

BAB II

BATASAN PENGEMBANG *ARTIFICEL INTELEGENCE* (AI) SEHINGGA DAPAT DIMINTAI PERTANGGUNG JAWABAN PIDANA ATAS PENYALAHGUNAAN TEKNOLOGI

2.1. Kedudukan Pengembang Individu *Artificial Intelligence* (AI) Dalam Sistem Hukum Pidana

Dalam tindak pidana biasa, pelaku kejahatan umumnya dapat dikenali secara langsung karena adanya interaksi dengan korban atau objek tindak pidana tersebut. Akan tetapi, dalam kejahatan siber, pelaku kejahatan seringkali berada dalam rantai yang panjang, mulai dari eksekutor, penyedia perangkat, perancang sistem, hingga pihak yang menyebarkan.¹⁷ Pengembang individu *Artificial Intelligence* (AI) sendiri dapat menempati posisi awal dalam rantai tersebut, sebab merekalah yang menciptakan alat atau sistem otomatis yang dimanfaatkan untuk melakukan kejahatan. Posisi ini dapat menempatkan pengembang sebagai pelaku tidak langsung, atau bahkan sebagai pihak yang turut serta (*accessory*) dalam tindak pidana tersebut.

¹⁷ Nasman, Pudji Astuti dan Dita Perwitasari *Etika Dan Pertanggungjawaban Penggunaan Artificial Intelligence Di Indonesia* Jurnal Hukum Lex Generalis. (2024)

2.1.1. Definisi dan Ruang Lingkup Pengembang individu *Artificial Intelligence* (AI)

Kemajuan teknologi *Artificial Intelligence* (AI) telah memberikan kesempatan yang luas bagi berbagai pihak untuk berpartisipasi, bukan hanya terbatas pada perusahaan teknologi besar atau lembaga tertentu, tetapi juga bagi individu yang memiliki keahlian di bidang pemrograman dan rekayasa perangkat lunak.¹⁸ Pengembang individu AI adalah mereka yang mengembangkan sistem kecerdasan buatan secara mandiri tanpa berada di bawah suatu badan hukum atau perusahaan. Mereka memanfaatkan teknologi *open-source*, berbagai platform online, serta akses terbuka terhadap data dan algoritma untuk menciptakan inovasi berbasis AI.¹⁹

Menurut definisi, pengembang individu *Artificial Intelligence* (AI) merupakan seseorang yang secara mandiri melakukan aktivitas merancang, melatih, menguji, dan menerapkan teknologi AI, baik untuk tujuan pendidikan, komersial, penelitian, maupun kepentingan sosial.²⁰ Secara konsep, pengembang individu AI adalah perseorangan yang melakukan proses desain, pembuatan, pelatihan, pengujian, dan/atau implementasi sistem AI tanpa berada di bawah suatu badan hukum. Mereka dapat berasal

¹⁸ Almira Ulimaz, et al. , Analisis Dampak Kolaborasi Pemanfaatan Artificial Intelligences (AI) Dan Kecerdasan Manusia Terhadap Dunia Pendidikan Di Indonesia, *Journal Of Social Science Research*, 2024

¹⁹ Grace Juanita, *Pemanfaatan Kecerdasan Artifisial (Artificial Intelligence/AI) Dalam Kerangka Pancasila*, *Jurnal Interpretasi Hukum*, 2024

²⁰ Pengembang artifificial Intelegence (AI) [bm.com/id-id/think/topics/ai-developer#:~:text=Pengembang%20kecerdasan%20buatan%20\(AI\)%20adalah,pengalaman%20pengguna%20yang%20lebih%20baik](https://bm.com/id-id/think/topics/ai-developer#:~:text=Pengembang%20kecerdasan%20buatan%20(AI)%20adalah,pengalaman%20pengguna%20yang%20lebih%20baik). Diakses tanggal 10 Juni 2025

dari kalangan akademisi, profesional di bidang teknologi informasi, atau masyarakat umum yang memiliki keterampilan teknis dalam pemrograman dan pembelajaran mesin (*machine learning*).²¹ Ruang lingkup kegiatannya meliputi:

Pemilihan dan penyesuaian algoritma *Artificial Intelligence* AI (*machine learning, deep learning, NLP, dll*);

1. Pengumpulan dan pengolahan data;
2. Pelatihan model kecerdasan buatan (*model training*);
3. Pengujian dan penerapan sistem *Artificial Intelligence* (AI) ke dalam platform tertentu (aplikasi web, chatbot, bot media sosial, dll).

Walaupun bekerja secara individu, peran pengembang ini tidak bisa dianggap remeh. Dalam berbagai kasus, pengembang individu berhasil menciptakan sistem *Artificial Intelligence* (AI) yang kemudian dimanfaatkan secara luas oleh masyarakat. Oleh karena itu, penting untuk memperjelas batasan serta tanggung jawab hukum mereka, khususnya ketika sistem tersebut digunakan untuk melakukan kejahatan siber.

2.1.2. Pengembang Individu *Artificial Intelligence* (AI) sebagai Subjek Hukum Pidana

Dalam hukum pidana Indonesia, terdapat prinsip mendasar bahwa tanggung jawab pidana hanya dapat dikenakan kepada subjek hukum yang

²¹ Muhammad Fauzen Adiman, et al. *Pengembangan Aplikasi Berbasis Artificial Intelligence (AI) Mengubah Paradigma Teknologi Informasi*, Indonesia Research Journal on Education, 2024

dianggap cakap dan memenuhi syarat menurut hukum. Subjek hukum pidana pada umumnya dibagi menjadi dua, yaitu individu (*natural person*) dan badan hukum atau korporasi (*legal entity*). Namun, dengan kemajuan teknologi, muncul subjek-subjek hukum baru yang memicu perdebatan, salah satunya adalah pengembang individu *Artificial Intelligence* (AI). Pengembang individu *Artificial Intelligence* (AI) adalah seseorang yang mengembangkan sistem kecerdasan buatan secara mandiri tanpa berada di bawah lembaga atau perusahaan manapun.

Mereka merancang, melatih, dan mendistribusikan sistem AI secara pribadi untuk berbagai keperluan, baik yang diakui secara hukum maupun yang berisiko melanggar ketentuan hukum, termasuk untuk melakukan kejahatan siber.²²

a. Pengembang Individu sebagai *Natural Person*

Sebagai manusia, pengembang individu merupakan subjek hukum pidana yang diakui. Berdasarkan KUHP Indonesia, seseorang dapat dimintai pertanggungjawaban pidana apabila memenuhi unsur perbuatan melawan hukum (*actus reus*) serta unsur kesalahan atau kesengajaan (*mens rea*). Oleh karena itu, jika seorang pengembang individu *Artificial Intelligence* (AI) secara sadar dan sengaja membuat atau menyediakan

²²Pengembang *Artificial Intelligence* (AI), *loc. cit.*

sistem yang kemudian digunakan untuk melakukan tindak kejahatan, maka ia dapat dinyatakan sebagai pelaku tindak pidana.²³

Pertanggungjawaban tersebut tidak hanya berlaku ketika pengembang terlibat secara langsung, tetapi juga mencakup bentuk keterlibatan tidak langsung atau sebagai penyerta, misalnya memberikan bantuan teknis, menyediakan akses terhadap sistem, atau memberikan instruksi penggunaan. Contohnya, seorang pengembang yang membuat model AI untuk memalsukan suara atau wajah seseorang (*deepfake*) dan kemudian mendistribusikannya kepada pihak lain yang memanfaatkannya untuk melakukan penipuan atau mencemarkan nama baik..

