

BAB III

URGENSI PENGATURAN TANGGUNG JAWAB PENGEMBANG INDIVIDU *ARTIFICIAL INTELEGENCE* (AI) DALAM UU ITE

3.1. Penyalahgunaan Teknologi AI Sebagai Bentuk Kejahatan Siber

3.1.1. Pengertian dan konsep teknologi AI dalam konteks kejahatan siber

Perkembangan zaman senantiasa diiringi dengan lahirnya berbagai inovasi teknologi yang membawa dampak signifikan bagi kehidupan manusia. Salah satu teknologi yang kini menjadi sorotan di berbagai sektor adalah kecerdasan buatan atau *Artificial Intelligence* (AI). Kehadiran AI bukanlah sesuatu yang muncul secara tiba-tiba, melainkan merupakan hasil dari proses penelitian panjang para ahli komputer yang sejak lama berupaya menciptakan sistem yang mampu berpikir dan bekerja menyerupai manusia. Saat ini, AI telah terintegrasi dalam berbagai aspek kehidupan sehari-hari, mulai dari aplikasi media sosial, peralatan rumah tangga, hingga sistem pertahanan dan keamanan negara..

Jika dilihat dari perspektif yang sederhana, AI sering dipahami sebagai teknologi yang mampu belajar dari data dan pengalaman untuk kemudian mengambil keputusan atau melaksanakan tugas tertentu tanpa perlu campur tangan manusia secara langsung. Namun, makna AI tidak berhenti sampai di situ. AI memiliki berbagai cabang dan metode, seperti

machine learning yang memungkinkan sistem belajar dari pola data, *deep learning* yang meniru mekanisme kerja *neuron* dalam otak manusia, hingga *natural language processing* (NLP) yang memungkinkan komputer memahami dan memproses bahasa manusia.³⁶ Keseluruhan teknologi tersebut menunjukkan bahwa AI dirancang untuk membantu pekerjaan manusia dengan cara yang lebih cepat, akurat, dan efisien.

Dalam ranah keamanan siber, AI memiliki dua sisi yang saling berlawanan. Di satu sisi, AI berperan penting dalam menjaga keamanan data, mengantisipasi potensi serangan siber, serta melindungi sistem dari upaya peretasan dengan mendeteksi berbagai aktivitas mencurigakan. Namun di sisi lain, AI juga rentan disalahgunakan oleh pihak-pihak tertentu untuk melakukan kejahatan siber dengan metode yang jauh lebih canggih dibandingkan teknik konvensional. Fenomena inilah yang melahirkan konsep penyalahgunaan AI dalam kejahatan siber, ketika teknologi yang sejatinya dirancang untuk membantu manusia justru dimanfaatkan untuk menimbulkan kerugian bagi manusia itu sendiri.

3.1.2. Bentuk-Bentuk Penyalahgunaan Teknologi AI Dalam Kejahatan Siber

Dalam membahas bentuk-bentuk penyalahgunaan AI, penting untuk memahami bahwa AI merupakan teknologi yang memiliki *fleksibilitas* tinggi. Dengan kemampuannya dalam mengolah data dan menghasilkan *output* berdasarkan *algoritma* tertentu, AI dapat dimanfaatkan untuk

³⁶ Miftakhur Rokhman Habibi-Isnatul Liviani, *Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia*, Jurnal Pemikiran dan Pembaharuan Hukum Islam, 2020

berbagai tujuan, termasuk perbuatan yang melanggar hukum. Salah satu contoh penyalahgunaan AI yang banyak disoroti adalah teknologi *deepfake*. *Deepfake* pada awalnya dikembangkan dari penelitian deep learning yang bertujuan meningkatkan kemampuan AI dalam menghasilkan gambar atau video yang tampak nyata.³⁷

Namun dalam praktiknya, teknologi ini kerap digunakan untuk tujuan yang merugikan, seperti pembuatan video pornografi non-konsensual. Masalah serius muncul ketika wajah seseorang ditempelkan pada tubuh orang lain dalam adegan pornografi tanpa sepengetahuan maupun persetujuan korban. Konten semacam ini tidak hanya menimbulkan rasa malu dan trauma psikologis, tetapi juga merusak reputasi korban di mata publik.

