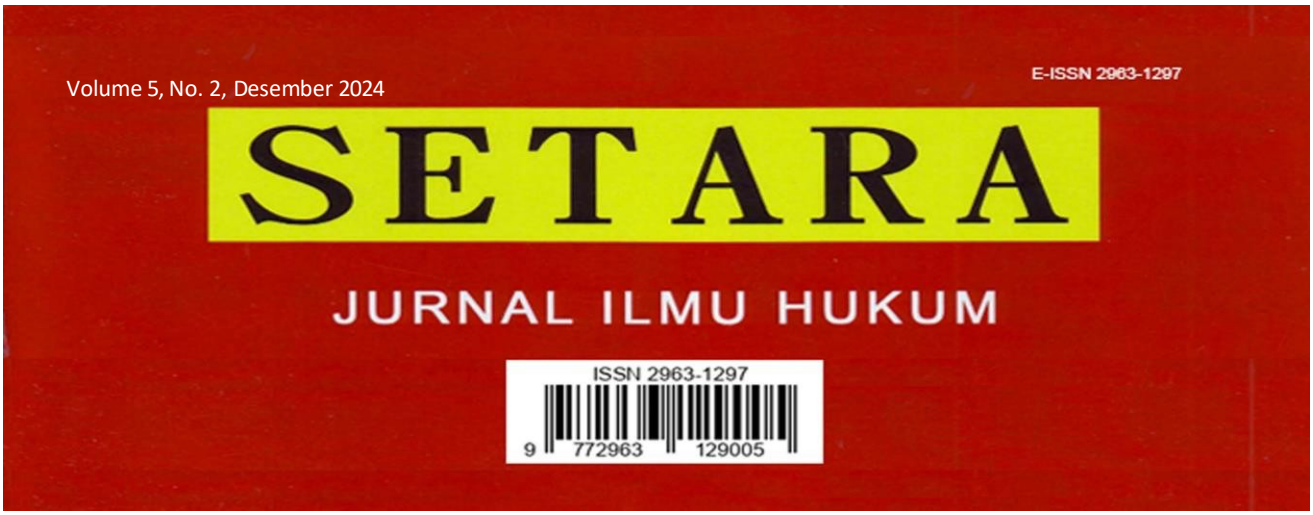

REFORMULASI KEBIJAKAN KRIMINAL DALAM PENANGGULANGAN KEJAHATAN BERBASIS TEKNOLOGI KECERDASAN BUATAN

Oleh :

Imam Subekti, Heru Sukrisno, Sugeng Wahyudi, Elly Kristiani Purwendah [1]
ellykpurwendah@gmail.com, *Universitas Wijayakusuma* [1]

ABSTRAK

Reformulasi kebijakan kriminal dalam penanggulangan kejahatan berbasis kecerdasan buatan (AI) menjadi isu yang mendesak seiring dengan 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. Hasilnya menunjukkan perlunya regulasi spesifik yang mengatur AI, pembentukan lembaga yang kompeten dalam teknologi, dan kerjasama internasional dalam penanggulangan kejahatan berbasis AI. Reformulasi kebijakan ini diharapkan dapat menciptakan sistem hukum yang lebih responsif terhadap ancaman digital.

Kata Kunci : *Kecerdasan Buatan, Kebijakan Kriminal, Penanggulangan Kejahatan, Regulasi, Teknologi.*

ABSTRACT

The reformulation of criminal policies to address AI-based crimes is an urgent issue given the rapid technological advancements. This study examines the legal challenges related to digital crimes, the strengthening of regulations, and the role of law enforcement agencies in addressing these issues. The research uses a literature study with a qualitative approach. The findings suggest the need for specific regulations on AI, the establishment of technology-competent institutions, and international collaboration in tackling AI-based crimes. This policy reform aims to create a legal system more responsive to digital threats.

Keywords ***:*** *Artificial Intelligence, Criminal Policy, Crime Prevention, Regulation, Technology.*

A. Pendahuluan

Perkembangan pesat teknologi kecerdasan buatan (Artificial Intelligence/AI) telah memberikan pengaruh besar dalam berbagai aspek kehidupan, termasuk di bidang kejahatan siber. AI tidak hanya dimanfaatkan untuk meningkatkan efisiensi dan efektivitas sistem, tetapi juga disalahgunakan oleh pelaku kejahatan untuk melakukan tindakan ilegal yang semakin canggih.

