Legal Realism*, yang menyoroti pentingnya mempertimbangkan realitas sosial, ekonomi, dan teknologi dalam proses penegakan hukum (Miles & Sunstein, 2008). Dalam konteks AI, teori ini menekankan bahwa hukum harus didasarkan pada kenyataan bahwa teknologi AI berkembang dengan cepat dan memiliki dampak yang luas terhadap masyarakat. Hukum tidak boleh bersifat kaku, tetapi harus fleksibel dan adaptif agar dapat mengakomodasi dinamika teknologi. Sebagai contoh, dalam kasus penggunaan AI untuk *deepfake* atau serangan siber, hukum perlu mempertimbangkan aspek teknis dan sosial dari teknologi tersebut untuk menciptakan regulasi yang efektif.

Selain itu, teori *Law and Economics* memberikan perspektif penting tentang bagaimana hukum dapat dirancang untuk mendorong efisiensi ekonomi dalam pengembangan dan penggunaan teknologi. Dalam konteks AI, teori ini menekankan pentingnya menciptakan regulasi yang tidak hanya melindungi masyarakat dari risiko kejahatan berbasis AI, tetapi juga mendorong inovasi yang dapat memberikan manfaat ekonomi. Misalnya, regulasi yang memberikan insentif bagi pengembangan AI yang bertanggung jawab dapat membantu menciptakan ekosistem teknologi yang aman dan berkelanjutan.

Dalam konteks hukum internasional, berbagai aturan telah dikembangkan untuk mengatur teknologi digital, termasuk aspek-aspek yang relevan dengan AI. Salah satu instrumen

penting adalah *Budapest Convention on Cybercrime* yang diadopsi pada tahun 2001. Konvensi ini merupakan kerangka hukum internasional pertama yang mengatur kejahatan siber, tetapi belum secara khusus mencakup aspek kejahatan berbasis AI. Selain itu, prinsip-prinsip yang diusulkan oleh organisasi internasional seperti UNESCO melalui rekomendasi tentang etika AI tahun 2021 menunjukkan upaya global untuk menciptakan standar universal dalam mengatur teknologi ini (Nguyen & Golman, 2021). Namun, masih terdapat kesenjangan yang signifikan dalam regulasi internasional terkait AI, khususnya mengenai penegakan hukum terhadap kejahatan yang melibatkan teknologi ini. Teori *Global Legal Pluralism* juga memiliki relevansi (Berman, 2020).

Teori ini mengakui bahwa dalam dunia yang semakin terhubung secara digital, hukum tidak hanya bersumber dari negara, tetapi juga dari aktor-aktor non-negara seperti organisasi internasional, perusahaan teknologi, dan komunitas digital. Dalam kerangka ini, regulasi teknologi, termasuk AI, harus melibatkan kolaborasi antara berbagai pemangku kepentingan di tingkat nasional dan internasional. Prinsip ini tercermin dalam berbagai upaya global untuk menciptakan standar etika dan regulasi AI, seperti rekomendasi UNESCO tentang etika AI dan kerangka kerja Uni Eropa tentang regulasi AI. Pendekatan ini menyoroti pentingnya hukum sebagai mekanisme yang mampu menjembatani perbedaan nilai, norma, dan kepentingan dalam pengaturan teknologi yang lintas batas.

Kecerdasan buatan adalah salah satu teknologi yang paling berpengaruh di era modern, tetapi sifatnya yang otonom, adaptif, dan kompleks menciptakan tantangan yang belum pernah terjadi sebelumnya dalam sistem hukum. Salah satu masalah mendasar adalah kecepatan perkembangan teknologi AI yang jauh melampaui kemampuan hukum untuk beradaptasi. Hukum, sebagai produk legislasi manusia, cenderung bersifat reaktif dan membutuhkan proses panjang untuk disahkan. Di sisi lain, teknologi AI berkembang dengan cepat, sering kali menciptakan inovasi baru yang tidak terduga dan di luar cakupan regulasi yang ada. Akibatnya, hukum sering kali tertinggal dalam mengatur perkembangan ini, menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan.

