KEBIJAKAN HUKUM PIDANA DALAM UPAYA MENANGGULANGI ARTIFICAL INTELLIGANCE (AI) DALAM CYBER CRIME

TESIS

Oleh:

YULIANA PUTRI DHARMAYANTI

NIM : 20302300559

Konsentrasi : Hukum Pidana

PROGRAM MAGISTER (S2) ILMU HUKUM
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG
2025

KEBIJAKAN HUKUM PIDANA DALAM UPAYA MENANGGULANGI ARTIFICAL INTELLIGANCE (AI) DALAM CYBER CRIME

TESIS

Diajukan untuk penyusunan Tesis
Program Studi Ilmu Hukum

Oleh:

YULIANA PUTRI DHARMAYANTI
NIM : 20302300559
Konsentrasi : Hukum Pidana

PROGRAM MAGISTER (S2) ILMU HUKUM
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG
2025

KEBIJAKAN HUKUM PIDANA DALAM UPAYA MENANGGULANGI ARTIFICAL INTELLIGANCE (AI) DALAM CYBER CRIME

Diajukan Untuk Penyusunan Tesis

Program Magister Hukum

Oleh:

Nama : **YULIANA PUTRI DHARMAYANTI**

NIM : 20302300559

Program Studi : Magister (S2) Ilmu Hukum (M.H.)

Disetujui oleh:

Pembimbing I

Tanggal,

Prof. Dr. Eko Soponyono, S.H., M.H.

NIDN. 88-8372-0016

Dekan

Fakultas Hukum

UNISSULA

Dr. Jawade Hafidz, S.H., M.H.

NIDN. 06-2004-6701

KEBIJAKAN HUKUM PIDANA DALAM UPAYA MENANGGULANGI ARTIFICAL INTELLIGANCE (AI) DALAM CYBER CRIME

Telah Dipertahankan di Depan Dewan Penguji
Pada Tanggal 31 Mei 2025
Dan dinyatakan **LULUS**

Tim Penguji
Ketua,
Tanggal,

Dr. Arpangi, S.H., M.H.
NIDN: 06-1106-6805

Anggota

Prof. Dr. Eko Soponyono, S.H., M.H.
NIDN. 88-8372-0016

Anggota,

Dr. Ratih Mega Puspasari, S.H., M.Kn.
NIDN. 06-2410-8504

Mengetahui

Dekan
Fakultas Hukum
UNISSULA

Dr. H. Jawade Hafidz, S.H., M.H.
NIDN: 06-2004-6701

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : YULIANA PUTRI DHARMAYANTI
NIM : 20302300559

Dengan ini saya nyatakan bahwa Karya Tulis Ilmiah yang berjudul:

KEBIJAKAN HUKUM PIDANA DALAM UPAYA MENANGGULANGI ARTIFICAL INTELLIGANCE (AI) DALAM CYBER CRIME

Adalah benar hasil karya saya dan penuh kesadaran bahwa saya tidak melakukan tindakan plagiasi atau mengambil alih seluruh atau sebagian besar karya tulis orang lain tanpa menyebutkan sumbernya. Jika saya terbukti melakukan tindakan plagiasi, saya bersedia menerima sanksi sesuai dengan aturan yang berlaku.

Semarang, 22 Mei 2025
Yang Membuat Pernyataan.

(YULIANA PUTRI DHARMAYANTI)

PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama	:	YULIANA PUTRI DHARMAYANTI
NIM	:	20302300559
Program Studi	:	Magister Ilmu Hukum
Fakultas	:	Hukum

Dengan ini menyerahkan karya ilmiah berupa ~~Tugas Akhir/Skripsi/~~Tesis~~/Disertasi~~* dengan judul:

KEBIJAKAN HUKUM PIDANA DALAM UPAYA MENANGGULANGI ARTIFICAL INTELLIGANCE (AI) DALAM CYBER CRIME

dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak Bebas Royalti Non-ekslusif untuk disimpan, dialihmediakan, dikelola dalam pangkalan data, dan dipublikasikannya di internet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak Universitas Islam Sultan Agung.

Semarang, 22 Mei 2025

Yang Membuat Pernyataan.

(YULIANA PUTRI DHARMAYANTI)

*Coret yang tidak perlu

KATA PENGANTAR

Assalamualaikum Wr,Wb.

Segala puji hanya milik Allah SWT, hanya kepada-Nya tempat makhluk bergantung, berlindung dan memohon pertolongan. Shalawat serta salam tetap tercurahkan kepada Nabi Muhammad SAW, yang telah diutus sebagai rahmat sekalian alam dan memberikan suri tauladan serta hidayatnya kepada kita dengan baik sepanjang jaman. Dengan mengucapkan puji syukur yang sedalamdalamnya kepada Allah SWT, atas segala limpah ramhat, nikmat serta hidayah yang diberikan-NYA, sehingga penulis dapat menyelesaikan tesis dengan judul: "KEBIJAKAN HUKUM PIDANA DALAM UPAYA MENANGGULANGI *ARTIFICAL INTELLIGANCE* (AI) DALAM *CYBER CRIME*" yang merupakan salah satu syarat untuk menyelesaikan Pendidikan jenjang program strata dua (S.2) Ilmu Hukum pada Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang.

Penulis menyadari sepenuhnya bahwa tesis ini sebagai sebuah karya manusia tentunya tidak terlepas dari kemungkinan kekhilafan, kekurangan dan ketidak sempurnaan dari uraian dalam skripsi ini dapat diperbaiki lagi. Penulis dalam menyusun skripsi ini membutuhkan banyak bantuan, dukungan masukan, dan bimbingan dari semua pihak. Oleh karena itu pada kesempatan ini penulis mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. H. Gunarto, SH, SE, Akt, M.Hum, selaku RektorUniversitas Islam Sultan Agung Semarang.
2. Bapak Dr.H. Jawade Hafidz, S.H., M.H. , selaku Dekan Fakultas Hukum Universitas Islam Sultan Agung Semarang.
3. Bapak Dr. Andri Winjaya Laksana, SH., MH. selaku Ketua Prodi Fakultas Hukum Universitas Islam Sultan Agung Semarang.
4. Bapak Dr. Arpangi, SH,. MH. selaku Sekretaris Prodi Fakultas Hukum Universitas Islam Sultan Agung Semarang.