Selain teknologi *deepfake*, AI juga dimanfaatkan dalam praktik *phishing modern*. Jika sebelumnya *phishing* dilakukan dengan mengirimkan email massal yang umumnya memiliki bahasa kaku dan mudah dicurigai, saat ini pelaku kejahatan siber menggunakan AI untuk menganalisis gaya bahasa calon korban melalui media sosial. Dengan cara ini, pesan phishing yang dikirimkan menjadi lebih meyakinkan karena disesuaikan dengan gaya komunikasi dan kebiasaan korban, sehingga pesan tersebut tampak personal

³⁷ Nabila Aulia Agustin dan Refania Meilani Firdos, Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital, JAMASTIKA, 2024 h.5

dan wajar. Akibatnya, korban menjadi lebih mudah tertipu dan mengikuti instruksi yang terdapat dalam email tersebut.³⁸

AI juga kerap dimanfaatkan dalam pengembangan *malware* cerdas. Berbeda dengan *malware konvensional* yang biasanya memiliki pola perilaku tetap sehingga mudah dideteksi oleh sistem antivirus, *malware* berbasis AI mampu mempelajari pola pertahanan sistem target dan secara otomatis menyesuaikan metode serangannya agar tidak terdeteksi. Teknologi semacam ini memungkinkan pelaku kejahatan siber menembus sistem keamanan dengan lebih mudah dan sering kali tanpa meninggalkan banyak jejak.³⁹

Selain itu, penyalahgunaan AI juga terlihat dalam praktik penyebaran disinformasi. Di era digital saat ini, informasi dapat tersebar dengan sangat cepat. AI dimanfaatkan untuk memproduksi ribuan konten *hoaks* atau propaganda dengan narasi yang menarik dan mudah dipercaya oleh publik. Tidak hanya itu, distribusi konten tersebut juga dilakukan melalui akun bot yang dikendalikan AI, sehingga menimbulkan kesan bahwa informasi tersebut didukung oleh banyak orang. Dalam konteks politik, praktik seperti ini sangat berbahaya karena dapat memengaruhi opini publik secara masif dan memicu konflik horizontal di masyarakat.⁴⁰

³⁸ Russel Butarbutar, *Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya*, *Technology And Economics Law Journal*, 2023. H. 412-420

³⁹ *Ibid.* 10

⁴⁰ Ervina Chintia, et al., *Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya*, *Journal Information Engineering and Educational Technology*, 2018 h 79

AI juga dimanfaatkan dalam melancarkan serangan siber otomatis (*automated cyber attacks*) melalui *botnet* berbasis kecerdasan buatan. Jika pada *botnet* tradisional fungsinya hanya terbatas untuk menjalankan perintah tertentu dari pelaku, maka *robot network* yang dilengkapi AI mampu melakukan pemindaian kerentanan pada sistem target, menentukan metode serangan yang paling efektif, serta mengeksekusi serangan tersebut secara mandiri. Kemampuan ini membuat serangan menjadi jauh lebih efisien dan cepat dibandingkan apabila dilakukan oleh manusia secara manual.

3.1.3. Cara Kerja Dan Dampak Penyalahgunaan Teknologi AI

Jika ditinjau dari metode pelaksanaannya, penyalahgunaan AI dalam kejahatan siber memiliki berbagai modus *operandi*. Salah satu modus tersebut adalah *reconnaissance* dan *profiling*, yaitu teknik pengumpulan informasi mengenai target yang dilakukan oleh AI melalui berbagai sumber terbuka, seperti media sosial, blog, hingga data publik lainnya. Data-data ini kemudian dianalisis oleh AI untuk mengidentifikasi kelemahan atau informasi pribadi yang dapat dimanfaatkan pelaku untuk melakukan penipuan atau serangan siber secara lebih efektif.

Modus lainnya adalah penggunaan AI untuk melakukan serangan otomatis (*automated attacks*). Dalam skema ini, pelaku hanya perlu melatih AI dengan dataset dan algoritma tertentu, selanjutnya AI akan menjalankan serangan ke banyak target sekaligus tanpa campur tangan langsung pelaku. Contoh penerapan modus ini adalah serangan *Distributed Denial of Service*

(DDoS) yang bertujuan melumpuhkan server atau situs web dengan membanjirinya melalui permintaan akses dalam jumlah besar secara bersamaan.

Dalam kasus *deepfake*, modus operandi pelaku biasanya diawali dengan mengumpulkan foto atau video korban dari media sosial atau sumber daring lainnya. Data visual tersebut kemudian diproses menggunakan teknologi AI untuk menghasilkan konten *deepfake* sesuai dengan tujuan kejahatan, seperti pemerasan, pembuatan materi pornografi non-konsensual, atau pencemaran nama baik. Setelah konten *deepfake* selesai dibuat, pelaku akan mengirimkannya kepada korban sambil mengancam akan menyebarkan konten tersebut apabila permintaan pelaku, seperti pembayaran sejumlah uang atau tindakan tertentu, tidak dipenuhi oleh korban.

