

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi terus berkembang pesat saat ini, perkembangan teknologi informasi dan komunikasi memberikan para penggunanya kemudahan dan akses informasi secara gratis dan mudah kapan saja dan dimana saja.¹ Inovasi merupakan salah satu bagian penting dalam era globalisasi saat ini, di mana inovasi merupakan bagian yang tidak terpisahkan dari kehidupan. Hal ini memungkinkan sains untuk menciptakan instrumen yang mendorong peningkatan teknologi informasi, mulai dari kerangka komunikasi hingga perangkat komunikasi cerdas, satu arah, dan dua arah.²

Dalam Kamus Besar Bahasa Indonesia (KBBI), pengembang diartikan sebagai "orang atau pihak yang menciptakan sesuatu." Sementara itu, menurut Wikipedia, pengembang elektronik diartikan sebagai orang yang membuat program komputer melalui proses pengkodean, pengujian, dan pengembangan kerangka kerja³. Dalam konteks hukum, pengembang sistem elektronik dapat diartikan sebagai subjek yang membangun atau membuat suatu sistem yang kemudian akan digunakan oleh penyelenggara atau pengguna.

¹ Imam Subekti, Heru Sukrisno, Sugeng Wahyudi, et al., "Reformulasi Kebijakan Kriminal Dalam Penanggulangan Kejahatan Berbasis Teknologi Kecerdasan Buatan" *Setara jurnal ilmu hukum* 2024 h.112

² Sinta Dewi Rosadi, *Hukum Siber Indonesia*, Refika Aditama Bandung 2020 h 56

³ Pengembang, <https://www.coursera.org/articles/ai-developer> diakses pada tanggal 3 Mei 2025

Dengan kata lain, pengembang merupakan pelaku awal dalam sistem biologis terkomputerisasi yang mengintegrasikan teknologi computer seperti pemantauan dan pengendalian, yang memiliki pengetahuan mendalam dan kendali awal atas desain dan kerja suatu sistem elektronik. Dalam kerangka hukum positif Indonesia, khususnya dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Undang-Undang Nomor 1 Tahun 2024 Perubahan kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dan Peraturan Pemerintah Nomor 71 Tahun 2019, penyelenggara sistem elektronik tidak secara tegas disebut atau diarahkan sebagai subjek hukum.

Peraturan tersebut hanya mengatur pihak-pihak yang disebut sebagai Penyelenggara Sistem Elektronik (PSE). Dalam Pasal 1 angka 6 Undang-Undang Nomor 19 Tahun 2016, Penyelenggara Sistem Elektronik (PSE) didefinisikan sebagai "setiap orang perseorangan, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik, baik sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan sendiri dan/atau keperluan pihak lain." Berdasarkan definisi tersebut, Penyelenggara Sistem Elektronik (PSE) adalah pihak yang menyediakan dan menjalankan sistem elektronik, tetapi tidak melibatkan perancang yang hanya merencanakan atau membangun sistem untuk digunakan oleh pihak lain. Mengakibatkan terjadi kekosongan hukum,

karena dalam praktiknya pengembang dapat berkontribusi terhadap potensi penyalahgunaan sistem, tetapi tidak memiliki status hukum yang jelas.

Internet memberikan peluang bagi pelaku kejahatan dunia maya untuk melakukan kejahatan dengan lebih sempurna, tersembunyi, terorganisasi, dan dapat memasuki ruang dan waktu dengan jangkauan yang sangat luas.⁴ Kemajuan yang inovatif dapat membuat akses data menjadi lebih mudah dan cepat dengan memanfaatkan web, hal ini berdampak pada perubahan perilaku baik individu maupun masyarakat secara luas saat ini. Perkembangan yang difokuskan di Indonesia sendiri mencakup berbagai teknologi canggih yaitu “(1) Kecerdasan buatan (*artificial intelligence*), (2) Perangkat fisik yang terhubung ke jaringan internet (*internet of thing* (IoT)), (3) Penggunaan teknologi terhadap peralatan atau aksesoris yang digunakan manusia (*wearables*), (4) Robotika dan sensor canggih, (5) Percetakan menggunakan teknologi 3 dimensi (*3D printing*)”.⁵

Kemajuan informasi memiliki dampak positif dan negatif, keduanya dapat diibaratkan sebagai dua sisi pedang bermata dua, di mana kemajuan informasi menyebabkan perubahan perilaku masyarakat. Selain itu, kemajuan informasi memberikan kesan bahwa dunia tidak memiliki batas. Namun, di balik kemajuan ini terdapat kekhawatiran tersirat tentang peningkatan pelanggaran

⁴ Bunga Dewi, “Politik Hukum Pidana Terhadap Penanggulangan Cybercrime” Jurnal Legislasi Indonesia, Vol 16, No. 1 (2019): h 1–5.