5. Prof. Dr. Eko Soponyono, S.H., M.H. selaku Dosen Pembimbing yang telah banyak meluangkan waktu untuk membantu membimbing dan tak henti memberikan motivasi dalam penulisan tesis ini.
6. Terima kasih kepada diriku sendiri karena senantiasa semangat dan berjuang dalam penyusunan skripsi ini.
7. Terimakasih Kepada kedua orang tua saya dan keluarga besar saya yang senantiasa mendoakan dan memberikan support materi maupun moril
8. Terimakasih kepada pacar saya Rizky Ade Satriya yang senantiasa mau saya repotkan setiap saat dalam pengerjaan tesis ini
9. Terimakasih kepada anggota BTS yang tidak bisa penulis sebut satu satu yang telah memberikan motivasi dan semangat karena karya musik mereka yang indah.

Penulis berharap adanya saran dan kritik guna membangun perbaikan tesis, karena penulis menyadari bilamana pada tesis ini masih memiliki banyak sekali kekurangan baik dari segi isi maupun penulisan disebabkan keterbatasan ilmu dan pengetahuan penulis. Apabila terdapat kata-kata ataupun kalimat yang kurang berkenan mohon dimaafkan. Akhir kata, semoga tesis ini bisa memberikan manfaat khususnya untuk saya, pembaca serta agama, negara, dan masyarakat dalam memberikan sumbangan pengetahuan khususnya pada Ilmu Hukum Pidana. Aamiiin.

Wassalamualaikum Wr. Wb.

Semarang, 23 Mei 2025

Penulis

Yuliana Putri Dharmayanti

NIM : 20302300559

ABSTRAK

Perkembangan teknologi Artificial Intelligence (AI) telah memberikan pengaruh besar dalam berbagai bidang kehidupan, termasuk dalam aspek hukum pidana. AI tidak hanya dimanfaatkan untuk kepentingan positif, tetapi juga membuka peluang munculnya kejahatan siber baru seperti deepfake, phishing otomatis, dan pencurian identitas digital. Kejahatan ini menimbulkan tantangan baru dalam penegakan hukum, khususnya terkait pertanggungjawaban pidana dan kekosongan pengaturan hukum yang secara spesifik mengatur tindak pidana berbasis AI. Penelitian ini bertujuan untuk menganalisis kebijakan hukum pidana dalam menanggulangi cyber crime berbasis AI, baik dalam hukum positif yang berlaku saat ini maupun prospek pengaturannya di masa depan.

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan deskriptif-analitis. Data dikumpulkan melalui studi pustaka terhadap peraturan perundang-undangan seperti KUHP, UU ITE, serta literatur yang relevan. Hasil penelitian menunjukkan bahwa regulasi yang ada belum mengatur secara eksplisit penggunaan dan penyalahgunaan AI dalam tindak pidana siber. Ketentuan hukum yang berlaku masih bersifat umum dan belum mampu mengakomodasi kompleksitas kejahatan berbasis AI. Hal ini menunjukkan adanya kekosongan hukum yang harus segera diisi melalui pembaharuan kebijakan hukum pidana yang lebih adaptif dan progresif terhadap perkembangan teknologi informasi.

Berdasarkan hasil analisis, diperlukan reformulasi kebijakan hukum pidana yang mampu menjawab tantangan kejahatan siber berbasis AI melalui pendekatan teori negara hukum, teori pertanggungjawaban pidana, dan teori kebijakan kriminal. Penelitian ini memberikan kontribusi teoretis terhadap pengembangan ilmu hukum pidana di era digital, serta menjadi referensi praktis bagi pembuat kebijakan dalam merumuskan regulasi yang relevan dan efektif. Dengan demikian, diharapkan sistem hukum Indonesia dapat merespons perkembangan teknologi dengan menciptakan regulasi yang adil, jelas, dan mampu melindungi masyarakat dari kejahatan siber yang semakin kompleks.

Kata Kunci: Kebijakan Hukum Pidana, Artificial Intelligence, Cyber Crime, Pertanggungjawaban Pidana, Legal Vacuum

ABSTRACT

The development of Artificial Intelligence (AI) technology has significantly influenced various sectors of life, including criminal law. While AI offers many positive benefits, it also facilitates the emergence of new forms of cyber crime such as deepfakes, automated phishing, and digital identity theft. These crimes present legal challenges, particularly in terms of criminal liability and the absence of specific regulations governing AI-based offenses. This research aims to analyze criminal law policies in addressing AI-based cyber crime, both under the current positive law and in terms of future legal developments.

This study employs a normative juridical method with a descriptive-analytical approach. Data were collected through literature studies of statutory regulations, including the Indonesian Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and related legal literature. The findings indicate that existing regulations do not explicitly address the criminal use or misuse of AI. The current legal framework remains general and lacks the capacity to address the complexity of AI-based crimes. This condition reveals a legal vacuum that must be filled by reformulating criminal law policies to be more adaptive and responsive to technological developments.

Based on the analysis, the study recommends reformulating criminal law policies by incorporating the rule of law theory, criminal liability theory, and criminal policy theory. This research contributes theoretically to the development of criminal law in the digital era and serves as a practical reference for policymakers in formulating relevant and effective legal frameworks. Thus, it is expected that Indonesia's legal system will be better equipped to respond to technological advancements by establishing fair, clear, and protective regulations against increasingly complex cyber crimes.