AI telah merevolusi berbagai sektor, mulai dari industri, kesehatan, pendidikan, hingga keamanan siber. Dalam konteks keamanan siber, AI dimanfaatkan untuk menganalisis pola data lalu lintas serta mengidentifikasi aktivitas mencurigakan yang berpotensi membahayakan keamanan informasi.. Kemampuan AI dalam memproses data dalam jumlah besar dan mendeteksi anomali yang tidak terlihat oleh manusia menjadikannya alat yang efektif dalam mencegah serangan siber.

Namun, seiring dengan manfaat yang ditawarkan, AI juga membuka peluang bagi munculnya jenis kejahatan baru. Pelaku kejahatan siber memanfaatkan AI untuk melakukan serangan yang lebih kompleks, seperti pembuatan deepfake, penipuan siber (cyber fraud), dan pelanggaran data. AI dapat digunakan untuk mengotomatisasi serangan, meningkatkan skala dan kecepatan serangan, serta mengaburkan jejak pelaku, sehingga menyulitkan upaya penegakan hukum.

Kebijakan kriminal yang ada saat ini sering kali belum mampu mengimbangi perkembangan teknologi dan modus operandi kejahatan yang semakin canggih. KUHP, misalnya, memiliki keterbatasan dalam menangani kejahatan yang memanfaatkan teknologi tinggi, seperti pemalsuan kartu kredit dan transfer dana elektronik, karena tidak adanya aturan khusus mengenai hal tersebut.

Selain itu, kurangnya kurangnya sumber daya manusia yang memiliki keahlian di bidang teknologi informasi dan komunikasi menjadi tantangan utama dalam upaya penegakan hukum terhadap kejahatan siber. Untuk itu, diperlukan reformulasi kebijakan kriminal yang adaptif terhadap perkembangan teknologi AI. Hal ini mencakup pembaruan regulasi yang spesifik mengatur kejahatan berbasis AI, peningkatan kapasitas penegak hukum dalam memahami dan menangani kejahatan siber,

selain itu, diperlukan kerja sama antara pemerintah, sektor swasta, dan masyarakat untuk membangun ekosistem digital yang aman..

Dengan demikian, reformulasi kebijakan kriminal menjadi langkah krusial dalam upaya penanggulangan kejahatan berbasis teknologi kecerdasan buatan, guna memastikan bahwa hukum tetap relevan dan efektif dalam menghadapi tantangan di era digital.

Tujuan dari artikel ini adalah untuk menganalisis kebutuhan reformulasi kebijakan kriminal dalam menghadapi kejahatan berbasis teknologi kecerdasan buatan (AI) yang semakin kompleks. Kejahatan berbasis AI, seperti deepfake, cyber fraud, dan pelanggaran data, membutuhkan regulasi yang spesifik agar dapat diatasi secara efektif. Selain itu, artikel ini bertujuan untuk memberikan rekomendasi kebijakan yang responsif dan adaptif terhadap perkembangan teknologi, termasuk pembaruan regulasi, peningkatan kompetensi penegak hukum, dan kolaborasi lintas sektor. Dengan reformulasi kebijakan ini, diharapkan sistem hukum mampu mengikuti perkembangan teknologi, sekaligus melindungi masyarakat dari risiko kejahatan berbasis AI.

B. Rumusan Masalah

Permasalahan utama dalam menangani kejahatan berbasis kecerdasan buatan (AI) terletak pada ketiadaan perangkat hukum yang secara spesifik mengatur tindak kejahatan semacam ini. Kekosongan hukum tersebut menciptakan hambatan serius dalam menegakkan aturan secara efektif terhadap jenis kejahatan baru yang terus berkembang. Di sisi lain, pelaksanaan penegakan hukum juga menghadapi tantangan besar akibat pesatnya kemajuan teknologi AI, yang sering kali melampaui kemampuan sistem hukum untuk mengatasi kompleksitas dan perubahan dinamisnya. Oleh karena itu, diperlukan strategi hukum yang lebih fleksibel dan responsif untuk menjawab tantangan tersebut..