2.1.3. Peran Pengembang individu Artificial Intelligence (AI) dalam Rantai Tindak Pidana Siber

Kejahatan siber atau *cybercrime* memiliki karakteristik yang rumit, terorganisir, dan umumnya melibatkan lebih dari satu pelaku. Dalam banyak kejadian, kejahatan siber dijalankan melalui kolaborasi berbagai pihak yang masing-masing memiliki perannya sendiri dalam rangkaian tindakan pidana.²⁴ Salah satu pihak yang sering terabaikan dalam penegakan hukum adalah pengembang *Artificial Intelligence* (AI), terutama pengembang individu yang memiliki kontribusi teknis dalam pembuatan atau penyebaran sistem AI yang kemudian dimanfaatkan untuk melakukan tindak kejahatan.

²³ Ahmad Sofian, *Konsepsi Subjek Hukum dan Pertanggungjawaban Pidana Artificial Intelligence*, Halu Oleo Law, 2025, h 57

²⁴ *Ibid.*

Peran pengembang dalam kejahatan siber ini dapat diklasifikasikan ke dalam beberapa bentuk., antara lain:

a. Sebagai Pencipta Teknologi

Pengembang *Artificial Intelligence* (AI) memiliki peran sebagai pihak yang mendesain dan menciptakan sistem atau perangkat lunak yang kemudian digunakan dalam tindak pidana siber.²⁵ Contohnya meliputi pembuatan *algoritma deepfake*, *chatbot* untuk tujuan penipuan, alat *web scraping* yang melanggar privasi, atau botnet yang dimanfaatkan untuk serangan *DDoS*. Dalam hal ini, meskipun pengembang tidak terlibat langsung dalam pelaksanaan kejahatan, ia telah menyediakan teknologi sebagai sarana untuk melakukan tindak pidana tersebut.

Apabila dalam proses pengembangan sistem tersebut terdapat unsur kesengajaan atau ia mengetahui bahwa karyanya akan digunakan untuk tujuan ilegal, maka pengembang dapat dimintai pertanggungjawaban pidana sebagai pelaku tidak langsung atau pihak yang turut serta (*accessory*) dalam kejahatan.

b. Sebagai Fasilitator dan Penyedia Akses

²⁵ Reyhan Haqiqi Alif Fourniawan, Ade Eviyanti, dan, Suhendro Busono *Pengembangan Artificial Intelligence Berupa Virtual Assistant Mobile Menggunakan Framework Flutter* , Jurnal tekinkom, 2024

Pengembang juga dapat berperan sebagai penyedia atau penyalur teknologi *Artificial Intelligence* (AI) yang memiliki risiko tinggi penyalahgunaan. Hal ini dapat terjadi melalui beberapa cara, seperti:

1. Mengunggah sistem ke platform *open-source*;
2. Memberikan akses kepada pihak lain melalui API atau layanan hosting
3. Menjual atau menyewakan produk AI kepada pihak yang diketahui akan menggunakannya untuk tujuan melanggar hukum.

Dalam posisi ini, pengembang berfungsi sebagai fasilitator, yaitu pihak yang mempermudah terlaksananya kejahatan. Menurut hukum pidana, tindakan semacam ini dapat digolongkan sebagai bentuk membantu pelaksanaan tindak pidana, terutama apabila dapat dibuktikan bahwa pengembang mengetahui atau menyadari potensi dampak dari perbuatannya.

c. Sebagai Bagian dari Konspirasi Digital

Dalam beberapa kasus, pengembang *Artificial Intelligence* (AI) terlibat secara aktif dalam konspirasi tindak pidana digital, yakni adanya kerja sama atau kesepakatan antara pengembang dengan pelaku utama untuk menggunakan sistem AI dalam melaksanakan kejahatan.²⁶ Contohnya, pengembang bekerja sama dengan pelaku penipuan *online* untuk menciptakan sistem AI yang dapat meniru suara korban dalam praktik *voice phishing*. Peran semacam ini bersifat langsung dan menjadikan pengembang

²⁶ Problem Payung Hukum dalam Penggunaan Artificial Intelligence <https://www.hukumonline.com/berita/a/problem-payung-hukum-dalam-penggunaan-artificial-intelligence-lt66d4b01adeaf2/> diakses pada tanggal 15 juni 2025

sebagai bagian integral dari pelaku tindak pidana, sesuai dengan ketentuan Pasal 55 KUHP tentang turut serta melakukan kejahatan.

d. Peran Tidak Langsung tetapi Berdampak Hukum

Ada kalanya pengembang *Artificial Intelligence* (AI) tidak memiliki niat jahat secara langsung, namun kelalaian dalam perancangan sistem, kurangnya pengawasan, atau pembiaran atas penyalahgunaan teknologinya dapat menimbulkan tanggung jawab hukum. Dalam situasi seperti ini, pertanggungjawaban pidana dapat dikenakan melalui konsep *culpa*, yaitu kesalahan yang timbul akibat kelalaian atau kurang hati-hati.

Dengan demikian, meskipun posisi pengembang AI dalam rantai kejahatan siber seringkali tidak terlihat, perannya sangat strategis. Oleh karena itu, diperlukan adanya norma hukum yang secara tegas mengatur tanggung jawab pengembang, agar semua pihak yang terlibat dalam kejahatan siber dapat dimintai pertanggungjawaban secara adil dan proporsional.