Keywords: *Criminal Law Policy, Artificial Intelligence, Cyber Crime, Criminal Liability, Legal Vacuum*

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Di era industri 5.0 saat ini, kemajuan teknologi dimanfaatkan untuk mempermudah pemenuhan kebutuhan manusia dan meningkatkan efisiensi dalam aktivitas sehari-hari. Inovasi dalam teknologi informasi memberikan keuntungan signifikan bagi masyarakat, karena berbagai manfaat positif yang ditawarkannya, seperti peningkatan efisiensi dan produktivitas, serta percepatan komunikasi dan penyebaran informasi. Teknologi informasi dapat digunakan untuk mengumpulkan, mengolah, dan menganalisis data, sehingga menghasilkan informasi yang cepat dan akurat. Dampak dari perkembangan ini sangat besar bagi masyarakat, salah satunya adalah kemajuan bisnis yang semakin pesat. Inovasi berkelanjutan dalam teknologi informasi, seperti kecerdasan buatan (AI), membuka peluang menarik untuk menciptakan nilai bersama di antara pelaku ekonomi dalam dunia bisnis. [1]

Teknologi memiliki peran yang sangat penting dalam era globalisasi saat ini, di mana ia telah menjadi elemen yang tak terpisahkan dari kehidupan sehari-hari. Kemajuan teknologi telah mengubah struktur masyarakat dari yang bersifat lokal menjadi lebih global. Perubahan ini dipicu oleh kehadiran teknologi informasi. Integrasi antara teknologi informasi, media, dan komputer telah menghasilkan dampak signifikan dalam cara kita berinteraksi dan berkomunikasi. Dengan adanya kemajuan ini, akses terhadap informasi menjadi lebih cepat dan luas, sehingga mempercepat proses penyebaran pengetahuan dan budaya. Hal ini mendorong pembentukan jejaring sosial yang lebih luas dan memungkinkan kolaborasi lintas negara, yang pada gilirannya memperkuat keterhubungan antarindividu dan komunitas di seluruh dunia.

[1] Marsella, dkk, "Analisis Implementasi Artificial Intelligence Untuk Bisnis: Systematic Literature Review", *Jurnal Hukum Pidana*. Vol.4, No.2, hlm.134

Manusia dan kecerdasan buatan dapat berkolaborasi dalam pengambilan keputusan yang minim pengaruh dari nilai-nilai pribadi. Dalam membandingkan cara pemecahan masalah antara keduanya, dapat dilihat bahwa kecerdasan buatan lebih unggul dalam menangani masalah yang memiliki tingkat ketidakpastian dan kompleksitas rendah, serta memerlukan kemampuan analitis yang tinggi. Sebaliknya, manusia lebih mampu mengatasi masalah yang memiliki tingkat ketidakpastian dan kompleksitas lebih tinggi, dengan kebutuhan analitis yang relatif lebih rendah. Selain itu, diharapkan kecerdasan buatan dapat menangani tugas dan masalah yang melibatkan tingkat ketidakpastian yang lebih besar melalui penerapan proses pembelajaran yang lebih dalam (*deep learning*).[2]

Teknologi Kecerdasan Buatan (AI) pada dasarnya serupa dengan alat atau media lainnya, di mana ia memiliki potensi untuk memberikan manfaat maupun menimbulkan risiko. Contohnya, sebuah pisau yang digunakan oleh chef dapat menghasilkan masakan yang sangat enak namun jika sebuah pisau diberikan kepada orang yang ingin bertindak jahat maka akan mejadi sebuah senjata yang berbahaya. Begitu juga dengan teknologi AI, jika tidak diterapkan dengan bijaksana dan proporsional dalam konteks pembelajaran, dapat menimbulkan dampak negatif.

Kemajuan teknologi juga memberikan dampak negatif bagi perkembangan dan peradaban manusia. Peningkatan penggunaan teknologi informasi dan komunikasi, terutama melalui media sosial, telah memunculkan berbagai jenis kejahatan siber *(cyber crime).* Salah satu contohnya adalah kejahatan siber manipulasi, atau yang dikenal sebagai *deepfake*. Ini merupakan bentuk baru dari kejahatan di era modern yang muncul berkat kecanggihan teknologi yang bersifat universal di dunia maya, sehingga memberikan dampak negatif yang tidak tampak secara fisik tetapi sama merugikannya dengan tindak pidana lainnya. Dalam penegakan hukum terkait kejahatan dunia maya, pelaku yang melakukan pelanggaran

[2] Tri Wahyudi, "Studi Kasus Pengembangan dan Penggunaan Artificial Intelligence (AI) Sebagai Penunjang Kegiatan Masyarakat Indonesia", *Jurnal Hukum Pidana.* Vol.9, No.1, hlm.29

hukum harus bertanggung jawab atas kerugian yang ditimbulkan, baik karena kelalaian maupun kesengajaan. Oleh karena itu, penerapan hak dan kewajiban hukum perlu menekankan pentingnya penegakan pertanggungjawaban hukum.

Dengan demikian, penting bagi sistem hukum untuk mengembangkan mekanisme yang efektif dalam menangani kejahatan siber, termasuk menetapkan sanksi yang sesuai dan prosedur penegakan hukum yang jelas. Pendidikan dan kesadaran masyarakat tentang risiko kejahatan siber juga harus ditingkatkan, agar individu lebih berhati-hati dalam menggunakan teknologi. Selain itu, kolaborasi antara pemerintah, penyedia layanan teknologi, dan masyarakat diperlukan untuk menciptakan lingkungan digital yang lebih aman. Upaya ini tidak hanya akan melindungi individu dari kejahatan siber, tetapi juga akan mendukung perkembangan teknologi yang lebih bertanggung jawab dan etis dalam masyarakat.