⁵ Ni Made Yordha Ayu Astiti, “Strict Liability of Artificial Intelligence: Pertanggungjawaban kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban?” undayana master law journal, 2023 h 145

mekanis, khususnya kejahatan dunia maya..⁶. Seiring berjalannya waktu, pada tahun 1955 peneliti Bernawa Newell dan Simon menciptakan master hipotesis rasional, yang merupakan pemrograman kecerdasan buatan *Artificial Intelligence* (AI) utama. Program ini membahas masalah sebagai diagram pohon, kemudian kerangka kerja kecerdasan buatan *Artificial Intelligence* (AI) memahami masalah dengan memilih cabang yang akan memberikan kesimpulan yang tepat.⁷

Perkembangan teknologi telah mengubah tatanan masyarakat dari masyarakat lokal menjadi masyarakat global. Kemajuan kecerdasan buatan *Artificial Intelligence* (AI) telah memberikan dampak yang besar terhadap berbagai aspek kehidupan di Indonesia, baik aspek ekonomi, sosial, hukum, dan lain sebagainya. Peluang yang dihasilkan menunjukkan potensi *Artificial Intelligence* (AI) dalam mendorong kemajuan yang signifikan di berbagai bidang dan memajukan kualitas hidup manusia. Dalam era *Transformasi Digital 5.0*, teknologi *Artificial Intelligence* (AI) telah menjadi penggerak utama perubahan sosial dan ekonomi. Namun, di balik manfaatnya, penerapan *Artificial Intelligence* (AI) juga menghadirkan tantangan dan risiko yang memerlukan pengendalian yang tidak biasa.⁸

⁶ Wahyu Beny Mukti Setiyawan, Erifendi Churniawan, dan Femmy Silaswaty Faried, “Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia,” *Jurnal USM Law Review*, h 3

⁷ Muhammad Dahria, “Kecerdasan Buatan (*Artificial Intelligence*),” *Jurnal Saintikom* vol V no 2 agustus 2008, h 187

⁸ Irawati Nastasia *Analisis yuridis atas kedudukan hukum & peran artificial intelligence (AI) dalam sistem hukum acara perdata indonesia*, Skripsi Fakultas Hukum Universitas Kristem Indonesia Tahun 2024, h 8

Industri hiburan, keamanan siber, dan komunikasi adalah beberapa bidang yang telah direvolusi oleh inovasi kecerdasan buatan *Artificial Intelligence* (AI). Inovasi deepfake adalah bentuk pemanfaatan kecerdasan buatan *Artificial Intelligence* (AI) yang semakin berkembang, dengan inovasi berbasis pembelajaran mesin yang memungkinkan kontrol konten visual dan suara dengan tingkat keaslian yang tinggi. *Deepfake* dapat digunakan secara khusus dalam bisnis film, pendidikan, dan hiburan, tetapi juga memiliki potensi luar biasa untuk disalahgunakan dalam berbagai bentuk kejahatan dunia maya. Kecerdasan buatan *Artificial Intelligence* (AI) di tengah kehidupan manusia memiliki dampak yang kuat. Namun, saat ini kecerdasan buatan *Artificial Intelligence* (AI) banyak disalahgunakan oleh penjahat dunia maya yang disebut dengan kecerdasan buatan-kejahatan *Artificial Intelligence Crime* (AIC).⁹

Salah satu bentuk kecerdasan buatan *Artificial Intelligence* (AI) yang saat ini sedang banyak diteliti adalah *deepfake*. *Deepfake* berasal dari kata *deep learning* dan *fake* yang dapat diartikan sebagai data audio-visual palsu berupa foto, rekaman, atau suara, yang dibuat melalui strategi pembelajaran mendalam. Pembelajaran mendalam sendiri merupakan bagian dari kecerdasan buatan *Artificial Intelligence* (AI) yang mengacu pada proses komputasi, yang dapat belajar secara mandiri dan membuat keputusan yang cerdas.¹⁰