Sementara itu, dalam sektor keuangan, AI dimanfaatkan untuk melakukan penipuan finansial. Teknologi AI digunakan untuk menganalisis data transaksi perbankan dalam jumlah besar guna menemukan celah atau pola keamanan yang lemah pada sistem bank. Berdasarkan temuan tersebut, pelaku merancang skema penipuan yang sulit dideteksi oleh sistem pengamanan bank, sehingga meningkatkan potensi kerugian finansial yang signifikan. Penyalahgunaan AI dalam tindak pidana siber seperti ini menimbulkan dampak serius tidak hanya terhadap korban individu, tetapi juga terhadap kepercayaan publik dan stabilitas sektor digital secara keseluruhan..

Dari perspektif hukum, penyalahgunaan AI menimbulkan tantangan yang signifikan karena pelaku kerap memanfaatkan teknologi tersebut untuk mengaburkan jejak kejahatannya. AI memungkinkan pelaku memalsukan identitas maupun lokasi sehingga aparat penegak hukum kesulitan dalam proses pelacakan dan pembuktian di pengadilan. Sementara itu, dari aspek sosial dan psikologis, korban penyalahgunaan AI, khususnya pada kasus *deepfake* pornografi, sering mengalami tekanan mental yang sangat berat. Korban merasa martabat dan harga dirinya direndahkan, serta hidup dalam ketakutan akan *stigma* negatif apabila konten tersebut tersebar luas di masyarakat.

Dari sisi ekonomi, penyalahgunaan AI dalam tindak pidana siber dapat menyebabkan kerugian finansial yang besar. Misalnya, dalam kasus penipuan perbankan berbasis AI, korban dapat kehilangan dana dalam jumlah signifikan. Selain itu, penyalahgunaan AI juga menurunkan tingkat kepercayaan masyarakat terhadap teknologi digital secara umum, padahal digitalisasi merupakan salah satu pilar penting dalam pembangunan ekonomi nasional saat ini.

3.2. Tinjauan Terhadap Kelemahan UU ITE Dalam Mengatur Pengembang Invidu *Artificial Intelegence* (AI)

3.2.1. Ruang Lingkup UU ITE Saat Ini Terhadap Pelaku Kejahatan Siber

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan regulasi utama di Indonesia yang mengatur berbagai aktivitas

dalam ranah digital, termasuk kejahatan siber. Dalam penyusunannya, UU ITE lebih berfokus pada pengaturan tindakan melawan hukum yang dilakukan oleh subjek hukum yang secara langsung terlibat dalam tindak pidana tersebut. Subjek hukum yang dimaksud umumnya adalah pelaku utama, pengguna, atau pihak yang mendistribusikan konten digital ilegal.

Sebagai contoh, Pasal 27 ayat (1) UU ITE melarang distribusi dan transmisi konten yang melanggar kesusilaan, sedangkan Pasal 27 ayat (3) mengatur mengenai penghinaan atau pencemaran nama baik melalui media elektronik. Sementara itu, Pasal 28 ayat (1) dan (2) menegaskan larangan penyebaran berita bohong atau menyesatkan yang dapat merugikan konsumen maupun masyarakat luas. Ketentuan-ketentuan tersebut menunjukkan bahwa UU ITE pada dasarnya menitik beratkan pertanggungjawaban pidana kepada pihak yang secara aktif membuat, mengunggah, atau menyebarkan konten ilegal di ruang digital.⁴¹

Namun, jika dianalisis secara mendalam, Undang-Undang ITE belum memiliki ketentuan yang secara khusus mengatur pengembang teknologi sebagai subjek hukum yang dapat dimintai pertanggungjawaban atas pembuatan sarana atau sistem yang berpotensi disalahgunakan untuk melakukan tindak pidana digital. Padahal, seiring dengan perkembangan teknologi, khususnya *artificial intelligence* (AI), pengembang menempati

⁴¹ Muhammad Anthony Aldriano dan Agus Priyambodo, “*Cyber Crime Dalam Sudut Pandang Hukum Pidana*”, Jurnal Kewarganegaraan, 2022 h 56

posisi yang sangat strategis sebagai pihak yang merancang algoritma dan membangun infrastruktur teknologi digital.