Tantangan berikutnya adalah sifat otonom AI yang menimbulkan perdebatan mengenai tanggung jawab hukum. Dalam teori hukum pidana tradisional, tanggung jawab pidana didasarkan pada unsur niat (*mens rea*) dan tindakan fisik (*actus reus*). Namun, dalam kasus AI, tanggung jawab menjadi lebih kompleks karena sistem AI sering kali bertindak secara independen berdasarkan algoritma yang dirancang oleh pengembang atau data yang diinput oleh pengguna. Misalnya, jika sebuah sistem AI digunakan untuk melakukan serangan siber, pertanyaan yang muncul adalah siapa yang harus bertanggung jawab: pengembang AI, pengguna, atau sistem itu sendiri? Dalam hal ini, konsep tanggung jawab hukum tradisional

menjadi sulit diterapkan, dan hukum belum memiliki mekanisme yang jelas untuk menangani situasi ini.

Di tingkat internasional, meskipun terdapat prinsip-prinsip umum yang dapat digunakan untuk mengatur kejahatan berbasis teknologi, seperti *Budapest Convention* atau kerangka kerja PBB terkait keamanan siber, tantangan lintas yurisdiksi tetap menjadi hambatan utama. Kejahatan berbasis AI sering kali dilakukan di dunia maya, yang tidak mengenal batas geografis. Pelaku kejahatan dapat berada di satu negara, sementara korban dan infrastruktur kejahatan tersebar di negara lain. Hal ini memerlukan kerja sama internasional yang lebih erat, tetapi sering kali terhambat oleh perbedaan hukum, kebijakan, dan kepentingan politik antarnegara. Sebagai contoh, dalam kasus serangan siber yang menggunakan algoritma AI, investigasi sering kali melibatkan banyak yurisdiksi, yang mempersulit proses penegakan hukum.

Selain itu, tantangan teknis dalam memahami teknologi AI juga menjadi kendala yang signifikan bagi penegak hukum. Teknologi AI sering kali melibatkan algoritma yang kompleks dan data dalam jumlah besar, yang memerlukan keahlian khusus untuk dianalisis. Banyak aparat penegak hukum, terutama di negara berkembang seperti Indonesia, tidak memiliki kapasitas teknis atau infrastruktur yang memadai untuk menyelidiki kejahatan berbasis AI. Sebagai contoh, dalam kasus *deepfake*, teknologi AI yang digunakan untuk memanipulasi video atau audio sehingga tampak autentik, penegak hukum memerlukan alat forensik digital yang canggih untuk mendeteksi manipulasi tersebut. Namun, alat dan keahlian ini sering kali tidak tersedia, sehingga menyulitkan proses investigasi dan penuntutan.

Di Indonesia, tantangan ini semakin diperburuk oleh keterbatasan kerangka hukum yang ada. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), meskipun telah diubah melalui Undang-Undang Nomor 19 Tahun 2016, masih belum sepenuhnya mencakup kompleksitas kejahatan berbasis AI. Sebagai contoh, UU ITE lebih fokus pada kejahatan siber tradisional seperti pencurian identitas dan akses ilegal, sementara kejahatan berbasis AI, seperti penyalahgunaan algoritma untuk manipulasi data atau penciptaan *deepfake*, belum secara eksplisit diatur. Hal ini menciptakan celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan (Respati, 2024).

Salah satu tantangan utama adalah ketidakjelasan aturan hukum dalam menentukan tanggung jawab atas tindakan kejahatan berbasis AI. Dalam banyak kasus, sistem AI bertindak secara otonom berdasarkan algoritma yang dirancang oleh pengembang atau data yang diberikan oleh pengguna. Jika sistem AI digunakan untuk melakukan kejahatan, seperti manipulasi pasar atau disinformasi politik, sulit untuk menentukan siapa yang harus bertanggung jawab secara hukum pengembang, pengguna, atau sistem itu sendiri. Hal ini menciptakan ketidakpastian hukum yang dapat dimanfaatkan oleh pelaku untuk menghindari

tanggung jawab pidana.

Selain itu, UU ITE dan regulasi lain yang relevan belum memberikan panduan teknis yang cukup bagi penegak hukum untuk menghadapi kejahatan berbasis AI. Sebagai contoh, teknologi *deepfake* yang menggunakan AI untuk menciptakan konten video atau audio yang sangat realistis memerlukan alat forensik digital dan pemahaman teknis yang mendalam untuk mendeteksi dan membuktikan manipulasi tersebut. Keterbatasan kapasitas teknis penegak hukum di Indonesia, terutama dalam memahami dan menyelidiki kejahatan berbasis teknologi tinggi, menjadi penghalang serius dalam penegakan hukum. Aparat penegak hukum sering kali tidak memiliki akses ke teknologi atau pelatihan yang memadai, yang membuat mereka rentan terhadap kejahatan berbasis AI yang semakin canggih.