Dalam penegakan hukum terhadap kejahatan dunia maya, pelaku yang melakukan tindakan melanggar hukum harus mempertanggungjawabkan kerugian yang diakibatkan, baik karena kelalaian maupun kesengajaan. Penerapan hak dan kewajiban hukum harus menekankan pentingnya penegakan melalui mekanisme pertanggungjawaban hukum.[3]

Pertanggungjawaban hukum ini berfungsi untuk memastikan bahwa pelaku kejahatan menerima sanksi yang sesuai, sehingga dapat memberikan efek jera dan mencegah terulangnya tindakan serupa. Selain itu, penegakan hukum yang efektif juga harus melibatkan kerjasama antara berbagai pihak, termasuk lembaga penegak hukum, penyedia layanan teknologi, dan masyarakat umum. Hal ini bertujuan untuk menciptakan lingkungan yang aman di dunia maya, serta meningkatkan kesadaran akan risiko dan konsekuensi dari kejahatan siber. Melalui pendekatan ini, diharapkan dapat

[3] Izil Hidayat Putra, "Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan Perundang-Undangan", vol.1, no.2, hlm.112

tercipta sistem hukum yang responsif dan adaptif terhadap perkembangan teknologi informasi. Selain itu, penting juga untuk meningkatkan kesadaran masyarakat mengenai risiko kejahatan dunia maya dan pentingnya menjaga keamanan informasi pribadi. Edukasi dan pelatihan tentang keamanan siber harus menjadi bagian integral dari upaya pencegahan dan penanggulangan kejahatan siber.

Dikarenakan perkembangan *artificial intelligence*, dewasa ini telah merambah ke berbagai perangkat yang digunakan dalam hampir semua sektor kehidupan, mulai dari keuangan dan bisnis, teknik, gawai, penerbangan, transportasi, dan lain sebagainya. Akses kecerdasan buatan yang semakin mudah dan umum digunakan saat ini mulai digunakan dengan tujuan kejahatan. Beberapa bentuk kejahatan siber berbasis *Artificial Intelligence* yang marak terjadi saat ini antara lain seperti *Deep Fake Fraud* yaitu penggunaan algoritma *Artificial Intelligence* untuk membuat video palsu yang menyerupai seseorang, *Artificial Intelligence - Generated Phising Emails* (pembuatan *phising* melalui email dengan tingkat personalisasi yang sangat tinggi), dan *Identify Theft* (pencurian data pribadi dari media sosial untuk membuat identitas palsu menggunakan *Artificial Intelligence*).[4]

Dalam membahas cyber crime dari perspektif hukum pidana, saya akan mengkaitkannya dengan beberapa delik yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Beberapa contoh tindak pidana cyber crime yang dapat dikaitkan dengan ketentuan KUHP antara lain: Pencurian sebagaimana diatur dalam Pasal 362 KUHP, Penipuan sebagaimana diatur dalam Pasal 378 KUHP, dan Pemerasan serta pengancaman sebagaimana diatur dalam Pasal 335 KUHP.

Berdasarkan penelitian penulis, tindak pidana yang berkaitan dengan *Malware-AI* [5] belum diatur secara spesifik dalam undang-undang di

---

[4] Smith, J. "AI and Fraud: The Rise of Deepfake Scams". *Cybersecurity Review.* Vol. 15, No. 3, hlm. 45-50.

[5] Malware-AI merupakan jenis perangkat lunak berbahaya yang memanfaatkan kecerdasan buatan *(artificial intelligence)* untuk menyerang sistem komputer.

Indonesia. Meskipun demikian, terdapat sejumlah ketentuan pidana di luar UU ITE yang dapat digunakan untuk menjerat pelanggaran tersebut, mengingat UU ITE adalah regulasi terbaru dan paling relevan dalam menangani kejahatan siber. Beberapa pasal dalam KUHP, seperti pasal 335, 362, 378, dan 406, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 mengenai Perlindungan Data Pribadi dalam Sistem Elektronik, juga dapat dipertimbangkan dalam konteks ini. [6]

Artificial Intelegance (AI) digunakan dalam sistem pelayanan publik, pengambilan keputusan otomatis, hingga pembuatan konten digital yang kompleks. Namun, bersamaan dengan itu, muncul pula tantangan baru dalam bentuk potensi pelanggaran hukum, ketidakjelasan pertanggungjawaban pidana, serta kemungkinan penyalahgunaan oleh individu maupun korporasi. Dalam konteks ini, UU ITE telah mengalami perubahan melalui UU No. 1 Tahun 2024 atas UU No 11 Tahun 2008, yang bertujuan untuk menjaga ruang digital Indonesia yang bersih, sehat, beretika, produktif, dan berkeadilan. Namun, meskipun UU ITE mengatur berbagai aspek tindak pidana di ranah digital, ketentuan mengenai penggunaan teknologi berbasis AI secara spesifik masih sangat terbatas. Hal ini menciptakan kekosongan hukum (legal vacuum) dalam menanggulangi kejahatan yang berbasis AI secara langsung.[7]

Dengan demikian diperlukan landasan teoritis yang mendalam antara lain:

a. Teori Kebijakan Kriminal (*Criminal Policy*):

   Teori ini menekankan pentingnya pendekatan hukum pidana yang strategis untuk mencegah dan menanggulangi tindak pidana. Dalam konteks AI, teori ini mendorong perumusan kebijakan hukum pidana yang bersifat antisipatif terhadap perkembangan teknologi.

b. Teori Pertanggungjawaban Pidana:

---

[6] Supanto, dkk "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016", vol.9, no.2, hlm.132

[7] UU ITE No 1 Tahun 2024

Teori ini menjadi sentral dalam diskusi mengenai siapa yang seharusnya dimintai pertanggungjawaban dalam konteks penggunaan AI. Dalam sistem hukum pidana klasik, subjek hukum adalah manusia atau badan hukum yang memiliki kesadaran dan kehendak. Namun, kehadiran AI sebagai entitas semi-otonom menantang konsep tradisional ini.

c. Pendekatan Hukum Progresif:

Pendekatan ini menekankan bahwa hukum harus mampu beradaptasi dengan perkembangan zaman dan menjawab kebutuhan masyarakat yang terus berubah akibat kemajuan teknologi. Dalam konteks ini, hukum pidana harus mampu beradaptasi dengan perkembangan teknologi dan menjawab kebutuhan masyarakat yang terus berubah akibat kemajuan teknologi.