Di sisi lain, dalam praktik penegakan hukum di Indonesia, sanksi pidana umumnya hanya dijatuhkan kepada pengguna akhir atau pihak yang menyebarkan konten ilegal, tanpa menyentuh pihak yang berada di balik penciptaan teknologi tersebut. Padahal, menurut doktrin hukum pidana modern, pertanggungjawaban pidana tidak semata-mata dibebankan kepada pelaku utama, melainkan juga dapat diarahkan kepada pihak-pihak yang membantu, memfasilitasi, atau menyediakan sarana bagi terjadinya tindak pidana, termasuk melalui penciptaan teknologi yang mendukung kejahatan.⁴²

Dengan demikian, cakupan pengaturan dalam UU ITE saat ini masih tergolong sempit karena belum mencakup seluruh pihak yang memiliki peran dalam rantai tindak pidana siber. Tidak adanya ketentuan yang menetapkan pengembang AI sebagai subjek hukum menimbulkan kelemahan dalam upaya perlindungan hukum bagi korban kejahatan digital, sehingga perlindungan yang diberikan belum dapat dianggap optimal.

3.2.2. Kekosongan Pengaturan Tentang Peran Dan Tanggung Jawab Pengembang Individu AI

Ketiadaan norma hukum (*rechtsvacuum*) dalam UU ITE terkait tanggung jawab pengembang individu AI terlihat jelas ketika dikaitkan dengan prinsip dasar hukum pidana mengenai pihak yang memberikan

⁴² *Ibid.*5

kemudahan atau sarana terjadinya tindak pidana. Dalam Kitab Undang-Undang Hukum Pidana (KUHP), Pasal 56 menegaskan bahwa setiap orang yang memberikan kesempatan, sarana, atau keterangan untuk terjadinya kejahatan dapat dipidana sebagai pembantu tindak pidana. Namun, prinsip ini belum diadopsi secara eksplisit dalam UU ITE untuk menjerat pengembang individu AI yang menciptakan atau menyediakan teknologi berisiko tinggi.⁴³

Padahal, pada praktiknya, pengembang individu AI memiliki kontrol penuh terhadap teknologi yang mereka rancang, mulai dari proses desain algoritma, penulisan kode, pelatihan data, hingga distribusi model melalui *platform* daring. Tanpa adanya kewajiban hukum yang mengatur tanggung jawab preventif, pengembang berpotensi menciptakan teknologi tanpa mempertimbangkan risiko penyalahgunaan oleh pihak lain. Kondisi ini berbeda dengan perusahaan atau lembaga penelitian yang umumnya memiliki protokol pengawasan dan tim hukum untuk memastikan teknologi yang dikembangkan telah memenuhi standar kehati-hatian (*due diligence*) sebelum dirilis ke publik.

Absennya norma yang secara khusus mengatur tanggung jawab pengembang individu dalam UU ITE menimbulkan berbagai implikasi serius. Pertama, kondisi ini membuka peluang bagi pengembang individu untuk menghindari pertanggungjawaban hukum dengan dalih bahwa

⁴³ M. Wildan Mufti et al., *Urgensi Pembentukan Peraturan Perundang-Undangan Teknologi Berbasis Artificial Intelligence*, Jurnal Penelitian Ilmu-Ilmu Sosial, 2024 h 36

penyalahgunaan teknologi berada di luar kendali mereka. Kedua, aparat penegak hukum menghadapi hambatan dalam menjerat pengembang meskipun teknologi yang mereka ciptakan memiliki fitur-fitur yang secara nyata memfasilitasi tindak pidana. Ketiga, kekosongan norma ini juga melahirkan ketidakpastian hukum (*legal uncertainty*) bagi korban kejahatan siber berbasis AI, terutama dalam hal menuntut pertanggungjawaban dan pemulihan hak mereka.

Lebih jauh, ketiadaan pengaturan ini tidak selaras dengan prinsip keadilan dalam hukum pidana. Dalam konteks kejahatan siber, pelaku langsung hanya merupakan aktor hilir dari suatu rangkaian kejahatan yang kompleks. Apabila pengembang individu selaku aktor hulu tidak memiliki pertanggungjawaban hukum yang jelas, maka tujuan hukum pidana untuk menciptakan efek jera, keadilan restoratif, serta fungsi preventif tidak akan tercapai secara optimal.