C. Metode Penelitian

Artikel ini menggunakan metode penelitian yuridis normatif, yang menitikberatkan pada analisis terhadap norma-norma hukum yang ada dalam konteks kejahatan berbasis teknologi

kecerdasan buatan (AI). Penelitian ini mengandalkan studi literatur sebagai teknik pengumpulan data, yang Meliputi kajian terhadap berbagai aturan hukum yang berkaitan, literatur ilmiah yang membahas topik kejahatan berbasis teknologi, serta kasus-kasus hukum terkait. Selain itu, dilakukan juga studi komparatif untuk membandingkan kebijakan kriminal berbasis teknologi yang diterapkan di negara lain, guna melihat bagaimana kebijakan tersebut diadaptasi dan diterapkan. Metode analisis data yang diterapkan adalah deskriptif kualitatif, dengan tujuan untuk mengidentifikasi kelemahan dalam regulasi yang ada serta mengungkap potensi reformulasi kebijakan kriminal yang diperlukan untuk menangani kejahatan berbasis AI. Dengan pendekatan ini, diharapkan dapat ditemukan solusi yang efektif dan relevan untuk mengatasi permasalahan hukum di era digital.

D. Hasil dan Pembahasan

A. Tantangan Hukum dalam Menghadapi Kejahatan Berbasis AI

Keberadaan kecerdasan buatan (AI) dalam dunia digital membawa berbagai tantangan hukum yang signifikan, terutama terkait dengan kemunculan bentuk-bentuk kejahatan baru yang tidak dapat sepenuhnya dijangkau oleh hukum pidana konvensional. Kejahatan berbasis AI memiliki beberapa karakteristik yang membuatnya lebih sulit diidentifikasi dan diatasi dibandingkan dengan kejahatan konvensional. Karakteristik utama kejahatan berbasis AI yang dihadapi oleh sistem hukum adalah anonimitas, skalabilitas, dan kompleksitas teknologi yang terlibat.

Anonimitas adalah salah satu aspek utama dalam kejahatan berbasis AI. Penggunaan teknologi AI memungkinkan pelaku kejahatan untuk beroperasi tanpa mengungkapkan identitas mereka secara jelas. Kejahatan seperti penipuan online, manipulasi data, atau penyebaran deepfake sering kali dilakukan dengan memanfaatkan identitas palsu atau dengan menyembunyikan jejak digital mereka.

Sebagai contoh, Dalam artikel "AI-Based Evidence in Criminal Trials?" yang diterbitkan dalam William & Mary Law School Scholarship, dibahas bahwa perangkat pintar semakin

menjadi sumber data penting dalam kasus pidana. Data yang dihasilkan oleh perangkat ini, terutama melalui metode pembelajaran mesin yang kompleks, menimbulkan tantangan dalam hal pembuktian dan penuntutan karena kesulitan dalam mengakses dan memverifikasi bukti yang dihasilkan secara otonom oleh perangkat tersebut.

Skalabilitas merujuk pada kemampuan teknologi AI untuk memperbesar dampak dari kejahatan dengan lebih cepat dan luas. Sebagai contoh, serangan siber otomatis menggunakan bot AI dapat menyebabkan kerusakan yang besar dalam waktu singkat tanpa perlu campur tangan manusia Serangan siber yang didukung oleh kecerdasan buatan (AI) semakin canggih dan sulit dideteksi pada tahap awal. Menurut MindPoint Group, serangan yang didorong oleh AI dapat mengeksploitasi kerentanan dengan cepat, melewati langkah-langkah keamanan standar, dan menyebabkan kerusakan luas sebelum terdeteksi. AI dapat mengotomatisasi berbagai serangan, termasuk pembuatan dan penyebaran varian malware, pemindaian kerentanan sistem, dan pelaksanaan serangan distributed denial-of-service (DDoS), yang menimbulkan tantangan signifikan bagi pertahanan keamanan siber.

Kompleksitas teknologi adalah tantangan besar lainnya. Teknologi AI, seperti algoritma pembelajaran mesin dan pemrosesan bahasa alami, sangat rumit dan canggih, sehingga hanya sedikit penegak hukum yang memiliki pengetahuan teknis yang cukup untuk menangani kasus kejahatan berbasis AI secara efektif. Integrasi kecerdasan buatan (AI) dalam dunia siber telah membawa tantangan signifikan dalam penegakan hukum terhadap kejahatan berbasis teknologi. Menurut National Cyber Security Centre (NCSC) Inggris, AI dapat meningkatkan efektivitas operasi siber, baik dalam pertahanan maupun serangan, yang menimbulkan implikasi serius terhadap ancaman siber dalam dua tahun ke depan.