Di sisi lain, kerangka hukum yang ada juga tidak mampu mengantisipasi dampak lintas sektor yang diakibatkan oleh kejahatan berbasis AI. Misalnya, penyalahgunaan AI dalam manipulasi data keuangan atau pencurian data pribadi dapat memiliki dampak luas terhadap ekonomi, privasi, dan kepercayaan publik. Namun, regulasi yang ada sering kali bersifat sektoral dan terfragmentasi, sehingga tidak memberikan pendekatan yang holistik dalam menghadapi kejahatan semacam ini. Ketiadaan kerangka hukum terpadu yang secara eksplisit mengatur teknologi AI membuat Indonesia rentan terhadap risiko yang lebih besar, baik di tingkat nasional maupun internasional.

Tantangan lain yang signifikan adalah ketidaksesuaian antara perkembangan teknologi AI dan proses legislasi yang lambat. Proses pembentukan undang-undang di Indonesia sering kali membutuhkan waktu bertahun-tahun, sementara teknologi AI berkembang dengan sangat cepat, menghasilkan inovasi baru dalam hitungan bulan. Akibatnya, regulasi yang ada cenderung tertinggal jauh dari realitas teknologi di lapangan, menciptakan celah hukum yang semakin lebar. Hal ini memberikan keuntungan strategis bagi pelaku kejahatan yang dapat mengeksploitasi ketiadaan regulasi yang relevan.

Lebih jauh lagi, isu lintas yurisdiksi dalam kejahatan berbasis AI menambah kompleksitas tantangan hukum di Indonesia. Sebagian besar kejahatan berbasis AI dilakukan di dunia maya, yang bersifat tanpa batas geografis. Pelaku kejahatan dapat berada di luar negeri, sementara korban atau dampak kejahatan dirasakan di Indonesia. Dalam kondisi seperti ini, penegakan hukum memerlukan kerja sama internasional yang erat, baik melalui perjanjian bilateral maupun mekanisme multilateral. Namun, perbedaan regulasi, sistem hukum, dan kepentingan politik antarnegara sering kali menghambat kolaborasi ini, sehingga memperumit upaya penegakan hukum di tingkat nasional.

Regulasi terkait AI juga menghadapi tantangan dalam memastikan keseimbangan antara pengawasan dan inovasi. Di satu sisi, regulasi yang terlalu ketat dapat menghambat

pengembangan teknologi AI, yang memiliki potensi besar untuk memberikan manfaat ekonomi dan sosial. Di sisi lain, regulasi yang terlalu longgar dapat membuka peluang bagi penyalahgunaan teknologi ini. Oleh karena itu, diperlukan pendekatan hukum yang seimbang, yang mampu melindungi masyarakat dari risiko kejahatan berbasis AI tanpa menghambat inovasi.

Salah satu contoh nyata dari tantangan ini adalah kasus serangan siber berbasis AI terhadap perusahaan teknologi besar di Amerika Serikat pada tahun 2020. Dalam kasus ini, pelaku menggunakan algoritma AI untuk menyusup ke sistem keamanan perusahaan, mencuri data sensitif jutaan pengguna, dan mengadaptasi serangan mereka terhadap upaya pencegahan yang dilakukan oleh perusahaan. Kasus ini menunjukkan bagaimana AI dapat digunakan untuk mengatasi sistem keamanan yang paling canggih sekalipun, menciptakan tantangan baru bagi hukum dalam mendeteksi dan mencegah kejahatan semacam itu.

Dalam kasus lain, penyalahgunaan AI untuk menciptakan *deepfake* telah menimbulkan kerusakan reputasi dan bahkan mempengaruhi stabilitas politik di beberapa negara. Di Asia, misalnya, teknologi *deepfake* digunakan dalam skandal politik untuk menyebarkan informasi palsu yang dirancang untuk merusak kredibilitas tokoh politik tertentu. Teknologi ini tidak hanya menciptakan tantangan hukum dalam hal pembuktian, tetapi juga menimbulkan dampak sosial yang luas, yang sering kali sulit untuk diperbaiki.