Dalam hal ini telah diatur juga dalam UU ITE No 1 Tahun 2024 atas perubahan UU ITE No 11 Tahun 2008 seperti pada Pasal 13A tentang Identitas Digital: Pasal ini mengatur tentang identitas digital yang digunakan dalam penyelenggaraan sertifikasi elektronik. Identitas digital adalah data elektronik yang dapat digunakan untuk mengenali seseorang secara elektronik. Penerapan pasal ini diharapkan dapat meningkatkan keamanan dan keandalan sertifikasi elektronik, karena identitas digital dapat digunakan untuk memastikan bahwa orang yang mengajukan permohonan sertifikasi elektronik adalah orang yang sebenarnya. Ini artinya identitas digital juga dapat digunakan untuk mencegah penipuan dan penyalahgunaan identitas. Pasal 16A, Pasal 27A, dan Pasal 40A.

Dengan demikian, meskipun UU ITE menjadi acuan utama dalam penanganan tindak pidana siber, ketentuan yang terdapat dalam KUHP dan peraturan lainnya masih memiliki relevansi yang signifikan. Hal ini menunjukkan bahwa untuk mengatasi isu-isu yang muncul akibat

perkembangan teknologi, khususnya dalam konteks *Malware-AI*, diperlukan pendekatan hukum yang komprehensif.[8]

Penelitian ini juga menyoroti bahwa regulasi dalam Undang-Undang Nomor 1 Tahun 2024 dirancang untuk menghadapi kompleksitas dan dinamika kejahatan siber yang terus berkembang. Selain itu, perlindungan terhadap sektor keuangan dan perbankan juga diperkuat melalui sanksi yang signifikan. Analisis yuridis menunjukkan bahwa undang-undang ini memberikan landasan hukum yang lebih jelas untuk menangani kejahatan siber yang memiliki sifat lintas batas dan berkembang pesat. Ini artinya bahwa Undang-Undang Nomor 1 Tahun 2024 yang direncanakan akan segera berlaku telah memberikan kerangka hukum yang lebih komprehensif dalam melindungi masyarakat dari kejahatan siber. Dengan revisi dan reformasi hukum yang berkelanjutan, regulasi ini diharapkan mampu mengikuti perkembangan teknologi dan modus kejahatan modern, sehingga menciptakan lingkungan digital yang lebih aman di Indonesia.

Selain itu, adanya kekosongan hukum secara spesifik mengenai *Malware-AI* mengindikasikan perlunya upaya lebih lanjut dalam pembaruan regulasi yang dapat mengakomodasi perkembangan teknologi dan kejahatan yang menyertainya. Dengan memahami kerangka hukum yang ada, kita dapat merumuskan langkah-langkah yang lebih efektif untuk melindungi masyarakat dari ancaman yang ditimbulkan oleh kejahatan siber. Penelitian ini diharapkan dapat memberikan kontribusi dalam diskusi mengenai perlunya revisi atau penambahan ketentuan hukum yang lebih sesuai dengan tantangan saat ini.

B. Rumusan Masalah

[8] Supanto, dkk, *Ibid* hlm.133

Berdasarkan latar belakang masalah diatas, maka peneliti merumuskan masalah sebagai berikut:

1. Bagaimana Kebijakan Hukum Pidana dalam upaya menanggulangi AI *(Artificial Intelegence) Cyber Crime* dalam Hukum Positif Saat Ini?
2. Bagaimana Kebijakan Hukum Pidana dalam upaya menanggulagi AI *(Artificial Intelegence) Cyber Crime* dalam Hukum Positif Yang Akan Datang?

C. Tujuan dan Manfaat Penelitian

1. Tujuan Penelitian

Penulisan Tesis dengan judul "Kebijakan Hukum Pidana Dalam Upaya Menanggulangi *Artifical Intelligance* (AI) Dalam *Cyber Crime*" mempunyai tujuan sebagai berikut:

a. Menganalisis dan mengevaluasi kebijakan hukum pidana yang saat ini diterapkan dalam menanggulangi kejahatan siber yang melibatkan AI, serta mengidentifikasi kelebihan dan kekurangan dari kebijakan tersebut dalam konteks hukum positif yang berlaku.
b. Mengembangkan rekomendasi kebijakan hukum pidana yang efektif untuk menanggulangi kejahatan siber yang dihasilkan oleh AI di masa depan, dengan mempertimbangkan perkembangan teknologi, dinamika kejahatan, dan kebutuhan untuk melindungi hak asasi manusia serta keadilan sosial.
c. Memberikan kontribusi terhadap pemahaman mengenai hubungan antara kebijakan hukum pidana dan teknologi AI dalam konteks kejahatan siber, serta menciptakan kerangka kerja yang dapat membantu pembuat kebijakan dalam merumuskan kebijakan yang lebih responsif dan adaptif terhadap tantangan yang muncul.