Selain karakteristik kejahatan berbasis AI itu sendiri, hukum pidana konvensional juga tidak memadai untuk menangani fenomena baru ini. Hukum pidana yang ada, seperti Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia, dirancang untuk mengatasi tindak pidana yang lebih tradisional dan tidak memperhitungkan perkembangan teknologi yang begitu pesat.

Hal ini terlihat dalam ketidakjelasan pengaturan terkait kejahatan berbasis AI, seperti manipulasi data menggunakan AI atau penyalahgunaan algoritma yang menyebabkan kerugian pada pihak lain.

Banyak negara yang belum memiliki regulasi hukum yang jelas untuk kejahatan berbasis AI, padahal ancaman yang ditimbulkan oleh kejahatan teknologi ini terus meningkat. Di Indonesia, meskipun telah ada beberapa regulasi terkait kejahatan siber, seperti Undang-Undang ITE, namun belum ada peraturan yang secara spesifik mengatur tentang penggunaan teknologi AI dalam melakukan kejahatan. Hal ini menciptakan celah hukum yang memungkinkan kejahatan berbasis AI tidak terdeteksi atau tidak mendapatkan penanganan yang sesuai.

Oleh karena itu, ada kebutuhan mendesak untuk memperbarui kebijakan hukum dan mengembangkan regulasi yang dapat mengakomodasi kejahatan berbasis AI. Sebuah pendekatan hukum yang lebih fleksibel dan adaptif terhadap teknologi baru perlu diperkenalkan untuk mengatasi tantangan yang dihadapi oleh sistem hukum dalam menangani kejahatan digital yang semakin kompleks ini.

B. Upaya Penanggulangan Melalui Reformulasi Kebijakan

Untuk menghadapi kejahatan berbasis teknologi kecerdasan buatan (AI), diperlukan reformulasi kebijakan kriminal yang menyeluruh dan adaptif. Kebijakan yang ada saat ini masih banyak yang belum mengakomodasi kompleksitas kejahatan berbasis AI, yang berkembang lebih cepat daripada kemampuan sistem hukum yang ada. Oleh karena itu, upaya untuk memperbarui dan memperkuat kebijakan hukum menjadi sangat penting, agar sistem hukum dapat berfungsi efektif dalam menghadapi tantangan kejahatan digital. Ada beberapa langkah kunci yang dapat diambil dalam reformulasi kebijakan ini, yaitu penguatan regulasi spesifik terkait AI, pembentukan lembaga penegakan hukum dengan kompetensi teknologi, dan penyelarasan antara perkembangan teknologi dan kebijakan hukum.

1. Penguatan Regulasi Spesifik Terkait AI dalam Hukum Pidana

Salah satu upaya pertama yang perlu dilakukan dalam reformulasi kebijakan adalah penguatan regulasi yang lebih spesifik terkait dengan kejahatan berbasis AI dalam hukum pidana. Mengingat kejahatan berbasis AI memiliki karakteristik yang berbeda dengan kejahatan konvensional, pengaturan yang ada saat ini sering kali tidak memadai untuk menangani bentuk kejahatan baru ini. Integrasi kecerdasan buatan (AI) dalam berbagai sektor telah menimbulkan tantangan signifikan dalam penegakan hukum, khususnya terkait kejahatan siber. Di Indonesia, regulasi mengenai AI masih terbatas. UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) mengidentifikasi AI sebagai "Agen Elektronik," yaitu perangkat dalam sistem digital yang dirancang untuk secara otomatis melaksanakan tindakan terhadap informasi elektronik dan dioperasikan oleh pihak terkait.

Berdasarkan penelitian tersebut, penting untuk menyusun regulasi yang dapat mengakomodasi kejahatan berbasis AI secara khusus. Regulasi ini dapat mencakup definisi yang jelas tentang jenis-jenis kejahatan yang melibatkan AI, serta sanksi yang sesuai untuk setiap jenis pelanggaran. Selain itu, peraturan yang dibuat harus memperhitungkan potensi penyalahgunaan teknologi AI, serta dampak jangka panjang yang ditimbulkan terhadap individu, masyarakat, dan negara.