2.1.4. Konsep Penyertaan Dalam Hukum Pidana Dan Implikasinya Terhadap Pengembang Individu *Artificial Intelligence* (AI)

Dalam hukum pidana, konsep penyertaan (*deelneming*) digunakan untuk menjelaskan keterlibatan lebih dari satu orang dalam melakukan suatu tindak pidana. Prinsip ini memungkinkan hukum pidana menjerat bukan hanya pelaku utama, tetapi juga mereka yang meskipun tidak terlibat secara langsung, tetap memiliki andil dalam terjadinya kejahatan. Dalam ranah

pengembangan teknologi, khususnya kecerdasan buatan (*Artificial Intelligence/AI*), konsep penyertaan menjadi relevan ketika teknologi yang dibuat oleh seorang pengembang individu dimanfaatkan untuk melakukan tindakan kriminal, baik secara langsung maupun tidak langsung.

a. Pengertian dan Jenis-Jenis Penyertaan Menurut KUHP

Kitab Undang-Undang Hukum Pidana (KUHP) Indonesia mengatur mengenai penyertaan dalam Pasal 55 dan Pasal 56. Berdasarkan ketentuan tersebut, bentuk-bentuk penyertaan dalam tindak pidana meliputi:

Pasal 55 ayat (1) KUHP: Orang yang melakukan tindak pidana, orang yang menyuruh orang lain melakukan, serta mereka yang turut serta melakukan tindak pidana tersebut

Mereka yang memberikan kesempatan, sarana, atau keterangan untuk terjadinya tindak pidana, baik dengan cara memberi janji atau imbalan, menyalahgunakan kekuasaan, menggunakan kekerasan, maupun melakukan tipu daya.

Pasal 56 KUHP:

Mereka yang sengaja memberi bantuan pada waktu atau sebelum kejahatan dilakukan. Dengan kata lain, penyertaan dalam hukum pidana terdiri dari:

1. Pelaku langsung (*dader*);
2. Pelaku yang menyuruh melakukan (*doen pleger*);
3. Pelaku yang turut serta (*medepleger*);

4. Pembantu (*medeplichtige*).

Setiap peran dalam struktur penyertaan tersebut dapat dikenakan pertanggungjawaban pidana, tergantung pada kontribusi dan intensi masing-masing pihak.

b. Relevansi Konsep Penyertaan terhadap Pengembang AI

Dalam kasus kejahatan siber yang memanfaatkan teknologi AI, pengembang individu dapat dikategorikan sebagai penyerta, tergantung pada perannya serta sejauh mana keterlibatannya dalam tindak pidana tersebut. Berikut adalah beberapa contoh bagaimana konsep penyertaan dapat diterapkan terhadap pengembang AI:

1. Sebagai Pelaku yang Menyuruh Melakukan

Jika seorang pengembang secara aktif menciptakan sistem AI dan memerintahkan orang lain untuk menggunakannya dalam melakukan kejahatan, seperti pembuatan deepfake pornografi atau chatbot untuk penipuan, maka ia dapat dimintai pertanggungjawaban sebagai pihak yang menyuruh melakukan tindak pidana sesuai dengan Pasal 55 ayat (1) angka 1 KUHP.

2. Sebagai Pelaku yang Turut Serta Melakukan

Apabila pengembang bekerja sama secara sadar dengan pihak lain untuk bersama-sama merancang dan menggunakan sistem AI dalam melakukan kejahatan, maka ia termasuk dalam kategori turut serta

melakukan tindak pidana sebagaimana diatur dalam Pasal 55 ayat (1) angka 1 KUHP. Situasi seperti ini umumnya terjadi pada konspirasi digital atau kolusi dalam kejahatan siber berbasis teknologi.

3. Sebagai Pembantu Tindak Pidana (*Medeplichtige*)

Apabila pengembang tidak ikut serta secara langsung dalam pelaksanaan kejahatan, tetapi memberikan sarana atau bantuan seperti menyediakan sistem, kode program, atau akses ke teknologi AI yang kemudian digunakan untuk melakukan kejahatan, maka dapat dianggap sebagai pembantu tindak pidana sesuai dengan Pasal 56 KUHP.²⁷ Dalam kasus ini, aspek penting yang harus dibuktikan adalah bahwa pengembang mengetahui atau setidaknya patut menduga bahwa sistem yang dibuatnya akan disalahgunakan.

5. Tantangan Pembuktian dalam Konteks Teknologi *Artificial Intelligence* (AI)

Penerapan konsep penyertaan terhadap pengembang *Artificial Intelligence* (AI) tidaklah mudah. Terdapat sejumlah tantangan utama dalam proses pembuktiannya, antara lain:

6. Kesulitan Membuktikan *Mens Rea* (Niat atau Kesengajaan)

Karena AI memiliki sifat otonom dan dapat belajar serta berkembang secara mandiri, pengembang kerap beralasan bahwa mereka

²⁷ Mudha'i Yunus, Hendra Saputra, dan Prima Angkupi, *Tantangan Hukum dalam Pengembangan Teknologi Kecerdasan Buatan (AI)*, JURNAL RENVOI, 2024

tidak mengetahui atau tidak berniat agar sistem yang dibuat digunakan untuk tujuan kejahatan.

7. Netralitas Teknologi

Sebagian besar teknologi AI bersifat umum (*general purpose*) sehingga dapat dimanfaatkan baik untuk tujuan positif maupun negatif. Hal ini menyulitkan pembuktian bahwa sejak awal pengembang memiliki niat jahat.

8. Distribusi Terbuka dan *Open-Source*

Pengembang yang merilis teknologinya secara bebas sering berdalih bahwa siapa pun dapat menggunakannya, sehingga ia tidak memiliki kendali atas potensi penyalahgunaan oleh pihak lain.

9. . Implikasi Hukum terhadap Pertanggungjawaban Pengembang

Penerapan konsep penyertaan terhadap pengembang individu *Artificial Intelligence* (AI) membawa sejumlah implikasi penting dalam hukum pidana, antara lain:

10. Memperluas Subjek Hukum dalam Tindak Pidana Siber

Dengan mengakui pengembang sebagai bagian dari penyerta, cakupan pelaku kejahatan siber tidak hanya terbatas pada eksekutor, tetapi juga meliputi pihak-pihak di belakang layar yang memberikan kontribusi teknis.

11. Mendorong Praktik Pengembangan Teknologi yang Beretika dan Patuh Hukum

Ancaman sanksi pidana bagi pengembang yang lalai atau dengan sengaja mendukung tindak pidana akan menumbuhkan tanggung jawab lebih tinggi dalam proses pengembangan AI, termasuk penerapan prinsip *privacy by design* dan *ethics by design*.

12. Membuka Jalan Bagi Reformasi Regulasi

Ketiadaan aturan khusus yang mengatur penyertaan pengembang dalam kejahatan siber menunjukkan perlunya pembaruan regulasi, baik melalui revisi UU ITE, pembentukan undang-undang khusus terkait AI, maupun penambahan norma baru dalam KUHP nasional ke depan..

2.2. Unsur Pertanggungjawaban Pidana dan Kaitannya dengan Tindakan Pengembang *Artificial Intelligence* (AI)

2.2.1. Unsur Perbuatan Pidana (*Actus Reus*)

Actus reus merupakan unsur objektif dalam tindak pidana yang menunjukkan adanya perbuatan atau tindakan nyata yang melanggar hukum.²⁸ Dalam kaitannya dengan pengembang individu *Artificial Intelligence* (AI), unsur ini terpenuhi apabila terdapat tindakan aktif seperti merancang, membuat kode program, atau mengunggah sistem AI yang

²⁸ Actus reus https://www.law.cornell.edu/wex/actus_reus diakses pada tanggal 18 juni 2025

dapat digunakan untuk kejahatan siber, misalnya manipulasi data, penyebaran malware, atau pencurian data pribadi.