⁹Sinta Dewi Rosadi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional Ed. Revisi*, Refika Aditama, Bandung 2022, h.30

¹⁰ Grace Shao, *What 'DEEPFAKE' are and how they may be dangerous*, CNBC, 13 September 2019, <https://www.cnbc.com/2019/10/14/what-is-DEEPFAKE-and-how-it-might-be-dangerous.html>, diakses pada 29 Maret 2025

Deepfake, meskipun merupakan visual suara palsu yang dibuat dengan memanfaatkan kecerdasan buatan *Artificial Intelligence* (AI), tidak berarti *deepfake* dapat dengan mudah dilihat sebagai palsu dengan mata telanjang. Sebaliknya, *deepfake* dapat terlihat sangat asli dan unik tergantung pada jumlah informasi yang digunakan. Semakin banyak informasi dalam bentuk tes suara dan gambar wajah dari subjek sumber (orang yang wajah dan/atau suaranya ditampilkan dalam *deepfake*) yang digunakan, semakin baik dan asli hasil *deepfake* tersebut.¹¹

Deepfake yang merupakan salah satu kemajuan yang berasal dari kemajuan teknologi itu sendiri, banyak digunakan untuk melakukan kejahatan. Salah satu contoh nyata penggunaan teknologi ini untuk kejahatan adalah untuk menyebarkan konten porno yang kemudian dikenal luas sebagai *deepfake* porno. Tindakan membuat rekaman porno tersebut merugikan pihak yang wajah dan suaranya digunakan sebagai bahan untuk membuat rekaman porno. Hal ini dapat menimbulkan kesalahpahaman antara pihak yang digunakan (korban) dan orang-orang di sekitarnya. Selain itu, apabila video yang ditayangkan oleh *deepfake porn* tersebut sangat halus, ada kemungkinan korban yang wajah dan suaranya digunakan akan dicurigai sebagai tersangka penyebar video porno tersebut..¹²

Deepfake sering kali dimanfaatkan untuk menyebarkan data palsu, pemerasan, kritik, dan bahkan pencurian identitas tingkat lanjut yang dapat

¹¹ Jihadul Akbar Ulumando, *Urgensi Pengaturan Terhadap Penyalahgunaan Artificial Intelligence Di Indonesia*, Skripsi Fakultas Hukum Universitas Islam Sunan Ampel, Tahun 2023

¹² Renata Christha Auli, "Apa Itu Deepfake Porn Dan Jerat Pidana Bagi Pelakunya," Hukum Online, January 19, 2024,

merugikan orang dan mendidik. Kejahatan ini memiliki berbagai dampak negatif, baik secara finansial, sosial, maupun mental pada korbannya. *Deepfake* juga dapat dimanfaatkan untuk kontrol politik dengan membuat rekaman palsu yang menipu anggapan umum. Hal ini berpotensi melemahkan kestabilan sistem berbasis suara dan keamanan nasional.¹³ Oleh karena itu, penting untuk melihat sudut pandang kewajiban pidana bagi pihak-pihak yang terlibat dalam pengembangan dan penggunaan inovasi *Counterfeit Insights Artificial Intelligence* (AI) dalam kejahatan dunia maya berbasis deepfake.

Selain *Deepfake Porn*, ada banyak cara memanfaatkan inovasi *Deepfake Counterfeit Insights Artificial Intelligence* (AI) ini, seperti membuat rekaman atau gambar atau suara yang digunakan untuk kredit online, mengubah suara seseorang menjadi audio resmi yang disalahgunakan untuk mengambil keuntungan dari pelakunya. Hal ini menyebabkan banyak bahaya terkait masalah keamanan yang sangat memungkinkan penyalahgunaan inovasi *Counterfeit Insights Artificial Intelligence* (AI). Informasi pribadi seseorang sangat rentan terhadap pencurian informasi dan digunakan oleh orang yang tidak dapat dipercaya yang mengakibatkan keamanan setiap orang tidak terjaga.¹⁴

Kejahatan siber berbasis AI meliputi pencurian data (*data theft*) dengan menggunakan AI untuk meretas sistem keamanan, penipuan (*fraud*) melalui