2. Manfaat Penelitian

a. Secara Teoritis Kontribusi pada pengembangan teori hukum pidana dengan memasukkan analisis tentang kejahatan siber yang melibatkan AI, memperkaya pemahaman akademik tentang hubungan antara hukum dan teknologi. Memperkaya literatur yang ada tentang hukum pidana dan kejahatan siber dengan perspektif baru mengenai AI, yang masih jarang dibahas.

b. Secara Praktis memberikan manfaat praktis yang dapat diperoleh antara lain:

1. Bagi Aparat Penegak Hukum:

   Penelitian ini dapat menjadi rujukan dalam memahami jenis-jenis kejahatan siber berbasis AI serta memperjelas kerangka pertanggungjawaban pidana terhadap pelaku, termasuk jika pelaku menggunakan teknologi AI sebagai alat kejahatan. Dengan demikian, aparat penegak hukum memiliki dasar yang lebih kuat dalam menegakkan hukum secara tepat dan proporsional.

2. Bagi Masyarakat Umum:

   Memberikan pemahaman kepada masyarakat mengenai risiko penggunaan AI yang tidak terkendali dan pentingnya dukungan terhadap kebijakan hukum yang dapat melindungi hak dan data pribadi dari potensi kejahatan digital.

3. Bagi Penulis:

   Penelitian ini memberikan kesempatan bagi penulis untuk memperdalam pemahaman terkait perkembangan kejahatan siber yang melibatkan teknologi Artificial Intelligence, serta memperluas wawasan dalam bidang hukum pidana kontemporer. Selain itu, penelitian ini juga menjadi sarana untuk mengembangkan kemampuan analisis terhadap kebijakan hukum pidana dalam konteks dinamika teknologi informasi, sehingga

dapat menjadi landasan dalam menghasilkan karya ilmiah yang relevan dan aplikatif terhadap kebutuhan hukum di era digital.

D. Ruang Lingkup

Ruang lingkup penelitian ini dibatasi pada implementasi bantuan hukum pada tahap penyidikan terhadap penyalahgunaan AI dalam *Cyber Crime* yang disangkakan melakukan tindak pindana penyalahgunaan AI dalam *Cyber Crime.*

E. Kerangka Konseptual

Penulisan tesis adalah tulisan ilmiah yang memiliki konsep penulisan, karena konsep adalah istilah, terdiri dari satu kata atau lebih yang menggambarkan suatu gejala atau menyatakan suatu ide (gagasan) tertentu. Kerangka konsep adalah kerangka yang menggambarkan hubungan antara konsep-konsep khusus yang diteliti. Konsep merupakan salah satu unsur konkrit dari teori. Namun masih diperlukan penjabaran lebih lanjut dari konsep ini dengan jalan memberikan definisi operasionalnya. Untuk selanjutnya peneliti memberikan definisi operasional dari beberapa variabel yang terkandung dalam judul tesis penelitian ini yang dimaksud dengan Kebijakan Hukum Pidana Dalam Upaya Menanggulangi *Artificial Intelegance* (AI) dalam *Cyber Crime.*

1. Kebijakan

Kebijakan merupakan serangkaian konsep dan prinsip yang berfungsi sebagai panduan dan dasar dalam merencanakan pelaksanaan suatu pekerjaan, kepemimpinan, serta tindakan. Istilah ini dapat diterapkan pada pemerintahan, organisasi, kelompok sektor swasta, maupun individu. Berbeda dengan peraturan dan hukum, kebijakan tidak bersifat memaksa atau melarang perilaku tertentu, misalnya hukum yang mewajibkan pembayaran pajak penghasilan. Sebaliknya,

kebijakan berperan sebagai pedoman untuk mencapai hasil yang diinginkan.[9]

Pengertian Kebijakan Pemerintah (Kebijakan Publik) dapat diartikan sebagai respon terhadap suatu permasalahan. Kebijakan ini bertujuan untuk memecahkan, mengurangi, dan mencegah dampak negatif, serta berfungsi sebagai pendorong inovasi dan inisiatif yang mengarah pada perbaikan. Kebijakan ini dilaksanakan dengan cara yang paling efektif dan terarah.

Menurut Thomas R. Dye Kebijakan publik, adalah apapun juga yang dipilih pemerintah, apakah mengerjakan sesuatu itu atau tidak mengerjakan (mendiamkan) sesuatu itu (Dye, 1995:1). Menurut Heinz Eulaudan Kenneth Prewitt, Kebijakan publik adalah keputusan tetap yang dicirikan dengan konsistensi dan pengulangan (repetisi) tingkah laku dari mereka yang membuat dan dari mereka yang mematuhi keputusan tersebut (Prewitt, 1973:265). [10]

Menurut James Anderson, Kebijakan publik adalah serangkaian kegiatan yang mempunyai maksud dan tujuan tertentu yang diikuti dan dilaksanakan oleh seorang aktor atau sekelompok aktor yang berhubungan dengan suatu permasalahan atau suatu hal yang diperhatikan (Anderson, 1984:3). Selanjutnya, Menurut Carl Frederick, kebijaksanaan pemerintah ini adalah suatu usulan tindakan oleh seseorang, keluarga, atau pemerintah pada suatu lingkungan politik tertentu, mengenai hambatan dan peluang yang dapat dibatasi, dimanfaatkan oleh suatu kebijaksanaan, dalam mencapai suatu tujuan atau merealisasikan suatu maksud (Friedrich, 1969:79).[11]

---

[9] https://elearning.menlhk.go.id/pluginfile.php/845/mod_resource/content/1/pengertian_kebijakan.html pada tanggal 21 Oktober 2024

[10] Bibit Santoso, "*Menata Kebijakan Publik Yang Tepat Agar Tidak Terjadi Gejolak Di Masyarakat Bila Diundangkan*" vol.13, no.1, hlm.39.

[11] Bibit Santoso, Ibid, hlm.40

2. Kebijakan Kriminal

Kebijakan sebagai panduan selalu terkait dengan pengelolaan publik *(public policy).* Menurut Carl J. Frederick, kebijakan publik merupakan serangkaian tindakan yang diusulkan oleh individu, kelompok, atau pemerintah dalam konteks tertentu, dengan mempertimbangkan hambatan-hambatan atau peluang yang ada dalam pelaksanaan usulan kebijakan tersebut untuk mencapai tujuan tertentu. Salah satu aspek yang muncul dari kebijakan perlindungan masyarakat *(social defense policy)* adalah kebijakan yang berkaitan dengan penanggulangan tindak pidana, yang dikenal sebagai kebijakan kriminal. Kebijakan ini menggunakan sarana penal dan disebut sebagai kebijakan hukum pidana atau politik hukum pidana.