Tindakan yang dilakukan oleh pengembang individu menjadi penting apabila sistem yang diciptakannya secara teknis memungkinkan terjadinya aktivitas melawan hukum. Perbuatan fisik tersebut memiliki relevansi pidana jika dapat dibuktikan menimbulkan dampak nyata bagi pihak lain dan menjadi bagian dari rangkaian penyebab terjadinya tindak pidana. Dalam hal ini, perbuatan pengembang tidak dapat dianggap netral apabila sistem yang dibuat memiliki fungsi yang secara langsung memfasilitasi pelanggaran hukum.

2.2.2. Unsur Kesalahan (*Mens Rea*): Kesengajaan dan Kelalaian

Mens rea merupakan unsur subjektif yang menunjukkan keadaan batin atau sikap mental dari pengembang individu dalam melakukan perbuatannya. Dalam hukum pidana, dua bentuk kesalahan utama adalah kesengajaan (*dolus*) dan kelalaian (*culpa*)²⁹. Kesengajaan muncul ketika pengembang individu secara sadar merancang sistem AI dengan fitur-fitur yang diketahuinya dapat digunakan untuk tujuan kejahatan. Contohnya, jika seorang pengembang menambahkan kode tersembunyi yang dapat dimanfaatkan untuk meretas atau menyalahgunakan data pengguna, maka ia dianggap memiliki *mens rea* dalam bentuk *dolus*.

²⁹ *Mens rea* <https://www.hukumonline.com/klinik/a/arti-mens-rea-dalam-hukum-pidana-lt6736aa8d70465/> diakses tanggal 18 juni 2025

Sebaliknya, kelalaian terjadi apabila pengembang tidak menerapkan standar keamanan yang memadai, gagal menguji risiko yang mungkin timbul dari sistem AI yang dibuat, atau mengabaikan potensi penyalahgunaan. Meskipun tidak terdapat niat jahat, kelalaian semacam ini tetap dapat menjadi dasar pertanggungjawaban pidana apabila terbukti menimbulkan akibat pidana karena kurangnya kehati-hatian. Dengan demikian, penilaian terhadap unsur *mens rea* pengembang individu menjadi sangat penting untuk menentukan apakah ia layak dimintai pertanggungjawaban pidana atas tindakannya..

2.2.3. Hubungan Kausal Antara Perbuatan Pengembang Individu *Artificial Intelligence* (AI) dan Akibat Pidana

Dalam hukum pidana, salah satu unsur utama yang perlu dibuktikan untuk menetapkan pertanggungjawaban pidana adalah adanya hubungan sebab akibat (*causaliteit*) antara tindakan pelaku dan akibat yang ditimbulkannya. Hubungan kausal ini menjadi dasar untuk menentukan apakah suatu akibat pidana dapat dibebankan sebagai tanggung jawab pelaku atau tidak³⁰. Dalam konteks pengembang individu *Artificial Intelligence* (AI), hubungan kausal fokus pada keterkaitan antara tindakan pengembang dalam merancang, mendesain, atau memprogram AI dengan terjadinya tindak pidana yang dilakukan menggunakan atau sebagai akibat dari AI tersebut. Aspek ini penting karena AI berfungsi sebagai alat atau

³⁰ Aryo Fadlian, “Pertanggungjawaban Pidana Dalam Suatu Kerangka Teoritis” Jurnal Hukum Positum, 2020 h 43

sistem otonom yang mengeksekusi perintah dan keputusan berdasarkan algoritma yang dibuat oleh pengembang.

Secara teori³¹, konsep hubungan kausal dapat dianalisis menggunakan dua pendekatan utama, yaitu::

- a. Teori *Conditio sine qua non* (kondisi tanpa mana akibat tidak akan terjadi)

Menurut teori ini, setiap tindakan yang menjadi syarat bagi terjadinya suatu akibat dianggap memiliki hubungan kausal. Artinya, apabila tindakan pengembang AI – seperti menambahkan fitur tertentu yang berpotensi disalahgunakan atau tidak melakukan langkah pencegahan terhadap risiko penyalahgunaan – menjadi syarat terjadinya tindak pidana melalui AI tersebut, maka dapat disimpulkan terdapat hubungan sebab akibat antara tindakan pengembang dan kejahatan yang timbul.

- b. Teori *Adequate Causation* (sebab yang wajar)

Teori ini membatasi hubungan kausal hanya pada tindakan yang secara umum dan layak dapat menyebabkan timbulnya akibat tersebut. Dalam praktiknya, apabila pengembang AI menyadari atau seharusnya menyadari bahwa desain maupun program yang dikembangkannya berpotensi digunakan untuk melakukan kejahatan siber seperti pornografi *deepfake*

³¹ Wasistha Budiarja Darmawan *Tinjauan Hukum Pidana Terhadap Pertanggungjawaban Pidana Lingkungan Yang Dilakukan Oleh Korporasi*, jurnal universitas 11 maret, 2015 h 8

atau penipuan, maka dapat dianggap terdapat hubungan kausal yang layak antara tindakannya dengan akibat pidana yang terjadi.

Dalam praktik penegakan hukum, membuktikan adanya hubungan kausal bukanlah hal yang sederhana, sebab AI memiliki sifat otonom untuk belajar (*machine learning*) dan dapat mengambil tindakan berdasarkan input data tanpa selalu memerlukan instruksi langsung dari pengembangnya.³² Oleh karena itu, dalam menilai hubungan kausal ini, perlu dipertimbangkan:

1. Apakah pengembang memiliki kontrol atas sistem AI saat AI melakukan tindak pidana
2. Apakah terdapat kelalaian atau kesengajaan pengembang dalam menciptakan algoritma yang berpotensi melanggar hukum
3. Apakah akibat pidana tersebut merupakan risiko yang wajar dapat diperkirakan oleh pengembang (*foreseeable risk*)

Sebagai ilustrasi, jika seorang pengembang individu AI membuat aplikasi *deepfake* dengan fitur yang memungkinkan manipulasi wajah secara bebas, lalu aplikasi tersebut digunakan untuk menghasilkan konten pornografi tanpa persetujuan korban, maka dapat dikemukakan bahwa terdapat hubungan kausal antara tindakan pengembang (merancang aplikasi

³² Ismi Adnin et al., *Responsivitas Tenaga Pendidik Terhadap Penyusunan Kebijakan Surat Edaran Pedoman Etika Artificial Intelligence*, PAMARENDA : Public Administration and Government Journal, 2024 h 74-85

dengan fitur tanpa batasan) dan akibat pidana yang timbul (seperti pencemaran nama baik atau penyebaran konten pornografi ilegal).