3.3. Urgensi Pengaturan Tanggung Jawab Pengembang *Artificial Intelligence* (AI) Dalam UU ITE

3.3.1. Pentingnya akuntabilitas pengembang individu dalam pencegahan kejahatan siber

Urgensi pengaturan tanggung jawab pengembang individu AI memiliki hubungan yang sangat erat dengan strategi pencegahan kejahatan siber di era digital saat ini. Pengembang individu pada dasarnya memiliki kebebasan dan kendali penuh dalam proses perancangan, pembuatan, serta publikasi teknologi AI yang mereka kembangkan. Mereka dapat dengan

mudah mengunggah kode program ke platform terbuka seperti *GitHub*, membuat model *deepfake* menggunakan perangkat pribadi, lalu mendistribusikannya ke forum daring tanpa melalui proses evaluasi risiko ataupun kebijakan kontrol.

Tanpa adanya norma hukum yang secara tegas mengatur kewajiban mereka, pengembang individu berpotensi mengabaikan prinsip kehati-hatian (*due diligence principle*) dalam merancang teknologi. Fokus pengembang umumnya hanya terpusat pada pencapaian teknis, inovasi, dan pengakuan intelektual, tanpa mempertimbangkan dampak etis maupun konsekuensi sosial yang mungkin timbul dari teknologi tersebut. Kondisi seperti ini menciptakan *moral hazard*, yakni suatu keadaan di mana pengembang tidak menanggung risiko maupun beban pertanggungjawaban atas akibat negatif dari ciptaannya.

Pengaturan mengenai akuntabilitas pengembang individu juga memiliki peran krusial dalam memastikan penerapan prinsip *ethics by design* dan *security by default*. Kedua prinsip ini menuntut agar sejak tahap perancangan, pengembang mempertimbangkan secara serius potensi risiko penyalahgunaan teknologi yang diciptakannya, serta memastikan adanya fitur keamanan dan pembatasan penggunaan yang efektif guna mencegah pemanfaatan teknologi untuk tujuan kejahatan. Contoh implementasi prinsip ini dapat berupa penambahan watermark permanen pada konten yang dihasilkan AI, penerapan sistem otentikasi bagi pengguna, atau

penetapan kebijakan lisensi yang secara tegas melarang penggunaan teknologi tersebut untuk aktivitas ilegal.⁴⁴

Tanpa adanya ketentuan hukum yang mengatur kewajiban tersebut, maka beban pertanggungjawaban pidana akan sepenuhnya ditimpakan kepada pelaku langsung dan pengguna akhir. Sementara itu, pengembang individu yang pada hakikatnya menyediakan sarana untuk terjadinya tindak pidana akan luput dari pertanggungjawaban hukum. Situasi semacam ini bertentangan dengan prinsip keadilan dalam hukum pidana (*equality before the law*), yang mengharuskan setiap pihak yang turut berkontribusi dalam terjadinya suatu tindak pidana dimintai pertanggungjawaban sesuai dengan tingkat kesalahan dan peranannya dalam kejahatan tersebut.

3.3.2. Perkembangan Hukum Di Negara Lain Terkait Pengembang Individu *Artificial Intelligence* (AI)

Perkembangan regulasi di tingkat internasional menunjukkan tren bahwa semakin banyak negara mulai memahami pentingnya menetapkan pengembang individu AI sebagai subjek hukum yang memiliki tanggung jawab atas ciptaan teknologinya. Kesadaran ini muncul seiring dengan meningkatnya kasus di mana pengembang individu, hanya dengan berbekal komputer pribadi dan keahlian teknis yang diperoleh dari forum daring atau komunitas *open-source*, mampu menciptakan model AI yang berpotensi

⁴⁴ Lailatul Badriah, Dwiyanto Indiahono, dan Sukarso, “Akuntabilitas dalam Kebijakan Perlindungan Data Pribadi di Indonesia”, Jurnal Inovasi Kebijakan, 2024. h 124-131

membahayakan, seperti teknologi *deepfake* untuk pornografi *non-konsensual* atau chatbot penipuan berbasis NLP.⁴⁵

Fenomena ini mendorong para pembuat kebijakan di berbagai yurisdiksi global untuk memperluas cakupan tanggung jawab hukum yang sebelumnya hanya menitikberatkan pada korporasi atau entitas kelembagaan besar. Saat ini, cakupan tersebut diperluas agar juga mencakup individu pengembang sebagai aktor sentral dalam ekosistem AI kontemporer, mengingat besarnya potensi risiko sosial dan keamanan yang dapat ditimbulkan oleh teknologi ciptaan mereka.