¹³ Budi Raharjo , *Teori Etika Dalamn Kecerdasan Buatan Artifical Intelligence* , Yayasan prima agus Teknik , Semarang , h.110

¹⁴ Adnasohn Aqilla Respati., “*Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban*” Media Hukum Indonesia (MHI) .2024 h 65

manipulasi suara atau video menggunakan *deepfake* untuk menipu korban, serta serangan phishing yang lebih canggih dengan AI yang mampu meniru gaya bahasa dan perilaku target agar korban mudah tertipu. Selain itu, AI juga digunakan dalam serangan malware yang otonom (*AI-powered malware attacks*), di mana *malware* dapat beradaptasi dan menghindari deteksi antivirus konvensional. Dalam ranah kejahatan finansial, AI dimanfaatkan untuk *automated trading fraud*, di mana pelaku memanipulasi algoritma perdagangan saham atau *crypto* untuk keuntungan pribadi. Tidak hanya itu, AI juga digunakan untuk pengawasan ilegal (*illegal surveillance*) melalui teknologi *facial recognition* tanpa izin yang melanggar privasi, pembuatan konten pornografi non-konsensual, serta *hoaks* politik dengan *deepfake* untuk memanipulasi ucapan tokoh publik guna memengaruhi opini masyarakat.

Lebih jauh, AI dimanfaatkan dalam pemerasan (*extortion*) dengan mengancam korban menggunakan video palsu hasil *deepfake*, serangan DDoS berbasis AI (*AI-driven DDoS attacks*) yang dapat secara otomatis memilih waktu dan metode serangan paling efektif, pencurian identitas (*identity theft*) dengan meniru data biometrik atau perilaku digital korban, serta spionase siber (*cyber espionage*) untuk memperoleh data rahasia negara atau perusahaan..¹⁵

Dalam ranah hukum pidana, salah satu persoalan krusial yang dihadapi adalah menetapkan siapa yang seharusnya bertanggung jawab dalam kasus kejahatan yang melibatkan teknologi *Artificial Intelligence* (AI). Pertanyaan

¹⁵ Ellen Kusuma dan Nenden Sekar Arum, *Memahami Dan Menyikapi Kekerasan Berbasis Gender Online*, Southeast Asia Freedom of Expression Network, 2019 h 36

mendasar yang muncul adalah apakah tanggung jawab pidana hanya dibebankan kepada pelaku yang secara langsung menggunakan teknologi seperti *deepfake* untuk tujuan kejahatan, atau apakah pengembang *Artificial Intelligence* (AI) juga dapat dimintai pertanggungjawaban atas dampak yang ditimbulkan dari sistem yang mereka ciptakan¹⁶. Hingga kini, perdebatan mengenai batas dan cakupan tanggung jawab pidana bagi pengembang *Artificial Intelligence* (AI) dalam konteks kejahatan siber masih terus berlangsung.

Penelitian ini menjadi penting karena diperlukan kejelasan mengenai batasan-batasan dan kondisi tertentu yang dapat menjerat pengembang dalam pertanggungjawaban pidana. Hal ini berkaitan erat dengan asas-asas pokok dalam hukum pidana. Tanpa adanya batasan hukum yang tegas, terdapat risiko terjadinya kriminalisasi berlebihan (*overcriminalization*) atau bahkan terjadinya impunitas terhadap pihak pengembang. Sebagai perbandingan, beberapa negara telah mengambil langkah konkret dalam mengatur hal ini. Uni Eropa, melalui *Artificial Intelligence Act* dan pedoman etika digitalnya, Dalam regulasi Uni Eropa, pengembang sistem *Artificial Intelligence* (AI) diwajibkan bertanggung jawab secara hukum atas risiko dari sistem *Artificial Intelligence* (AI) berisiko tinggi (*high-risk AI systems*) yang mereka buat. Ini menunjukkan adanya kecenderungan global yang semakin mengedepankan akuntabilitas

¹⁶ Muhammad Dhafin Saptari, *Artificial Intelligence sebagai entitas subjek hukum perdata*, Skripsi Fakultas Hukum Universitas Katolik Parahyangan, Tahun 2022, h 10

hukum bagi pengembang, tidak hanya bagi pengguna atau penyedia layanan teknologi.