Batasan hubungan kausal yang dapat membebani pengembang *Artificial Intelligence* (AI) dengan pertanggungjawaban pidana terletak pada sejauh mana tindakan atau kelalaiannya memiliki keterkaitan langsung dengan tindak pidana yang dilakukan oleh pengguna. Hubungan kausal dianggap terpenuhi apabila perbuatan pengembang, baik berupa kesengajaan maupun kelalaian berat, secara nyata memfasilitasi, mempermudah, atau menciptakan kondisi yang memungkinkan terjadinya kejahatan. Sebaliknya, apabila tindak pidana timbul murni dari kehendak dan tindakan pengguna tanpa adanya kontribusi atau kelalaian yang substansial dari pengembang, maka batas kausalitas dianggap terputus dan pertanggungjawaban tidak dapat dialamatkan kepada pengembang. Dengan demikian, batasan yang jelas mencakup adanya keterkaitan langsung, keterdugaan wajar (*foreseeability*) atas risiko penyalahgunaan, serta peran aktif atau pasif pengembang dalam menciptakan peluang terjadinya tindak pidana.

Dengan demikian, hubungan kausal antara tindakan pengembang individu AI dan akibat pidana sangat ditentukan oleh apakah perbuatannya secara langsung atau sewajarnya dapat menimbulkan akibat pidana tersebut, serta sejauh mana unsur kesengajaan atau kelalaian hadir dalam proses desain, pembuatan, dan distribusi sistem AI tersebut..

2.3. Batasan Pertanggungjawaban Pengembang Individu Atas Tindakan Pihak Ketiga

Tanggung jawab pidana pengembang individu *Artificial Intelligence* (AI) atas tindak pidana yang dilakukan pihak ketiga menggunakan teknologi ciptaannya memiliki batasan hukum tertentu. Pembatasan ini diperlukan untuk menghindari perluasan pertanggungjawaban pidana yang melebihi prinsip keadilan pidana, khususnya berkaitan dengan asas legalitas, asas subjektivitas, serta prinsip kehati-hatian (*due diligence*) dalam proses pengembangan AI.

2.3.1. Prinsip *Lex Certa* Dan Legalitas Dalam Hukum Pidana

Prinsip *lex certa* dan legalitas merupakan asas mendasar dalam hukum pidana Indonesia, sebagaimana tertuang dalam Pasal 1 ayat (1) KUHP yang menyatakan bahwa “Tiada suatu perbuatan dapat dipidana kecuali berdasarkan kekuatan aturan pidana dalam perundang-undangan yang telah ada.” Asas *lex certa* mengharuskan rumusan tindak pidana disusun dengan jelas, tidak menimbulkan multitafsir, dan dapat dipahami secara tegas oleh setiap warga negara.

Prinsip legalitas dan *lex certa* ini bersumber dari asas *nullum crimen, nulla poena sine lege*, yang berarti tidak ada perbuatan yang dapat dipidana tanpa adanya ketentuan hukum yang mengaturnya terlebih dahulu.³³ Asas

³³ Asas Legalitas : Pengertian, Tujuan dan Prinsip <https://fahum.umsu.ac.id/info/asas-legalitas-pengertian-tujuan-dan-> diakses pada tanggal 28 juni 2025

tersebut diadopsi dari tradisi hukum pidana Eropa Kontinental, khususnya Belanda dan Jerman, dan tercermin dalam

A. Pasal 1 ayat (1) KUHP

Menegaskan bahwa seseorang hanya dapat dijatuhi pidana jika terdapat aturan pidana yang mengatur perbuatan tersebut secara tegas dalam perundang-undangan. Dengan kata lain, peraturan pidana tidak boleh berlaku surut, sehingga melindungi warga negara dari kriminalisasi atas perbuatan yang belum diatur sebelumnya.

B. *Lex Certa*

Prinsip ini merupakan bagian dari asas legalitas yang menuntut agar setiap aturan pidana dirumuskan dengan jelas, tegas, dan tanpa menimbulkan penafsiran ganda. Tujuannya adalah agar setiap orang mengetahui secara pasti perbuatan apa saja yang dilarang dan sanksi apa yang akan dikenakan jika melanggarnya. Apabila rumusan delik tidak jelas, maka hal tersebut akan bertentangan dengan prinsip kepastian hukum sebagaimana dijamin dalam Pasal 28D ayat (1) UUD 1945. Dalam kaitannya dengan pertanggungjawaban pengembang AI, penerapan asas legalitas dan *lex certa* menegaskan bahwa:

- a. Pengembang individu hanya dapat dimintai pertanggungjawaban apabila terdapat aturan pidana yang secara tegas mengatur perbuatan yang dilakukannya sebagai tindak pidana, baik berupa kesengajaan (*dolus*) maupun kelalaian (*culpa*).

- b. Tidak dapat dikenakan pertanggungjawaban pidana atas tindakan pihak ketiga yang menggunakan AI secara melawan hukum tanpa adanya unsur kesengajaan atau kelalaian pengembang dalam menciptakan sistem yang memungkinkan kejahatan tersebut.

Norma pidana tidak boleh ditafsirkan meluas (*extensive interpretation*) sehingga mengorbankan kepastian hukum bagi pengembang.

2.3.2. Asas Subjektivitas Dan Batas Maksimal Pertanggungjawaban

Asas subjektivitas menyatakan bahwa pertanggungjawaban pidana hanya dapat dikenakan kepada seseorang atas kesalahan (*schuld*) pribadinya, bukan karena kesalahan orang lain. Dalam penerapannya:

1. Pengembang hanya bertanggung jawab atas kesalahannya sendiri, yaitu jika terdapat unsur kesengajaan (*dolus*) atau kelalaian (*culpa*) dalam perbuatannya yang menimbulkan akibat pidana.

Contohnya, jika pengembang dengan sengaja membuat AI yang dirancang untuk melakukan penipuan atau peretasan, maka ia bertanggung jawab atas akibat pidana yang ditimbulkan.

2. Jika AI disalahgunakan oleh pihak ketiga tanpa adanya keterlibatan pengembang, maka pertanggungjawaban pidana tidak dapat dibebankan kepada pengembang karena tidak terdapat kesalahan subjektif darinya. Hal ini sejalan dengan doktrin "*actio libera in causa*" yang menekankan adanya kehendak bebas pelaku saat melakukan perbuatan pidana.

3. Batas maksimal pertanggungjawaban pengembang individu AI ditentukan oleh tingkat kontrol dan kewenangan yang dimilikinya. Jika pengembang telah merilis AI sebagai *open source* dan tidak memiliki kontrol lebih lanjut atas modifikasi dan distribusi ulang oleh pihak ketiga, maka tanggung jawab pidananya terbatas.