Di Uni Eropa, *Artificial Intelligence Act* yang diajukan oleh *European Commission* pada tahun 2021 memberikan kerangka hukum yang komprehensif terkait pengembang AI, termasuk individu. Dalam regulasi ini, istilah provider tidak hanya merujuk pada badan usaha atau lembaga riset, tetapi juga kepada orang perseorangan yang mengembangkan dan mendistribusikan sistem AI.⁴⁶ Regulasi tersebut menekankan bahwa setiap pengembang individu memiliki kewajiban untuk:

- a. Melakukan penilaian risiko (*risk assessment*) sebelum teknologi dipublikasikan, untuk mengidentifikasi potensi penyalahgunaan dan dampak negatif bagi hak asasi manusia, keamanan data, dan keamanan publik.

⁴⁵ Linda Ikawati, Sulaiman Sulaiman, dan Muhammad Fahri Husein, *Masa Depan Penegakan Hukum Indonesia: Sistem Peradilan Pidana Berbasis Kecerdasan Buatan (AI)*, Prosiding Seminar Nasional Ilmu Hukum, 2024.h 245-256

⁴⁶ *Ibid.*10

- b. Menyediakan dokumentasi teknis (*technical documentation*) yang menjelaskan cara kerja algoritma, batasan penggunaan, dan potensi risiko yang terkandung dalam teknologi.
- c. Memastikan adanya fitur keamanan minimum (*minimum safety requirements*) dalam sistem AI, seperti pembatasan akses, verifikasi penggunaan, serta *fail-safe mechanism* untuk mencegah penggunaan di luar tujuan yang diizinkan.

Apabila kewajiban tersebut dilanggar, baik oleh pengembang korporasi maupun individu, maka sanksi administratif yang berat dapat dijatuhkan, mulai dari denda dalam jumlah signifikan, pembatasan distribusi produk, hingga penarikan teknologi AI dari pasar Uni Eropa. Ketentuan ini menegaskan bahwa status individu tidak lagi dapat dijadikan alasan untuk menghindari tanggung jawab hukum ketika teknologi yang dikembangkannya menimbulkan kerugian atau risiko bagi masyarakat.

Perkembangan regulasi ini mencerminkan adanya pergeseran paradigma dalam hukum internasional, di mana pengembang individu tidak lagi dipandang sekadar sebagai aktor pasif yang hanya bertanggung jawab atas tindakan pribadinya. Sebaliknya, pengembang individu kini diakui sebagai subjek hukum yang memiliki pengaruh besar terhadap kehidupan sosial melalui teknologi yang mereka ciptakan dan sebar. Oleh karena itu, sudah saatnya Indonesia menyesuaikan kerangka hukumnya dengan tren global ini, baik melalui revisi UU ITE maupun pembentukan Undang-Undang khusus AI di masa depan. Langkah ini penting untuk memastikan

bahwa perlindungan hukum di Indonesia mencakup seluruh rantai pelaku dalam ekosistem kejahatan siber berbasis AI, mulai dari pengembang individu sebagai aktor hulu hingga pengguna dan penyebar konten ilegal sebagai aktor hilir.

3.4. Alternatif Dan Bentuk Pengaturan Yang Dapat Dimasukkan Dalam UU ITE

3.4.1. Model Pengaturan Preventif Dan Represif Terhadap Pengembang Individu AI

Dalam konteks hukum pidana, pengaturan tanggung jawab pengembang individu AI dapat dirumuskan melalui dua pendekatan utama, yaitu pendekatan *preventif* dan *represif*. Pendekatan *preventif* berfokus pada upaya pencegahan terjadinya tindak pidana dengan mewajibkan pengembang untuk menerapkan prinsip kehati-hatian (*due diligence*) dalam setiap tahap pengembangan teknologi AI.⁴⁷ Sementara itu, pendekatan *represif* menitikberatkan pada pemberian sanksi pidana atau administratif apabila pengembang terbukti dengan sengaja atau karena kelalaiannya telah memungkinkan teknologi yang diciptakannya digunakan untuk kejahatan siber.

Pendekatan *preventif* sendiri dapat diterapkan melalui pengaturan sejumlah kewajiban hukum bagi pengembang individu AI, antara lain:

- a. Melakukan Penilaian Risiko (*Risk Assessment*).

⁴⁷ Akmal Muhammad Abdullah, *Pelindungan Hak Privasi Terhadap Pengumpulan Data Pribadi oleh AI Generatif Berdasarkan Percakapan Dengan Pengguna*, *Padjajaran Law Review*, 2024 h 54

Pengembang diwajibkan melakukan penilaian risiko secara komprehensif sebelum mempublikasikan teknologi AI kepada masyarakat. Penilaian ini bertujuan untuk mengidentifikasi berbagai potensi penyalahgunaan maupun kerugian yang mungkin timbul akibat penggunaan teknologi tersebut.

b. Menerapkan Prinsip *Ethics by Design dan Security by Default*.