Oleh karena itu, penelitian ini memiliki nilai strategis dalam mengisi kekosongan regulasi mengenai tanggung jawab pidana pengembang sistem elektronik dalam konteks hukum nasional Indonesia. Selain itu, penelitian ini diharapkan dapat menjadi dasar normatif dalam merumuskan batasan pertanggungjawaban pengembang, sekaligus memperkuat posisi hukum Indonesia agar lebih adaptif terhadap perkembangan hukum global di era kecerdasan buatan dan teknologi digital.

1.2 Rumusan Masalah

1. Apa batasan pengembang *Artificial Intelligence* (AI) sehingga dapat dimintai pertanggung jawaban pidana atas penyalahgunaan teknologi yang mereka kembangkan?
2. Apa urgensi pengaturan tentang tanggung jawab pengembang *Artificial Intelligence* (AI) dalam UU ITE?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan dari penelitian ini adalah:

1. Untuk mengetahui apa batasan pengembang *Artificial Intelligence* (AI) sehingga dapat dimintai pertanggung jawaban atas teknologi *Artificial Intelligence* (AI) yang dikembangkan
2. Untuk mengetahui dan menganalisis perlunya pengaturan tanggung jawab pengembang *Artificial Intelligence* (AI) dalam UU ITE guna mencegah penyalahgunaan teknologi seperti *deepfake*

1.4 Manfaat Penelitian

Dengan adanya penelitian ini maka muncul lah manfaat bagi beberapa pihak:

1.4.1 Manfaat Teoritis

- a. Penelitian ini diharapkan dapat memberikan kontribusi teoritis terhadap pengembangan ilmu hukum pidana, khususnya dalam aspek pertanggungjawaban pidana terhadap pelaku kejahatan yang menggunakan teknologi berbasis kecerdasan buatan *Artificial Intelligence* (AI).
- b. Memberikan kontribusi terhadap literatur dan kajian akademik mengenai keterkaitan antara teknologi informasi dengan konsep pertanggungjawaban pidana dalam hukum positif Indonesia.
- c. Memberikan dasar pemikiran dan argumentasi hukum yang dapat dijadikan referensi dalam perumusan kebijakan atau pembentukan regulasi baru yang relevan dengan perkembangan teknologi *Artificial Intelligence* (AI) dan penggunaannya dalam kejahatan siber.

1.4.2. Manfaat Praktis

- a. Penelitian ini dapat menjadi referensi tambahan dalam pengembangan ilmu hukum pidana, khususnya yang berkaitan dengan pertanggungjawaban pidana dalam penggunaan teknologi berbasis kecerdasan buatan *Artificial Intelligence* (AI). Selain itu, hasil penelitian ini dapat dijadikan bahan ajar atau diskusi akademik dalam mata kuliah hukum pidana, hukum dan teknologi, atau hukum siber, guna

memperkaya literatur tentang dinamika kejahatan berbasis teknologi modern.

- b. Bagi masyarakat dan instansi pemerintah, penelitian ini diharapkan mampu menambah wawasan terkait dengan pertanggung jawaban dalam penyalahgunaan teknologi *artificial intelligence* (AI) dalam kacamata hukum pidana di Indonesia.
- c. Bagi mahasiswa, penelitian ini diharapkan dapat menambah pengetahuan dan dapat menjadi sumber referensi untuk penelitian selanjutnya.

1.5 Orisinalitas Penelitian

Nama Peneliti	Judul dan Tahun	Perbedaan	Persamaan
Muhammad Dhafin Saptari	<i>Artificial Intelligence</i> sebagai entitas subjek hukum perdata (2022)	Perbedaan dari penelitian terdahulu adalah pada penelitian terdahulu meneliti <i>Artificial intelligence</i> (AI) sebagai subjek hukum dan dilihat dari sudut pandang hukum perdata yang ada di indonesia	Persamaan dari peneliti terdahulu adalah tentang <i>Artificial Intelligence</i> (AI) dalam hukum yang ada