Menurut Barda Nawawi Arief, dalam konteks kebijakan hukum pidana, sasaran atau subjek hukum pidana tidak hanya mencakup pengaturan perilaku masyarakat secara umum, tetapi juga meliputi pengaturan tindakan (dalam arti "kewenangan/kekuasaan") dari penguasa atau aparat penegak hukum. Peters juga menyatakan bahwa "pembatasan dan pengawasan atas kekuasaan negara merupakan dimensi yuridis yang sebenarnya dari hukum pidana, tugas yuridis hukum pidana bukanlah untuk mengatur masyarakat, melainkan untuk mengatur penguasa." Selanjutnya, M. Cherif Bassiouni menjelaskan aspek-aspek kebijakan tersebut dengan menyebutnya sebagai "proses legislasi, proses peradilan, dan proses administrasi," yang mencakup tahap formulasi, aplikasi, dan eksekusi.

3. Hukum Pidana

Tindak pidana merupakan tindakan yang dilarang oleh suatu ketentuan hukum, yang disertai dengan ancaman sanksi pidana bagi siapa pun yang melanggar larangan tersebut. Hukum pidana adalah cabang hukum yang mengatur perbuatan-perbuatan yang dilarang dan

diancam dengan pidana oleh negara karena melanggar kepentingan hukum yang dilindungi.

Menurut Moeljatno, hukum pidana adalah bagian dari keseluruhan hukum yang berlaku di suatu negara dan mengatur pelanggaran serta kejahatan yang diancam dengan pidana sebagai sanksi bagi pelanggarnya. [12] Fungsi utama hukum pidana adalah memberikan perlindungan kepada kepentingan umum (kepentingan hukum masyarakat) dari tindakan yang merugikan.

Hukum pidana mencakup dua aspek utama, yaitu hukum pidana material dan hukum pidana formal. Hukum pidana material *(substantive criminal law)* mengatur ketentuan mengenai tindak pidana (delik), jenis pidana, dan pertanggungjawaban pelaku. Sementara itu, hukum pidana formal *(procedural criminal law)* mengatur mekanisme penegakan hukum pidana, mulai dari proses penyidikan, penuntutan, hingga pelaksanaan pidana.

Seseorang dianggap melakukan tindak pidana jika perbuatannya telah diatur dalam undang-undang, sesuai dengan Asas Legalitas yang tertuang dalam Pasal 1 ayat (1) KUHP. Pasal tersebut menyatakan bahwa tidak ada satu pun perbuatan yang dapat dipidana kecuali berdasarkan ketentuan hukum pidana yang sudah ada sebelum perbuatan itu dilakukan.[13]

Dalam konteks *cyber crime*, hukum pidana menghadapi tantangan baru akibat perkembangan teknologi, khususnya *artificial intelligence* (AI). Kejahatan siber sering kali melibatkan dimensi transnasional, kerumitan teknologi, serta sulitnya menentukan subjek hukum, terutama jika AI digunakan sebagai alat atau bahkan aktor dalam tindak pidana. Hal ini memerlukan kebijakan hukum pidana yang adaptif dan futuristik untuk mengatasi isu pertanggungjawaban,

[12] Moeljatno. Asas-asas Hukum Pidana. Jakarta: PT Rineka Cipta, 2002, hlm. 1.

[13] Diakses melalui https://e-journal.uajy.ac.id/16530/3/HK114662.pdf pada tanggal 21 Oktober 2023

pengumpulan alat bukti digital, dan pembuktian dalam tindak pidana yang melibatkan AI.[14]

Oleh karena itu, pengembangan hukum pidana dalam menanggulangi *cyber crime* berbasis AI harus mempertimbangkan asas legalitas, keadilan, dan perlindungan hak asasi manusia, serta menyelaraskan pendekatan regulasi dengan kerangka internasional. Pendekatan ini diperlukan untuk memastikan efektivitas hukum pidana dalam menghadapi tantangan dunia digital.

4. Artifical Intelligance (AI)

Artificial Intelligence (AI) adalah suatu teknologi yang dapat difungsikan oleh manusia sebagai alat pembantu untuk menunjang kegiatan-kegiatan yang dilakukan oleh manusia itu sendiri. Secara fungsional, *Artificial Intelligence* memiliki fungsi yang kurang lebih sama dengan robot, namun, *Artificial Intelligence* hadir dalam tampilan yang berbeda yang berupa sistem komputer yang ditampilkan dalam bentuk visual.[15]

Dapat dikatakan bahwa *Artificial Intelligence* merupakan otak dari sebuah robot. *Artificial Intelligence* (AI) adalah sebuah bidang multidisiplin yang bertujuan untuk mengotomatisasi kegiatan yang saat ini memerlukan kecerdasan manusia. Dalam konteks ini, manusia dan kecerdasan buatan dapat bekerja sama untuk membuat keputusan yang minim dipengaruhi oleh nilai-nilai pribadi. Salah satu keberhasilan terbaru dalam AI adalah pengembangan sistem yang secara otomatis menyesuaikan perangkat keras sesuai dengan kebutuhan pengguna tertentu.

---

[14] Sutan Remy Sjahdeini. Kejahatan Siber: Cybercrime. Jakarta: Pustaka Utama Grafiti, 2003, hlm. 12-15.