2. Evaluasi Efektivitas Regulasi Hukum terhadap Kejahatan Berbasis AI dan Rekomendasi Pembentukan Kerangka Hukum yang Adaptif

Perkembangan teknologi kecerdasan buatan (AI) membawa dampak besar dalam berbagai dimensi hukum, khususnya dalam mengidentifikasi batas kemampuan regulasi yang ada untuk menangani kejahatan berbasis AI. Salah satu aspek penting yang harus dievaluasi adalah kemampuan regulasi untuk tetap relevan dalam menghadapi inovasi teknologi yang bergerak dengan kecepatan tinggi. Di Indonesia, regulasi seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memiliki nilai strategis sebagai instrumen hukum utama dalam mengatur aktivitas di dunia maya. Namun, UU ITE menunjukkan keterbatasan dalam menghadapi sifat otonom dan adaptif AI, yang menghasilkan bentuk kejahatan baru, seperti manipulasi data berskala besar, pencurian identitas yang canggih, atau penciptaan konten palsu melalui *deepfake* (Rachmadie & Supanto, 2020).

Kejahatan berbasis AI memiliki karakteristik yang kompleks dan sering kali tidak terdeteksi dalam tahap awal. Hal ini menjadi tantangan tersendiri bagi regulasi yang bersifat reaktif. Misalnya, UU ITE lebih fokus pada kejahatan siber yang melibatkan tindakan langsung oleh manusia, seperti penipuan daring atau akses ilegal. Sebaliknya, AI dapat bertindak secara independen berdasarkan algoritma yang telah diprogram sebelumnya, menciptakan dilema

hukum tentang tanggung jawab. Dalam konteks ini, regulasi yang ada kurang memberikan kejelasan mengenai aktor yang dapat dimintai pertanggungjawaban, baik itu pengembang, pengguna, atau entitas yang memanfaatkan teknologi tersebut.

Dari perspektif internasional, upaya untuk menciptakan regulasi yang efektif terhadap kejahatan berbasis AI masih berada dalam tahap awal. Konvensi Budapest tentang Kejahatan Siber merupakan salah satu kerangka internasional yang sering dirujuk. Namun, konvensi ini belum mencakup secara spesifik kejahatan yang melibatkan AI. Sebagai contoh, serangan siber berbasis AI, di mana algoritma canggih digunakan untuk mengidentifikasi dan mengeksploitasi kelemahan dalam sistem keamanan, tidak memiliki pengaturan yang eksplisit dalam konvensi tersebut (Agung et al., 2022). Hal ini menciptakan kesenjangan yang signifikan, terutama mengingat skala ancaman yang ditimbulkan oleh teknologi AI dalam ranah digital global.

Efektivitas regulasi hukum juga bergantung pada kemampuan penegak hukum untuk memahami dan menerapkan aturan tersebut. Dalam konteks kejahatan berbasis AI, penegakan hukum membutuhkan pemahaman mendalam tentang algoritma, analisis data, dan teknologi pendukung lainnya. Di Indonesia, tantangan ini semakin diperburuk oleh keterbatasan infrastruktur, sumber daya manusia, dan pelatihan yang memadai bagi aparat penegak hukum. Hal ini menyebabkan proses investigasi kejahatan berbasis AI, seperti pencurian data yang menggunakan algoritma pembelajaran mesin, menjadi lambat dan sering kali tidak optimal. Keterbatasan ini memperlihatkan perlunya regulasi yang tidak hanya merancang norma hukum, tetapi juga memberikan panduan teknis dan dukungan operasional kepada penegak hukum.

Lebih jauh, evaluasi efektivitas regulasi hukum terhadap kejahatan berbasis AI juga harus mempertimbangkan faktor lintas yurisdiksi. Kejahatan AI sering kali bersifat transnasional, melibatkan pelaku yang berada di berbagai negara dan memanfaatkan perbedaan hukum di masing-masing yurisdiksi untuk menghindari penegakan hukum. Dalam situasi ini, kolaborasi internasional menjadi sangat penting. Namun, regulasi nasional yang ada sering kali tidak kompatibel dengan standar internasional, sehingga menyulitkan koordinasi antara negara dalam menangani kasus kejahatan AI (Mariyam & Setiyowati, 2021). Sebagai contoh, ketidaksesuaian prosedur hukum antara Indonesia dan negara lain dapat memperlambat proses ekstradisi atau pertukaran informasi terkait kejahatan lintas negara.

Untuk mengatasi tantangan tersebut, diperlukan pembentukan kerangka hukum yang adaptif, yang tidak hanya merespons kejahatan berbasis AI, tetapi juga memberikan ruang bagi perkembangan teknologi yang bertanggung jawab. Langkah pertama adalah memperbarui regulasi yang ada, seperti UU ITE, untuk secara eksplisit mencakup kejahatan berbasis AI. Pembaruan ini harus mencakup definisi yang jelas tentang kejahatan berbasis AI, mekanisme pertanggungjawaban yang adil, serta sanksi yang sesuai dengan tingkat ancaman yang

ditimbulkan.