Sebagai contoh, ketika seorang pengembang menciptakan platform AI untuk editing video yang pada dasarnya bersifat netral dan legal, kemudian digunakan oleh pihak ketiga untuk membuat konten deepfake pornografi tanpa persetujuan korban, maka pengembang tersebut tidak dapat dikenakan pidana karena tidak ada unsur kesengajaan atau kelalaian yang menyebabkan terjadinya perbuatan tersebut.

Namun, jika pengembang menyadari bahwa AI yang dibuatnya memiliki potensi besar untuk disalahgunakan dan ia tidak melakukan langkah mitigasi atau tidak memberikan peringatan, maka berdasarkan *doktrin culpa in omittendo* (kelalaian karena tidak melakukan tindakan pencegahan) ia dapat dimintai pertanggungjawaban pidana terbatas, tergantung pada sejauh mana risiko penyalahgunaan tersebut dapat diperkirakan (*foreseeability*).

2.3.3. Prinsip Kehati-Hatian Dan Akuntabilitas Etis

Selain asas legalitas dan subjektivitas, pengembang individu AI juga terikat pada prinsip kehati-hatian (*due diligence principle*) serta akuntabilitas etis (*ethical accountability*) yang menjadi standar moral dan

profesional dalam pengembangan teknologi AI. Prinsip kehati-hatian (*due diligence*) serta kewajiban melakukan tindakan pencegahan yang memadai (*reasonable precaution*) oleh pengembang AI pada dasarnya berakar dari teori *culpa* dalam hukum pidana. Teori ini menyatakan bahwa setiap individu memiliki tanggung jawab untuk mencegah timbulnya akibat yang secara wajar dapat dia prediksi dari tindakannya. Dalam konteks pengembangan AI, kewajiban tersebut mencakup tanggung jawab untuk melakukan penilaian risiko (*risk assessment*), mengimplementasikan fitur keamanan atau pembatasan akses, serta menyediakan pedoman penggunaan yang sesuai dengan norma etika dan hukum.

Selain itu, prinsip kehati-hatian ini ditegaskan pula dalam pedoman etika AI internasional, seperti *OECD AI Principles* yang mewajibkan pengembang memastikan AI dikembangkan secara aman, transparan, adil, dan akuntabel, serta dalam *UNESCO Recommendation on the Ethics of AI* (2021) yang menekankan perlindungan hak asasi manusia, keamanan, dan keberlanjutan. Oleh karena itu, apabila pengembang AI melanggar prinsip kehati-hatian ini, kelalaiannya dapat dijadikan dasar pembuktian culpa ketika risiko penyalahgunaan AI sebenarnya dapat diperkirakan dan dicegah sejak awal. Prinsip ini menetapkan bahwa:

- a. Pengembang wajib melakukan tindakan pencegahan yang layak (*reasonable precaution*) agar AI yang dikembangkannya tidak menimbulkan risiko kejahatan atau pelanggaran hak pihak lain.

Tindakan tersebut mencakup:

1. Melakukan *risk assessment* terhadap potensi penyalahgunaan AI.
2. Menerapkan fitur pengamanan atau pembatasan akses (misalnya *watermarking* pada AI *deepfake* atau verifikasi pengguna).
3. Memberikan panduan penggunaan yang etis dan legal dalam dokumentasi teknologi AI.
4. Prinsip kehati-hatian bersifat *preventif* dan etis. Namun, pelanggaran prinsip kehati-hatian dapat menjadi dasar pembuktian adanya kelalaian (*culpa*) jika akibat perbuatan pidana yang terjadi merupakan risiko yang wajar dapat diperkirakan.
5. Akuntabilitas etis menekankan pada tanggung jawab moral dan sosial pengembang dalam menciptakan teknologi yang aman dan bermanfaat bagi masyarakat. Hal ini sejalan dengan berbagai pedoman etika AI internasional seperti:
 - A. *Organisation for Economic Co-operation and Development* (OECD) AI Principles yang mengatur *fairness, transparency, dan accountability*.
 - B. UNESCO *Recommendation on the Ethics of AI* (2021) yang menekankan pada perlindungan HAM, keamanan, dan keberlanjutan.

Namun, pelanggaran terhadap prinsip akuntabilitas etis tidak secara otomatis dapat dijadikan dasar pemberian sanksi pidana apabila tidak ada norma hukum positif yang dilanggar. Umumnya, pelanggaran akuntabilitas etis termasuk dalam pelanggaran moral atau etika yang sanksinya dapat berupa sanksi administratif, seperti pencabutan sertifikat profesi; sanksi disipliner, misalnya teguran tertulis atau larangan praktik sementara;

tanggung jawab perdata berupa kewajiban membayar ganti rugi kepada pihak yang dirugikan; atau sanksi sosial berupa hilangnya kepercayaan publik terhadap pengembang maupun perusahaannya. Akan tetapi, pelanggaran etis tersebut tidak menimbulkan tanggung jawab pidana kecuali apabila perbuatan yang dilakukan juga memenuhi unsur tindak pidana menurut hukum yang berlaku.

Prinsip akuntabilitas etis ini lebih bersifat sebagai standar etik profesional yang dapat dijadikan landasan dalam penyusunan kebijakan atau regulasi di masa mendatang untuk memperjelas batas tanggung jawab pengembang AI di Indonesia. Dengan demikian, dapat disimpulkan bahwa batasan pertanggungjawaban pengembang individu AI atas perbuatan pihak ketiga harus sejalan dengan asas legalitas, prinsip subjektivitas, dan prinsip kehati-hatian, yang mengharuskan adanya kesalahan subjektif serta dasar hukum positif yang jelas untuk dapat dipidana, tanpa mengesampingkan tanggung jawab etis dalam memastikan penggunaan teknologi AI yang aman dan bertanggung jawab..

2.4. Kerangka Hukum Positif Indonesia Terkait Batas Pertanggungjawaban Pengembang Individu

2.4.1. Ketentuan Relevan Dalam Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE)

Dalam sistem hukum positif Indonesia, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), belum terdapat ketentuan yang secara khusus mengatur mengenai tanggung jawab pengembang

individu *Artificial Intelligence* (AI). UU ITE pada dasarnya hanya mengatur perbuatan melawan hukum yang berkaitan dengan informasi elektronik dan transaksi elektronik, dengan fokus utama pada pelaku yang mendistribusikan, mentransmisikan, atau memberikan akses terhadap konten ilegal atau yang menimbulkan kerugian, sebagaimana diatur dalam Pasal 27 hingga Pasal 29.

Secara khusus, Pasal 30 ayat (1), (2), dan (3) UU ITE melarang setiap orang untuk mengakses komputer atau sistem elektronik dengan cara yang melanggar hukum, dengan tujuan memperoleh atau menguasai informasi elektronik atau dokumen elektronik. Selain itu, Pasal 40 ayat (2a) UU ITE memberikan kewenangan kepada pemerintah untuk memutus akses atau memerintahkan penyelenggara sistem elektronik memutus akses terhadap informasi elektronik yang melanggar hukum. Namun, ketentuan ini juga tidak memuat pengaturan mengenai tanggung jawab *preventif* maupun tanggung jawab hukum khusus bagi pengembang AI yang menciptakan teknologi dengan potensi besar untuk disalahgunakan oleh pihak lain.