2. Pembentukan Lembaga Penegakan Hukum dengan Kompetensi Teknologi

Selain penguatan regulasi, reformulasi kebijakan juga memerlukan pembentukan lembaga penegakan hukum yang memiliki kompetensi teknologi yang memadai. Kejahatan berbasis AI tidak hanya memerlukan pemahaman hukum yang kuat, tetapi juga pemahaman teknis tentang cara kerja teknologi tersebut. Sebagai contoh, serangan siber yang melibatkan AI sering kali menggunakan algoritma kompleks yang memerlukan keterampilan khusus untuk menganalisis dan melacak sumber serangan.

Lembaga penegakan hukum yang memiliki kompetensi teknologi dapat mencakup pembentukan unit khusus dalam kepolisian atau badan keamanan siber yang memiliki

spesialisasi dalam investigasi dan penuntutan kejahatan berbasis AI. Di banyak negara maju, seperti Amerika Serikat dan Uni Eropa, lembaga seperti FBI Cyber Division dan Europol telah mengembangkan unit-unit yang memiliki keahlian dalam menangani kejahatan berbasis teknologi. Ini adalah contoh yang dapat diterapkan di negara lain, termasuk Indonesia, untuk membangun kapasitas penegak hukum dalam menghadapi kejahatan digital.

3. Penyelarasan Antara Perkembangan Teknologi dan Kebijakan Hukum

Langkah ketiga yang perlu diambil adalah penyelarasan yang lebih baik antara perkembangan teknologi dan kebijakan hukum. Teknologi berkembang dengan sangat cepat, sering kali lebih cepat daripada kemampuan sistem hukum untuk mengaturnya.

Untuk mengatasi hal ini, penting bagi pemerintah dan pembuat kebijakan untuk melakukan riset dan konsultasi dengan ahli teknologi secara terus-menerus, agar kebijakan hukum tetap relevan dan efektif. Penyelarasan ini juga memerlukan kolaborasi internasional, karena banyak kejahatan berbasis AI bersifat lintas batas negara. Melalui forum internasional seperti United Nations Office on Drugs and Crime (UNODC), negara-negara dapat berbagi pengetahuan dan pengalaman dalam menangani kejahatan berbasis teknologi, serta merumuskan standar global yang dapat diadopsi oleh negara-negara di seluruh dunia. Kolaborasi semacam ini dapat memastikan bahwa kebijakan hukum tetap responsif terhadap ancaman yang ditimbulkan oleh kemajuan teknologi.

C. Studi Komparasi

1. Analisis Kebijakan Kriminal Terkait AI di Negara Maju

Di negara maju seperti Uni Eropa dan Amerika Serikat, kebijakan kriminal yang berhubungan dengan kecerdasan buatan (AI) telah berkembang pesat untuk mengatasi tantangan yang ditimbulkan oleh kejahatan berbasis teknologi. Negara-negara ini telah mulai merumuskan regulasi yang lebih spesifik terkait dengan penggunaan teknologi AI dalam

dunia kriminal. Misalnya, Uni Eropa melalui General Data Protection Regulation (GDPR) dan Artificial Intelligence Act (AIA) berusaha untuk mengatur penggunaan AI, termasuk dalam konteks perlindungan data pribadi dan pencegahan penyalahgunaan teknologi. Dalam konteks ini, AIA menetapkan bahwa penggunaan AI yang berisiko tinggi, seperti dalam sistem pengenalan wajah atau deepfake, harus diatur dengan ketat, dan penyalahgunaannya dapat dikenakan sanksi berat. Kebijakan ini bertujuan untuk melindungi masyarakat dari potensi penyalahgunaan AI dalam berbagai aspek kehidupan, terutama yang berkaitan dengan keamanan dan privasi.

Amerika Serikat juga telah mengembangkan kebijakan yang mengarah pada penanggulangan kejahatan berbasis AI, meskipun pendekatannya cenderung lebih terfragmentasi. Pemerintah AS, melalui badan-badan seperti Federal Trade Commission (FTC) dan Department of Justice (DOJ), mulai memperkenalkan regulasi yang berfokus pada pengawasan AI dalam konteks perlindungan data dan penanggulangan penipuan siber.