Pengembang perlu memastikan sejak tahap desain bahwa teknologi AI yang dikembangkan memiliki fitur pembatasan penggunaan ilegal. Contohnya adalah penambahan *watermark* permanen pada teknologi *deepfake* atau fitur deteksi penyalahgunaan yang dapat mengurangi risiko pemanfaatan AI untuk kejahatan.

c. Menyediakan Dokumentasi Teknis yang Lengkap.

Dokumentasi teknis wajib disusun secara jelas dan transparan, mencakup tentang cara kerja algoritma, tujuan pengembangan, batasan penggunaan, serta larangan pemanfaatan teknologi untuk tindak pidana tertentu.

d. Memublikasikan Perjanjian Lisensi Penggunaan (*License Agreement*).

Pengembang perlu mencantumkan perjanjian lisensi yang secara tegas melarang penggunaan teknologi AI untuk tujuan melawan hukum. Selain itu, lisensi juga harus menetapkan tanggung jawab pengguna akhir atas penyalahgunaan teknologi tersebut.

Kewajiban *preventif* tersebut akan mendorong pengembang individu AI untuk senantiasa mempertimbangkan aspek etika dan hukum sebelum mempublikasikan teknologi yang mereka kembangkan. Selain itu, pengaturan ini juga berperan penting dalam meminimalisasi risiko *moral*

hazard, yakni kondisi ketika pengembang merasa bebas dari tanggung jawab akibat ketiadaan ketentuan hukum yang tegas.⁴⁸

Kedua, model pengaturan represif terhadap pengembang individu AI perlu diterapkan guna menciptakan efek jera (*deterrent effect*) serta memastikan kepatuhan terhadap norma hukum yang berlaku. Bentuk sanksi yang dapat dijatuhkan dalam pendekatan *represif* ini meliputi:

1. Sanksi pidana apabila pengembang individu AI dengan sengaja menciptakan teknologi yang memang ditujukan untuk melakukan tindak pidana, atau apabila ia dengan sengaja tidak memasang sistem pengamanan minimum meskipun menyadari potensi risiko teknologi tersebut.
2. Sanksi pidana karena kelalaian (*culpa*) diterapkan apabila pengembang individu AI terbukti lalai dalam menerapkan prinsip kehati-hatian (*due diligence*), sehingga teknologi ciptaannya disalahgunakan untuk melakukan kejahatan yang menimbulkan kerugian bagi orang lain.
3. Sanksi administratif, seperti pencabutan hak distribusi teknologi, larangan publikasi di platform tertentu, hingga denda administratif, dapat dijatuhkan apabila pelanggaran dilakukan tanpa unsur kesengajaan tetapi memiliki risiko tinggi terhadap kepentingan publik.

Pendekatan *preventif* dan *represif* ini sejalan dengan tujuan hukum pidana, yaitu untuk melindungi masyarakat dari kejahatan serta menciptakan

⁴⁸ Maharani Qaulan Syadida, Nadhila Citra Supriantoro, dan Moh. Suci Sugianto, *Konseptualisasi Badan Pengawasan dan Perlindungan Artificial Intelligence Sebagai Pemenuhan Perlindungan Hukum Teknologi di Indonesia*, Jurnal Pemuliaan Hukum, 2023 h 57.

ketertiban sosial melalui upaya pencegahan (*preventie*) dan penindakan (*repressie*) yang adil dan proporsional.⁴⁹

3.4.2. Rekomendasi Norma Yang Dapat Dimasukkan Dalam Pasal Pada Revisi UU ITE atau Undang-Undang Khusus AI

Berdasarkan hasil analisis terhadap kelemahan pengaturan dalam UU ITE, terlihat adanya kebutuhan mendesak untuk menetapkan norma baru yang secara tegas mengatur tanggung jawab hukum pengembang individu AI.⁵⁰ Norma tersebut berperan penting untuk mewajibkan para pengembang AI mengambil langkah-langkah *preventif* dalam mencegah potensi penyalahgunaan teknologi ciptaan mereka oleh pihak lain.

Norma ini mencakup:

- a. Kewajiban melakukan penilaian risiko penyalahgunaan sejak tahap perancangan,
- b. Kewajiban menyediakan informasi teknis terkait cara kerja dan tujuan AI,
- c. Kewajiban menyiapkan fitur keamanan yang memadai, serta
- d. Kewajiban mencantumkan larangan penggunaan teknologi AI untuk tindakan melanggar hukum.