2.4.2. Kelemahan Dan Kekosongan Pengaturan Tentang Pengembang Individu AI Dalam UU ITE.

Kelemahan utama dalam UU ITE terkait pengembang individu AI adalah tidak adanya norma yang secara eksplisit mengatur tanggung jawab *preventif* maupun *represif* bagi pengembang. Kekosongan ini menciptakan beberapa persoalan hukum, yaitu:

a. Absennya Kewajiban Preventif bagi Pengembang

UU ITE belum memuat ketentuan yang mewajibkan pengembang untuk memastikan bahwa sistem AI yang dikembangkannya terlindungi dari potensi penyalahgunaan. Sebagai contoh, pengembang aplikasi *deepfake generator* tidak memiliki kewajiban hukum untuk menambahkan watermark permanen sebagai tanda keaslian atau menerapkan pembatasan berupa verifikasi identitas bagi pengguna. Ketiadaan kewajiban tersebut pada akhirnya membuka peluang terjadinya kejahatan siber, seperti pembuatan konten pornografi non-konsensual atau tindak penipuan daring.

b. Tidak Diaturnya Standar Desain dan Etika AI

UU ITE maupun peraturan pelaksanaannya belum memuat pengaturan mengenai standar desain yang etis dan aman bagi pengembangan AI (*AI safety and ethics by design*). Padahal, dalam literatur hukum teknologi, tanggung jawab preventif pengembang dianggap sebagai bagian dari kewajiban profesional berbasis prinsip kehati-hatian (*due diligence*) yang telah diterapkan di berbagai negara.

Selain UU ITE, Kitab Undang-Undang Hukum Pidana (KUHP) hanya mengatur pertanggungjawaban berdasarkan asas kesalahan (*fault liability*). Pasal 55 dan Pasal 56 KUHP mengatur mengenai penyertaan dalam tindak pidana, sehingga pengembang individu AI hanya dapat dimintai pertanggungjawaban sebagai penyerta apabila terbukti turut serta atau membantu pelaksanaan tindak pidana secara langsung. Dalam konteks

teknologi AI, pembuktian unsur *mens rea* (niat jahat) dari pengembang menjadi sulit karena sifat AI yang netral (*dual-use technology*) dan dapat dimanfaatkan baik untuk tujuan yang legal maupun ilegal.

Di sisi lain, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta dan Undang-Undang Nomor 13 Tahun 2016 tentang Paten hanya mengatur mengenai perlindungan hak kekayaan intelektual bagi pengembang AI, tanpa mencantumkan kewajiban atau tanggung jawab hukum apabila karya cipta tersebut digunakan untuk tindak pidana. Kondisi ini menimbulkan risiko *moral hazard*, di mana pengembang tetap mendapatkan perlindungan hukum atas hak cipta atau patennya, tetapi tidak dibebani kewajiban hukum apabila ciptaannya menimbulkan kerugian bagi masyarakat.

2.4.3. Implikasi Tidak Adanya Norma Khusus Terhadap Penegakan Hukum

Ketiadaan norma khusus yang mengatur tanggung jawab pengembang individu AI dalam UU ITE maupun KUHP menimbulkan sejumlah implikasi serius bagi penegakan hukum di Indonesia. Penegak hukum menghadapi kesulitan dalam menjerat pengembang AI yang produknya dimanfaatkan untuk tindak pidana apabila pengembang tersebut tidak terlibat secara langsung, karena belum adanya dasar hukum yang mengatur tanggung jawab *preventif* ataupun tanggung jawab atas kelalaian (*negligence liability*) pengembang dalam merancang AI yang aman. Ketidadaan norma khusus tentang tanggung jawab pengembang individu AI

dalam UU ITE maupun KUHP menimbulkan berbagai implikasi serius, yaitu:

a. Kesulitan dalam Penegakan Hukum terhadap Kejahatan Siber Berbasis AI

Penegak hukum menghadapi tantangan dalam memproses pengembang AI yang teknologinya digunakan untuk kejahatan apabila pengembang tersebut tidak terlibat secara langsung dalam tindak pidana. Kesulitan ini muncul karena belum adanya pengaturan mengenai tanggung jawab preventif atau pertanggungjawaban atas kelalaian (*negligence liability*) pengembang dalam merancang AI yang aman.

b. Lemahnya Perlindungan Hukum bagi Korban

Korban kejahatan siber yang melibatkan AI, misalnya korban deepfake pornografi, tidak memiliki dasar hukum yang memungkinkan mereka menuntut pengembang AI ketika teknologi tersebut dirancang tanpa dilengkapi fitur keamanan yang memadai. Akibatnya, upaya pemulihan kerugian dan rehabilitasi korban hanya terfokus pada pelaku langsung yang menyalahgunakan teknologi tersebut.

c. Tidak Terciptanya Deterrent Effect bagi Pengembang

Ketiadaan pengaturan mengenai tanggung jawab hukum bagi pengembang individu AI mengakibatkan hilangnya efek jera (*deterrent effect*) yang mendorong mereka untuk menerapkan prinsip kehati-hatian dan etika dalam proses pengembangan teknologi. Kondisi ini membuat para

pengembang cenderung hanya berfokus pada aspek inovasi dan keuntungan semata, tanpa mempertimbangkan risiko sosial yang mungkin timbul dari teknologi yang mereka kembangkan.

d. Kesenjangan dengan Regulasi Internasional

Ketiadaan pengaturan mengenai tanggung jawab pengembang individu AI membuat regulasi di Indonesia tertinggal dibandingkan perkembangan hukum internasional. Sebagai contoh, Uni Eropa melalui *EU AI Act* tahun 2024 telah mewajibkan para pengembang AI berisiko tinggi untuk mematuhi standar keamanan tertentu serta melakukan penilaian risiko (*risk assessment*) sebelum teknologi AI tersebut dapat digunakan secara luas oleh masyarakat.

Situasi ini juga berdampak pada lemahnya perlindungan hukum bagi korban kejahatan siber berbasis AI, seperti korban *deepfake* pornografi, karena mereka tidak memiliki dasar hukum yang kuat untuk menggugat pengembang AI apabila teknologi tersebut dibuat tanpa dilengkapi fitur keamanan yang memadai. Akibatnya, proses pemulihan kerugian hanya dapat dilakukan terhadap pelaku langsung, tanpa menyentuh pihak pengembang yang turut berkontribusi secara tidak langsung.