Dalam laporan "Recent Cases Highlight Growing Conflict Between AI and Data Privacy" yang diterbitkan oleh Haynes and Boone LLP, dibahas mengenai ketegangan yang berkembang antara kebutuhan AI akan data pribadi dalam jumlah besar untuk melatih algoritma pembelajaran mesin dan status data pribadi sebagai komoditas yang dilindungi di bawah undang-undang privasi AS seperti California Consumer Privacy Act (CCPA) dan Health Insurance Portability and Accountability Act (HIPAA).[1]

2. Pelajaran yang Dapat Diambil untuk Indonesia

Pelajaran yang dapat diambil dari kebijakan yang diterapkan di Uni Eropa dan Amerika Serikat sangat relevan untuk Indonesia, terutama dalam hal penguatan regulasi yang lebih spesifik dan penyusunan kebijakan yang dapat menangani kejahatan berbasis AI. Salah satu pelajaran utama adalah pentingnya memiliki regulasi yang jelas dan komprehensif

[1] Johnston Lee. (2020, April 20). Recent Cases Highlight Growing Conflict Between AI and Data Privacy. https://www.haynesboone.com/news/publications/recent-cases-highlight-growing-conflict-between-ai-and-data-privacy?

terkait dengan penggunaan AI dalam kehidupan sehari-hari, terutama yang menyangkut privasi, keamanan, dan keadilan. Dalam konteks ini, Indonesia bisa mengadaptasi beberapa prinsip dari AIA Uni Eropa, yang menetapkan kewajiban bagi perusahaan yang menggunakan teknologi AI untuk transparan mengenai algoritma yang mereka gunakan, serta bertanggung jawab atas potensi dampak sosial yang ditimbulkan.

Komisi Eropa telah mengusulkan Artificial Intelligence Act (AI Act), yang bertujuan untuk membentuk kerangka hukum komprehensif untuk kecerdasan buatan (AI) di Uni Eropa. Regulasi ini menekankan pentingnya transparansi dan akuntabilitas bagi perusahaan yang menggunakan teknologi AI. Secara khusus, undang-undang ini mengharuskan sistem AI, terutama yang dianggap berisiko tinggi, untuk memenuhi kewajiban transparansi yang ketat. Hal ini mencakup penyediaan informasi yang jelas tentang algoritma yang digunakan serta memastikan bahwa potensi dampak sosial dari teknologi tersebut dinilai dan diminimalkan.

AI Act juga mengkategorikan sistem AI berdasarkan tingkat risikonya dan menetapkan persyaratan yang sesuai untuk memastikan teknologi AI dikembangkan dan diterapkan secara bertanggung jawab, sehingga melindungi hak asasi manusia serta kepentingan sosial.

Selain itu, pengembangan lembaga penegakan hukum yang memiliki kompetensi dalam teknologi, seperti yang diterapkan di negara-negara maju, juga penting untuk diterapkan di Indonesia. Bahwa Indonesia meskipun telah memiliki regulasi terkait teknologi melalui Undang-Undang ITE, belum memiliki lembaga yang secara khusus menangani kejahatan berbasis AI. Oleh karena itu, pengembangan unit-unit khusus dalam kepolisian atau badan keamanan siber yang memiliki keahlian teknis dalam menangani kasus kejahatan berbasis AI sangat diperlukan. Misalnya, di Amerika Serikat, FBI Cyber Division telah dibentuk untuk menangani kejahatan digital dan siber, dengan fokus pada penyelidikan teknologi canggih seperti AI. Ini merupakan contoh yang dapat diadaptasi di Indonesia untuk

meningkatkan kemampuan penegakan hukum dalam menangani kejahatan berbasis teknologi.

Selain itu, kerja sama internasional yang semakin intensif dalam penanggulangan kejahatan berbasis AI juga dapat menjadi model untuk Indonesia. Negara-negara maju seperti Amerika Serikat dan Uni Eropa telah mengembangkan kolaborasi lintas negara untuk menangani kejahatan digital, terutama yang melibatkan teknologi yang melintasi batas negara. Indonesia, sebagai bagian dari komunitas internasional, perlu meningkatkan kerja sama dengan negara-negara lain untuk membangun regulasi bersama dan mengatasi kejahatan berbasis AI yang bersifat lintas negara. Menurut laporan Global Cybersecurity Index 2024 oleh International Telecommunication Union (ITU), penguatan kerjasama internasional menjadi salah satu indikator penting dalam meningkatkan kesiapan dan respons terhadap ancaman siber.