Irawati Nastasia	Analisis yuridis atas kedudukan hukum & peran <i>Artificial Intelligence</i> (AI) dalam sistem hukum acara perdata indonesia (2024)	Pada penelitian terdahulu Perbedaan Dilihat Dari Pemfokusan Penelitian Yang Dimana Pada penelitian terdahulu tentang kedudukan dan peran <i>Artificial Intelligence</i> (AI) dalam hukum acara perdata perbedaan terletak dimana focus penelitian adalah <i>Artificial Intelligence</i> (AI) sebagai subjek nya dan sudut pandang hukumnya.	Pada penelitian terdahulu persamaan nya dilihat dari terfokuskan tentang Peran <i>Artificial Intelligence</i> (AI)
Jihadul Akbar Ulumando	Urgensi Pengaturan Terhadap Penyalahgunaan <i>Artificial</i>	Pada penelitian terdahulu Perbedaan Dilihat Dari pemfokusan kebutuhan regulasi terhadap	Pada penelitian terdahulu Persamaan terlihat Dari Kedua penelitian mengangkat isu

	Intelligence Di Indonesia (2023)	penyalahgunaan <i>Artificial Intelligence</i> (AI) secara umum di Indonesia, dengan menekankan pentingnya pembentukan atau revisi regulasi agar dapat mengantisipasi dan mengatasi penyalahgunaan <i>Artificial Intelligence</i> (AI).	kekosongan atau ketidakjelasan hukum dalam menghadapi fenomena baru terkait <i>Artificial</i> <i>Intelligence</i> (AI) di Indonesia.
--	-------------------------------------	--	---

1.6 Tinjauan Pustaka

1.6.1. Teori Pertanggung Jawaban Pidana

Teori ini membahas tentang ketika seseorang atau entitas dapat dikenakan sanksi pidana. Dalam konteks pengembang *Artificial Intelligence* (AI), teori ini membantu menentukan apakah mereka bisa dimintai pertanggungjawaban atas penyalahgunaan teknologi *Artificial Intelligence* (AI).

1.6.2. Teori Perlindungan Hukum

Teori perlindungan hukum adalah teori yang menjelaskan tentang upaya melindungi hak-hak asasi manusia dan harkat martabat subjek hukum.

1.6.3. Teori Kepastian Hukum

Teori kepastian hukum adalah teori yang menjelaskan tentang kejelasan dan ketegasan hukum dalam masyarakat. Teori ini juga menjelaskan bahwa hukum harus jelas, dipahami dengan mudah, dan dapat diprediksi dalam pengambilan keputusan hukum.

1.6.4. Teori Pertanggungjawaban Korporasi (*Corporate Criminal Liability*)

Ketika pengembang *Artificial Intelligence* (AI) berbentuk perusahaan atau tim dalam suatu organisasi, teori ini dapat menjelaskan apakah badan hukum dapat dimintai pertanggungjawaban atas kejahatan siber.

1.6.5. Teori *Cybercrime* dan Hukum Teknologi

Konsep dalam studi hukum yang membahas kejahatan siber (*cybercrime*) terjadi serta bagaimana hukum beradaptasi untuk mengatur, mencegah, dan menghukum tindakan kriminal yang dilakukan menggunakan teknologi.

1.6.6. Teori Hukum dan Etika dalam Teknologi *Artifical Intelligence*

(AI)

Teori Hukum dan Etika dalam Teknologi *Artifical Intelligence* (AI) adalah pendekatan yang membahas bagaimana kecerdasan buatan *Artifical Intelligence* (AI) harus diatur secara hukum dan dipertimbangkan dari aspek etika, agar penggunaannya tidak merugikan masyarakat.

1.6.7. Teori *Causality* (Kausalitas)

Dalam menjatuhkan pertanggungjawaban pidana, diperlukan pembuktian hubungan sebab-akibat antara tindakan dan akibat yang ditimbulkan. Teori kausalitas, digunakan untuk menentukan apakah suatu perbuatan secara wajar dapat dipandang sebagai penyebab dari suatu akibat yang terjadi. Dalam konteks pengembang *Artifical Intelligence* (AI) penting untuk menelusuri apakah teknologi yang diciptakan secara langsung atau tidak langsung menjadi sebab dari kerugian yang timbul pada korban.

1.7 Metode Penelitian

1.7.1 Jenis Penelitian

Metode yang digunakan dalam penelitian ini adalah *normative* yaitu penelitian yang dilakukan dengan menelaah kaidah-kaidah atau norma-norma hukum yang berlaku. Penelitian ini berfokus pada analisis terhadap peraturan perundang-undangan, doktrin hukum, dan prinsip-prinsip hukum yang berkaitan dengan pertanggungjawaban pidana pengembang *Artificial Intelligence* (AI) dalam konteks kejahatan siber.