Selain itu, ketiadaan pengaturan mengenai tanggung jawab pengembang individu AI mengakibatkan tidak adanya efek jera (*deterrent effect*) yang mendorong pengembang untuk mengutamakan prinsip kehati-hatian dan etika dalam proses pengembangan teknologi. Akibatnya, para

pengembang cenderung hanya berfokus pada aspek inovasi dan keuntungan, tanpa mempertimbangkan dampak sosial yang dapat ditimbulkan. Tidak adanya norma yang mengatur kewajiban tersebut juga membuka peluang semakin meluasnya penyalahgunaan AI, karena tanpa adanya kewajiban hukum untuk memasang fitur keamanan, teknologi AI dapat dengan mudah dimanfaatkan untuk berbagai tindak kejahatan, seperti penipuan, pemerasan melalui *deepfake*, hingga serangan siber otomatis.

Kondisi ini menimbulkan ketidakpastian hukum (*legal uncertainty*) baik bagi penegak hukum, korban, maupun pengembang AI itu sendiri, karena belum adanya pedoman yang tegas mengenai batas tanggung jawab hukum mereka. Selain itu, ketiadaan norma khusus juga menghambat upaya pengembangan kebijakan keamanan siber nasional secara menyeluruh, sebab pengaturan yang ada saat ini hanya berfokus pada pelaku kejahatan sebagai pengguna AI, tanpa melibatkan pengembang yang memiliki kendali atas desain teknologi tersebut sejak awal. Dalam cakupan yang lebih luas, hal ini meningkatkan risiko terjadinya pelanggaran hak asasi manusia, seperti pelanggaran privasi dan kehormatan pribadi korban, serta berpotensi mengancam keamanan nasional apabila AI disalahgunakan untuk kepentingan spionase atau propaganda digital.³⁴

Di samping itu, ketertinggalan regulasi Indonesia dibandingkan dengan hukum internasional, seperti Uni Eropa melalui *EU AI Act* (2024)

³⁴ Nasman, Pudji Astuti dan Dita Perwitasari, *Etika Dan Pertanggungjawaban Penggunaan Artificial Intelligence Di Indonesia*, Jurnal Hukum Lex Generalis, 2024 h 11

yang mewajibkan pengembang AI berisiko tinggi untuk memenuhi standar keamanan dan melakukan penilaian risiko (*risk assessment*), menunjukkan adanya kesenjangan hukum yang perlu segera dibenahi agar Indonesia dapat menyeimbangkan kemajuan inovasi teknologi dengan perlindungan kepentingan publik secara optimal.

2.4.4. Urgensi Pengaturan Khusus Dalam UU ITE Atau Peraturan Baru Terkait AI

Kemajuan teknologi *Artificial Intelligence* (AI) yang begitu cepat telah menimbulkan berbagai dampak dalam bidang hukum, sosial, dan keamanan di Indonesia. Di satu pihak, AI memberikan peluang besar bagi inovasi dan peningkatan efisiensi di berbagai sektor, namun di pihak lain, pemanfaatannya juga menghadirkan potensi penyalahgunaan yang dapat merugikan masyarakat serta menimbulkan ketidakpastian hukum.³⁵ Oleh sebab itu, diperlukan langkah serius untuk mengatur secara tegas tanggung jawab pengembang individu AI dalam kerangka hukum nasional. Mengingat pesatnya perkembangan teknologi AI dan berbagai dampak yang ditimbulkannya bagi masyarakat Indonesia, pembentukan norma khusus yang mengatur tanggung jawab pengembang individu AI menjadi kebutuhan mendesak yang tidak dapat diabaikan. Hal ini penting untuk memastikan bahwa perkembangan teknologi sejalan dengan perlindungan

³⁵ Linda Permata Sari dan Nur Jannani, *Urgensi Regulasi Artificial Intelligence di Indonesia Perspektif Teori Hukum Responsif dan Sadd Al-Dzariah*, *AL-BALAD: Journal Of Constitutional Law*, 2024. H 65-72

kepentingan publik serta kepastian hukum dalam sistem hukum nasional.

Urgensi tersebut meliputi:

a. Menutup Kekosongan Hukum dan Memberikan Kepastian Hukum

Adanya norma khusus akan mengatasi kekosongan hukum yang selama ini membuat posisi pengembang individu AI berada dalam area abu-abu. Dengan regulasi yang jelas, para pengembang memperoleh kepastian hukum mengenai batas tanggung jawab mereka, baik dalam konteks preventif berupa kewajiban memastikan keamanan sistem AI, maupun dalam konteks represif melalui ancaman sanksi pidana atau administratif apabila lalai.

b. Mendorong Penerapan Prinsip Kehati-hatian dan Desain Aman (*Security by Design*)

Pengaturan tanggung jawab preventif dalam UU ITE atau peraturan khusus AI akan memotivasi pengembang individu AI untuk menerapkan prinsip kehati-hatian dan desain aman di seluruh tahapan pengembangan teknologi, mulai dari tahap perancangan, pengujian keamanan, hingga peluncuran produk ke publik.

c. Memperkuat Perlindungan Hukum bagi Masyarakat

Norma baru ini akan menjadi dasar hukum yang memungkinkan korban menuntut pertanggungjawaban pengembang AI apabila terjadi kerugian akibat kelalaian mereka dalam merancang sistem yang aman. Dengan demikian, tercipta keseimbangan antara kepentingan inovasi

teknologi dengan perlindungan hukum masyarakat dari risiko kejahatan siber berbasis AI.

d. Meningkatkan Reputasi dan Daya Saing Indonesia dalam Teknologi AI Global

Pengaturan yang jelas mengenai tanggung jawab pengembang individu AI juga akan meningkatkan citra Indonesia di mata internasional sebagai negara yang mengatur perkembangan AI secara bertanggung jawab dan beretika, sekaligus memperkuat daya saing ekosistem AI nasional di kancah global.

e. Menjadi Dasar Pembentukan Undang-Undang Khusus AI di Masa Depan

Norma awal dalam UU ITE dapat berfungsi sebagai fondasi pembentukan Undang-Undang khusus AI di masa depan, sebagaimana dilakukan oleh Uni Eropa melalui *EU AI Act*. Undang-undang khusus tersebut nantinya akan mengatur seluruh ekosistem AI secara komprehensif, mulai dari pengembang, penyedia layanan, hingga mekanisme pengawasan dan penegakan hukumnya.

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa diperlukan revisi terhadap UU ITE atau pembentukan regulasi baru berbasis *AI Law* yang secara eksplisit mengatur tanggung jawab pengembang individu AI. Pengaturan ini perlu mencakup kewajiban melakukan uji keamanan, penerapan standar desain yang etis, serta kewajiban untuk

memitigasi risiko penyalahgunaan teknologi. Dengan demikian, perkembangan AI di Indonesia dapat berlangsung secara aman dan memberikan manfaat maksimal bagi masyarakat, tanpa mengesampingkan prinsip perlindungan hukum dan hak asasi manusia.