Selain memuat kewajiban, norma ini juga perlu mengatur larangan bagi pengembang yang dengan sengaja menciptakan dan menyebarluaskan AI untuk tujuan tindak pidana. Selain itu, pengaturan mengenai kelalaian juga

⁴⁹ *Ibid.*5

⁵⁰ Adnasohn Aqilla Respati, Reformulasi Undang-Undang ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation, Jurnal USM Law Review, 2024 h 74

harus dimasukkan,⁵¹ sehingga pengembang yang gagal menjalankan kewajiban kehati-hatian dan akibatnya menimbulkan kejahatan siber tetap dapat dimintai pertanggungjawaban pidana sesuai prinsip asas kesalahan dalam hukum pidana.

Dengan demikian, norma ini akan menjadi landasan hukum yang memberikan kepastian mengenai kedudukan dan tanggung jawab pengembang individu AI, baik dalam revisi UU ITE maupun pembentukan Undang-Undang khusus tentang AI di masa mendatang. Berdasarkan analisis tersebut, berikut adalah rekomendasi formulasi pasal yang dapat diusulkan untuk mengatur tanggung jawab pengembang individu AI secara tegas dan komprehensif:

Contoh formulasi norma untuk revisi UU ITE

I. Pasal [baru]

1. Setiap orang yang mengembangkan sistem kecerdasan buatan secara individu wajib:
 - a. Melakukan penilaian risiko atas potensi penyalahgunaan teknologi yang dikembangkannya;
 - b. Menyediakan dokumentasi teknis yang menjelaskan cara kerja dan tujuan penggunaan teknologi tersebut;
 - c. Menerapkan fitur keamanan minimum untuk mencegah penggunaan yang melanggar hukum;

⁵¹ Dedi Komarudin, *Dinamika Kebijakan Publik dan Inovasi Kecerdasan Buatan di Indonesia Tahun 2020-2024*, Arus Jurnal Sosial dan Humaniora, 2024. H 123-124

d. Mencantumkan larangan penggunaan teknologi untuk tujuan yang melanggar peraturan perundang-undangan.

2. Setiap orang yang dengan sengaja mengembangkan dan mendistribusikan sistem kecerdasan buatan yang digunakan untuk melakukan tindak pidana sebagaimana dimaksud dalam Pasal 27 dan Pasal 28 UU ini, dipidana dengan pidana penjara paling lama [x] tahun dan/atau denda paling banyak [x] rupiah.

3. Setiap orang yang karena kelalaiannya tidak menerapkan kewajiban sebagaimana dimaksud pada ayat (1) sehingga mengakibatkan sistem kecerdasan buatanya digunakan untuk tindak pidana yang merugikan pihak lain, dipidana dengan pidana penjara paling lama [x] tahun dan/atau denda paling banyak [x] rupiah.

a. Prinsip hukum untuk Undang-Undang Khusus AI

Jika penyusunan Undang-Undang khusus AI dirumuskan, maka prinsip hukum berikut dapat dimasukkan:

A. Prinsip akuntabilitas individual: Setiap pengembang individu AI bertanggung jawab atas desain dan risiko penggunaan teknologi ciptaannya.

B. Prinsip kehati-hatian (*due diligence*): Pengembang individu AI wajib mengidentifikasi dan mengurangi risiko penyalahgunaan teknologi sejak tahap desain.

C. Prinsip transparansi algoritma: Pengembang individu wajib memberikan informasi teknis dan batasan penggunaan secara terbuka kepada publik.

D. Prinsip pencegahan kejahatan teknologi (*technology crime prevention*): Setiap sistem AI wajib dilengkapi fitur yang dapat mencegah atau meminimalisir risiko penyalahgunaan untuk tindak pidana.

E. Prinsip kesetaraan pertanggungjawaban hukum (*equality of liability*): Pengembang individu AI memiliki kewajiban hukum yang sama dengan pengembang korporasi atas risiko teknologi ciptaannya.

Dengan adanya pengaturan ini, hukum di Indonesia tidak hanya akan menindak pelaku langsung atau pengguna AI yang melakukan kejahatan siber, tetapi juga memastikan adanya tanggung jawab pengembang individu sebagai pihak utama dalam proses penciptaan teknologi. Ketentuan ini penting untuk menciptakan keseimbangan antara kebebasan berinovasi dan perlindungan hukum bagi masyarakat di era digital saat ini. Oleh karena itu, diperlukan perumusan pasal atau prinsip hukum yang dapat dimasukkan ke dalam UU ITE atau dijadikan dasar dalam pembentukan Undang-Undang khusus mengenai AI di masa mendatang