E. Penutup

1. Kesimpulan

Kehadiran teknologi kecerdasan buatan (AI) membawa tantangan hukum baru dalam menangani kejahatan berbasis teknologi yang semakin kompleks. Karakteristik utama kejahatan berbasis AI seperti anonimitas, skalabilitas, dan kompleksitas teknologi membuatnya sulit untuk diidentifikasi dan diatasi dengan hukum pidana konvensional. Selain itu, regulasi yang ada, seperti UU ITE di Indonesia, belum secara khusus mengatur kejahatan berbasis AI. Studi komparasi terhadap kebijakan di negara maju, seperti Uni Eropa dengan Artificial Intelligence Act dan Amerika Serikat dengan pendekatan institusional seperti FBI Cyber Division, menunjukkan pentingnya regulasi spesifik, pembentukan lembaga yang kompeten dalam teknologi, dan kolaborasi internasional untuk menangani ancaman lintas negara yang ditimbulkan oleh kejahatan berbasis AI.

2. Saran

Berdasarkan hasil analisis, ada beberapa rekomendasi yang perlu dipertimbangkan untuk menghadapi tantangan hukum yang ditimbulkan oleh kejahatan berbasis AI

1. Penguatan Regulasi Khusus AI

   Indonesia perlu menyusun regulasi yang spesifik dan adaptif terhadap perkembangan AI, mencakup pengaturan tentang jenis kejahatan berbasis AI, sanksi hukum, dan mekanisme perlindungan hak asasi manusia serta dampak sosial. Regulasi ini harus mencontoh praktik terbaik seperti Artificial Intelligence Act di Uni Eropa.

2. Pembentukan Lembaga Penegakan Hukum Teknologi

   Pemerintah perlu membentuk unit khusus dalam lembaga penegakan hukum, seperti unit siber dengan keahlian teknologi tingkat lanjut. Unit ini dapat mengadopsi model FBI Cyber Division atau Europol untuk menangani kejahatan berbasis AI secara efektif.

3. Peningkatan Kompetensi Penegak Hukum

   Program pelatihan dan sertifikasi teknologi untuk penegak hukum perlu diimplementasikan untuk memastikan mereka memiliki kemampuan dalam menangani kasus kejahatan berbasis AI.

4. Kerjasama Internasional

   Indonesia harus aktif dalam forum internasional seperti ITU dan UNODC untuk membangun kolaborasi lintas negara, berbagi informasi, dan mengembangkan standar global dalam penanganan kejahatan berbasis AI.

5. Peningkatan Kesadaran Publik

   Pemerintah perlu meningkatkan literasi masyarakat tentang ancaman kejahatan berbasis AI dan cara melindungi diri, termasuk melalui kampanye publik dan kerjasama dengan pihak swasta yang menggunakan teknologi AI.

Secara keseluruhan, reformulasi kebijakan kriminal untuk menghadapi kejahatan berbasis

AI memerlukan pendekatan yang holistik dan inklusif. Penyusunan regulasi yang komprehensif, kolaborasi lintas sektor, serta peningkatan kompetensi penegak hukum dalam hal teknologi akan membantu menciptakan sistem hukum yang lebih responsif dan siap menghadapi tantangan yang ditimbulkan oleh perkembangan teknologi kecerdasan buatan.

DAFTAR PUSTAKA

5th Edition . ITUPublications. Global Cybersecurity Index (2024). https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

Alkhazraji, M. A. (2024). Assessing the Effectiveness of Law Enforcement Strategies in Combating E-Crime Using AI (Master's thesis, Rochester Institute of Technology).

Bhatara, A. (2024, February 29). Sosialisasi Security Awareness Jakarta Barat: Pengaruh Artificial Intelligence (AI) dalam Keamanan Siber. https://arcs.sgu.ac.id/?s=Sosialisasi+Security+Awareness+Jakarta+Barat%3A+Pengaruh+Artificial+Intelligence+%28AI%29+dalam+Keamanan+Siber

Down, L., & Act, I. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

European Commission. (2022). Regulatory framework proposal on artificial intelligence. Digital Strategy European Commission.