1.7.2 Pendekatan Penelitian

1.7.2.1 Peraturan Perundang-Undangan

Pendekatan Perundang-undangan adalah pendekatan dengan menggunakan legilasi dan regulasi, Suatu penelitian normatif menggunakan pendekatan perundang-undangan karena yang akan diteliti adalah berbagai aturan hukum yang menjadi fokus sekaligus tema sentral dari suatu penelitian.

1.7.2.2. Pendekatan Konsep

Pendekatan konsep merupakan Pendekatan penelitian yang menganalisis permasalahan hukum dari sudut pandang konsep-konsep hukum yang melatar belakanginya. Pendekatan ini dilakukan untuk memahami makna istilah-istilah hukum, dan menguji istilah hukum tersebut dalam teori dan praktik.

1.7.2.3. Pendekatan Komparatif

Untuk memperluas perspektif, penelitian ini juga membandingkan pengaturan hukum dan penerapan pertanggungjawaban pidana terhadap pengembang *Artificial Intelligence* (AI) di negara lain, seperti Uni Eropa (melalui GDPR dan EU *Artificial Intelligence* (AI) Act), yang telah memiliki regulasi lebih maju dalam bidang *Artificial Intelligence* (AI) dan *cybercrime*. Pendekatan ini bertujuan untuk memberikan masukan bagi pengembangan hukum nasional.

1.7.3 Sumber Hukum

1.7.3.1. Sumber Hukum Primer

Sumber hukum primer adalah hukum aktual dalam bentuk konstitusi, kasus pengadilan, undang-undang, dan peraturan serta ketentuan administratif.

1. Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik
2. Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik
2. Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas undang-undang nomor 11 tahun 20088 tentang informasi dan transaksi elektronik
3. Kitab undang-undang Hukum Pidana (KUHP)
4. Peraturan Pemerintah no. 71 tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik

1.7.3.2. Sumber Hukum Skunder

Sumber hukum sekunder adalah bahan hukum yang membantu memahami undang-undang serta memberikan penjelasan, menafsirkan, dan menganalisis sumber primer. seperti pendapat hukum (*doktrin*) ataupun teori-teori yang diperoleh dari literatur hukum, hasil penelitian, artikel ilmiah, maupun website yang terkait dalam penelitian ini.

bahan hukum sekunder dipergunakan untuk memberikan penjelasan terhadap bahan hukum primer.

1.7.3.3. Sumber Hukum Tersier

Sumber hukum tersier merupakan bahan hukum yang memberikan informasi dan penjelasan terkait bahan hukum primer dan sekunder. Contoh sumber hukum tersier adalah kamus, ensiklopedia, majalah, media massa, dan internet.

1.8 Sistematika Penulisan

Bab I

Berisikan gambaran umum tentang apa yang akan diteliti, pada bab ini ada beberapa sub bab yang pertama ada latar belakang masalah yang menggambarkan urgensi penelitian dan menjadi dasar perumusan masalah sehingga penulis dapat acuan dalam merumuskan rumusan masalah, yang kedua ada rumusan masalah yang dimana menjadi batas peniliti untuk membahas permasalahan yang akan diteliti, ada tujuan apa yang diharapkan oleh peniliti dalam penelitian dan mafaat penelitian selanjutnya ada orisinalitas penelitian yang dimana untuk mengetahui apakah hal yang diteliti oleh peneliti itu orisinil, lalu ada tinjauan pustaka yang berisikan teori teori landasan dalam penelitian, selanjutnya metode penelitian yang berisikan metode apa yang digunakan didalam penelitian sumber hukum apa saja yang dimuat didalam penelitian dan sistematika penulisan yang dimana berisi kerangka penelitian.

Bab II

Bab ini membahas dan menganalisis rumusan masalah pertama berdasarkan teori, peraturan, dan data yang relevan, hingga memperoleh jawaban.

Bab III

Berisikan pembahasan rumusan masalah kedua yang membahas berkaitan tentang permasalahan yang telah dirumuskan berdasarkan teori, peraturan, dan data yang relevan, hingga memperoleh jawaban.

Bab IV

Bab ini memuat kesimpulan dari hasil pembahasan rumusan masalah pertama dan kedua, serta memberikan saran sebagai rekomendasi untuk mengatasi permasalahan yang ditemukan dalam penelitian.