Langkah kedua adalah memperkuat kapasitas penegak hukum melalui pendidikan dan pelatihan khusus dalam bidang teknologi AI. Aparat penegak hukum perlu dibekali dengan pengetahuan teknis tentang cara kerja AI, metode analisis data, dan alat forensik digital. Selain itu, perlu ada investasi dalam infrastruktur teknologi yang memungkinkan penegak hukum untuk mendeteksi, menganalisis, dan membuktikan kejahatan berbasis AI secara efektif. Dalam hal ini, kerja sama dengan sektor swasta dan akademisi dapat menjadi solusi strategis untuk mengatasi keterbatasan sumber daya pemerintah.

Langkah ketiga adalah menciptakan kerangka kerja internasional yang lebih komprehensif untuk menangani kejahatan berbasis AI. Kerangka ini harus mencakup pengaturan tentang ekstradisi, pertukaran informasi, dan kolaborasi dalam investigasi lintas negara. Selain itu, diperlukan standar internasional yang dapat menjadi panduan bagi negara-negara dalam merancang regulasi nasional terkait AI. Misalnya, standar ini dapat mencakup prinsip-prinsip tentang transparansi algoritma, perlindungan data, dan etika penggunaan AI.

Pembentukan kerangka hukum yang adaptif juga harus mempertimbangkan aspek etika dalam pengembangan dan penggunaan AI. Regulasi harus mampu menciptakan keseimbangan antara mendorong inovasi teknologi dan melindungi hak asasi manusia. Misalnya, regulasi dapat mendorong pengembangan AI yang transparan dan akuntabel melalui insentif kepada perusahaan teknologi yang mematuhi standar etika. Pada saat yang sama, regulasi juga harus melindungi masyarakat dari risiko penyalahgunaan AI, seperti pelanggaran privasi atau diskriminasi algoritmik.

Sebagai penutup, evaluasi terhadap efektivitas regulasi hukum yang ada menunjukkan bahwa tantangan kejahatan berbasis AI tidak dapat diatasi hanya dengan pendekatan hukum yang bersifat reaktif. Diperlukan kerangka hukum yang adaptif, progresif, dan holistik, yang tidak hanya merespons ancaman yang ada, tetapi juga memberikan dasar bagi pengembangan teknologi yang bertanggung jawab. Melalui pembaruan regulasi, peningkatan kapasitas penegak hukum, dan kolaborasi internasional, hukum dapat menjadi instrumen yang efektif untuk mengelola risiko yang ditimbulkan oleh kecerdasan buatan di era digital ini.

SIMPULAN

Tantangan hukum dalam penegakan terhadap kejahatan berbasis kecerdasan buatan (AI) terletak pada ketertinggalan regulasi dibandingkan kecepatan perkembangan teknologi, ketidakjelasan tanggung jawab pidana, keterbatasan kapasitas teknis penegak hukum, dan kompleksitas lintas yurisdiksi. Regulasi yang ada, seperti UU ITE di Indonesia dan Konvensi Budapest di tingkat internasional, belum mencakup kejahatan berbasis AI secara memadai.

Untuk mengatasi ini, diperlukan pembaruan regulasi yang mencakup definisi, mekanisme tanggung jawab, dan sanksi yang relevan, disertai peningkatan kapasitas teknis aparat penegak hukum melalui pelatihan dan teknologi pendukung. Di tingkat internasional, kerja sama lintas negara dan penyelarasan standar hukum global harus diperkuat untuk menghadapi sifat transnasional dari kejahatan berbasis AI. Dengan pembaruan ini, hukum dapat lebih adaptif, progresif, dan efektif dalam melindungi masyarakat dari ancaman yang ditimbulkan oleh kecerdasan buatan.