Gless, S., Lederer, F., & Weigend, T. (2024). AI-Based Evidence in Criminal Trials?. Tulsa L. Rev., 59, 1.

Hartana, H. (2016). Hukum Perjanjian (Dalam Perspektif Perjanjian Karya Pengusahaan Pertambangan Batubara). *Jurnal Komunikasi Hukum (JKH)*, *2*(2).

Hartana, H. (2017). Hukum Pertambangan (Kepastian Hukum Terhadap Investasi Sektor Pertambangan Batubara di Daerah). *Jurnal Komunikasi Hukum (JKH)*, *3*(1), 50-81.

Hartana, H. (2017). Proses Membentuk Perusahaan Baru dalam Pelaksanaan Ekspansi Perusahaan Group di Sektor Pertambangan Batubara. *Perspektif*, *22*(2), 142-165.

Hartana, H. (2019). Ekspansi Perusahaan Group Ditinjau dari Undang-Undang No. 4 Th. 2009 Tentang Pertambangan Mineral dan Batubara. *Cakrawala Hukum: Majalah Ilmiah Fakultas Hukum Universitas Wijayakusuma*, *21*(2), 40-51.

Hartana, H. (2019). Initial public offering (ipo) of capital market and capital market companies in

Indonesia. *Ganesha Law Review*, *1*(1), 41-54.

Hartana, H. (2020). Existence And Development Group Companies In The Mining Sector (PT. Bumi Resources Tbk). *Ganesha Law Review*, *2*(1), 54-69.

Hartana, H. (2021). Eksistensi Dan Perkembangan Perusahaan Group Di Sektor Pertambangan. *Jurnal Pendidikan Kewarganegaraan Undiksha*, *9*(3), 669-681.

Hartana, H. (2021). Regulation of Group Company Expansion Restrictions in the Coal Mining Sector Viewed from Indonesian Laws and Regulations. *Jurnal Komunikasi Hukum (JKH)*, *7*(2), 520-526.

Hartana, H. (2022). Implikasi Ekspansi Perusahaan Group Pada Sektor Pertambangan Batubara Di Indonesia. *Jurnal Pendidikan Kewarganegaraan Undiksha*, *10*(1), 251-260.

Hartana, H. (2022). Pengaturan Pembatasan Ekspansi Perusahaan Group Di Sektor Pertambangan Batubara Ditinjau Dari Undang-Undang No. 40 Tahun 2007 Tentang Perseroan Terbatas. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 233-243.

Hartana, H., & Yasmiati, N. L. W. (2022). Pengembangan UMKM di Masa Pandemi melalui Optimalisasi Teknologi. *Jurnal Pengabdian Kepada Masyarakat Media Ganesha FHIS*, *3*(2), 50-64.

Hartana, H., Abdullah, D., Mulyati, S., Mangku, D. G. S., Yuliartini, N. P. R., & Sucandrawati, N. L. K. A. S. (2024, September). Online-based marketing information system for handicrafts from water hyacinth. In *AIP Conference Proceedings* (Vol. 3065, No. 1). AIP Publishing.

Johnston Lee. (2020, April 20). Recent Cases Highlight Growing Conflict Between AI and Data Privacy. https://www.haynesboone.com/news/publications/recent-cases-highlight-growing-conflict-between-ai-and-data-privacy?

Marwin, M. (2013). Penanggulangan Cyber Crime Melalui Penal Policy. ASAS: Jurnal Hukum Ekonomi Syariah, 5(1).

NCSC.GOV.UK. (2024, January 24). The near-term impact of AI on the cyber threat. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat?

Pamungkas, A. T., Muliyono, A., & Lahangatubun, N. (2024). Tracing Legal Regulations in Dealing with Cybercrime in Indonesia: Examining Obstacles and Solutions.

Poling Lindsay. AI Poses Significant Challenges to Cybersecurity. https://www.mindpointgroup.com/blog/ai-challenges-to-cybersecurity?

Rachmadie, D. T. (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), 128-156.

Rosgani, Oki. (2023, September 4). Tantangan dan Dampak Teknologi AI dalam Dunia Keamanan Siber. https://www.tintahijau.com/teknologi/tantangan-dan-dampak-teknologi-ai-dalam-dunia-keamanan-siber/

Setiawan, D. A. Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa. Masalah-Masalah Hukum, 53(1), 79-90.