DAFTAR PUSTAKA

Abdussamad, Z., & Muhtar, M. H. (2022). Etika Penggunaan Media Sosial Dalam Promosi Destinasi Wisata di Desa Patoameme. *Akuntansi Dan Humaniora: Jurnal Pengabdian Masyarakat*, *1*(2), Article 2. https://doi.org/10.38142/ahjpm.v1i2.339

Agung, A., Hafrida, H., & Erwin, E. (2022). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS: Journal of Criminal Law*, *3*(2), Article 2. https://doi.org/10.22437/pampas.v3i2.23367

Al-Hadrawi, B. K., Al-hadrawi, K. K., Ezzerouali, S., Al-Hadraawy, S. K., Aldhalmi, H. K., & Muhtar, M. H. (2024). *Mind Intruders: Psychological, Legal, and Social Effects of Human Parasites in the Age of Technological Progress*. https://www.researchgate.net/profile/Baqer-Al-Hadrawi/publication/384358843_Mind_Intruders_Psychological_Legal_and_Social_Effects_of_Human_Parasites_in_the_Age_of_Technological_Progress/links/66f5995db753fa724d4c6274/Mind-Intruders-Psychological-Legal-and-Social-Effects-of-Human-Parasites-in-the-Age-of-Technological-Progress.pdf

Berman, P. S. (2020). *The Oxford Handbook of Global Legal Pluralism*. Oxford University Press.

Hakim, H. A., Edhita Praja, C. B., & Sung, M.-H. (2023). AI in Law: Urgency of the Implementation of Artificial Intelligence on Law Enforcement in Indonesia. *Jurnal Hukum Novelty (1412-6834)*, *14*(1). https://www.researchgate.net/profile/Hary-Abdul-Hakim/publication/370607456_AI_in_Law_Urgency_of_the_Implementation_of_Artificial_Intelligence_on_Law_Enforcement_in_Indonesia/links/6459cd28809a5350215a340e/AI-in-Law-Urgency-of-the-Implementation-of-Artificial-Intelligence-on-Law-Enforcement-in-Indonesia.pdf?origin=journalDetail&_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9

Hauer, T. (2017). Technological determinism and new media. *International Journal of English Literature and Social Sciences*, *2*(2), 239174.

Hildebrandt, M. (2015). *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*. Edward Elgar Publishing.

Mariyam, S., & Setiyowati, S. (2021). Legality of Artificial Intelligence (AI) Technology in Public

Service Transformation: Possibilities and Challenges. *Lex Publica*, *8*(2), Article 2. https://doi.org/10.58829/lp.8.2.2021.75-88

Masithoh, M. Q. D., Hakim, H. A., Praja, C. B. E., & Iswanto, B. T. (2023). AI in Law: How Artificial Intelligence Is Transforming the Legal Profession in Indonesia. *Justitia Jurnal Hukum*, *7*(2), Article 2. https://doi.org/10.30651/justitia.v7i2.17832

Miles, T. J., & Sunstein, C. R. (2008). The New Legal Realism. *University of Chicago Law Review*, *75*, 831.

Nguyen, Dr. C. L., & Golman, Dr. W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Puluhulawa, J., Muhtar, M. H., Towadi, M., & Swarianata, V. (2023). The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia. *Law, State and Telecommunications Review*, *15*(2), 132–145.

Rachmadie, D. T., & Supanto, '. (2020). REGULASI PENYIMPANGAN ARTIFICIAL INTELLIGENCE PADA TINDAK PIDANA MALWARE BERDASARKAN UNDANG-UDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016. *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *9*(2), Article 2. https://doi.org/10.20961/recidive.v9i2.47400

Rahman, I., Muhtar, M. H., Mongdong, N. M., Setiawan, R., Setiawan, B., & Siburian, H. K. (2024). Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions. *Innovative: Journal Of Social Science Research*, *4*(1), Article 1. https://doi.org/10.31004/innovative.v4i1.8240

Respati, A. A. (2024). Reformulasi UU ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation. *JURNAL USM LAW REVIEW*, *7*(3), Article 3. https://doi.org/10.26623/julr.v7i3.10578

Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., Syahril, M. A. F., Utami, R. D., Rustan, A., & Nasution, H. S. (2024). *METODE METODE PENELITIAN PENELITIAN HUKUM HUKUM*. GET Press Indonesia. https://www.researchgate.net/profile/Mohamad-Hidayat-Muhtar/publication/381460823_METODE_PENELITIAN_HUKUM/links/666e76f8de777205a32ff37b/METODE-PENELITIAN-HUKUM.pdf

Tamanaha, B. Z. (2019). *Sociological Jurisprudence Past and Present* (SSRN Scholarly Paper No. 3350467). Social Science Research Network. https://papers.ssrn.com/abstract=3350467

Theis, T. N., & Wong, H.-S. P. (2017). The End of Moore's Law: A New Beginning for Information Technology. *Computing in Science & Engineering*, *19*(2), 41–50. Computing in Science & Engineering. https://doi.org/10.1109/MCSE.2017.29