[15] Ahmad Sudi Pratikno, "Implementasi Artificial Intelligence Dalam Memetakan Karakteristik, Kompetensi, dan Perkembangan Psikologi Siswa Sekolah Dasar Melalui Platform Offline", terdapat dalam https://scholar.google.co.id/citations?view_op=view_citation&hl=id&user=-FbwaL4AAAAJ&citation_for_view=-FbwaL4AAAAJ:d1gkVwhDpl0C. Diaksesn15 November 2024.

AI sebagai subbidang ilmu komputer bertujuan untuk menciptakan kecerdasan buatan yang meniru pola pikir dan perilaku manusia. Dalam pendidikan, AI dapat berperan dalam membentuk moral dan karakter siswa, meningkatkan kemampuan mental mereka, serta memberikan wawasan baru. Selain itu, AI juga dapat diterapkan dalam berbagai bidang seperti kesehatan, ekonomi, dan pertanian *(smart garden)*.[16]

Indonesia merupakan salah satu negara pengguna *Artificial Intelligence* terbesar di dunia. Dikutip dari liputan6.com, Indonesia merupakan salah satu negara yang memiliki kontribusi yang sangat besar dalam penggunaan AI dalam berbagai bidang kehidupan. Hal ini dibuktikan dengan telah dimanfaatkannya AI oleh 22,1 persen pekerja di berbagai sektor.[17] Di balik manfaat kecerdasan buatan bagi manusia, namun timbul kekhawatiran akan timbulnya risiko penyalahgunaa.

Peningkatan angka penggunaan *Artificial Intellegence* di Indonesia pada saat ini tidak diimbangi dengan kehadiran regulasi hukum yang secara khusus mengatur mengenai *Artificial Intellegence* dalam konteks hukum pidana. Perkembangan yang ada pada pemanfaatan kecerdasan buatan tentunya dapat menciptakan jenis kejahatan baru dan berbagai macam modus kejahatan yang dilakukan dengan memanfaatkan AI sebagai media dalam berbuat kejahatan.

5. Cyber Crime

Dalam beberapa literatur, cybercrime umumnya dianggap sebagai *computer crime*. The U.S. Department of Justice mendefinisikan kejahatan komputer sebagai: *"...any illegal act requiring knowledge of computer technology for its perpe-tration, investigation, or*

---

[16] Diakses melalui https://ejournal.bsi.ac.id/ejurnal/index.php/ijse/article/view/15631 pada 21 Oktober 2024

[17] Giovani Dio Prasasti, "Wamenkominfo: 22,1 Persen Pekerja di Indonesia Sudah Mulai Menggunakan AI",
terdapat dalam https://www.liputan6.com/tekno/read/5467690/wamenkominfo-221-persen-pekerja-diindonesia-sudah-mulai-pakai-ai?page=2 . Diakses pada tanggan 15 November 2024.

prosecution". *Organization of European Community Development* membagikan definisi lain, yaitu: *"any illegal, un-ethical or unauthorized behavior relating to the automatic processing and/or the transmission of data"*. Hamzah mendefinisikan sebagai "kejahatan di bidang PC *(personal computer)* secara universal bisa dimaksud bagaikan pemakaian PC secara ilegal".

Dari penafsiran di atas, Wisnubroto mengartikan kejahatan PC bagaikan perbuatan melawan hukum yang dicoba dengan memakai pc bagaikan fasilitas/ perlengkapan PC bagaikan objek, baik buat memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[18] *Cyber crime* atau kejahatan siber merujuk pada tindakan kriminal yang memanfaatkan teknologi komputer dan jaringan internet untuk melakukan berbagai aktivitas seperti peretasan, pencurian, penipuan, penyebaran virus, serta tindakan kriminal digital lainnya.[19]

Cyber crime atau kejahatan dunia maya adalah tindakan melawan hukum yang dilakukan melalui atau terhadap sistem teknologi informasi, yang biasanya melibatkan penggunaan komputer, jaringan internet, atau perangkat digital lainnya. Menurut definisi umum, *cyber crime* mencakup berbagai aktivitas ilegal, seperti pencurian data, penipuan daring, serangan siber *(cyber attack)*, dan pelanggaran hak cipta.[20]

Dalam konteks konseptual, kejahatan siber dapat diklasifikasikan menjadi dua kategori utama:[21]

1. *Cyber-dependent crimes*, yaitu kejahatan yang hanya bisa terjadi melalui teknologi digital, seperti peretasan, pencurian identitas daring, atau *ransomware* (virus komputer).

[18] Miftakhur Rokhman Habibi, Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangan dalam Sistem Hukum Indonesia". *Jurnal Al-Qanun: Pemikiran dan Pembaharuan Hukum Islam.* Vol. 23, No.2. Desember 2020. Hlm. 407.

[19] Diakses melaui https://www.linknet.id/article/cyber-crime pada 21 Oktober 2024

[20] Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

[21] Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

2. *Cyber-enabled crimes*, yakni kejahatan tradisional yang diperluas cakupannya melalui teknologi, seperti perdagangan manusia, terorisme, atau penipuan online.

Karakteristik utama *cyber crime* adalah anonimitas pelaku, ruang lingkup internasional, serta kerentanan teknologi yang terus berkembang. Hal ini menciptakan tantangan dalam aspek penegakan hukum, termasuk kesulitan melacak pelaku, keterbatasan yurisdiksi lintas negara, dan kecepatan evolusi teknologi.

Fenomena kejahatan siber melalui ruang-ruang digital menjadi fenomena lama yang perkembangan jenis kejahatannya terus berkembang mengikuti perkembangan teknologi. Berdasarkan *Strain Theory*, kejahatan siber dapat muncul karena adanya tekanan sosial, seperti kesenjangan ekonomi. Pelaku kejahatan siber biasanya akan melakukan kejahatannya ketika muncul peluang keuntungan secara finansial yang risiko hukumannya rendah.

Dengan kemunculan *artificial intelligence* (AI), ancaman kejahatan siber semakin kompleks. AI dapat digunakan untuk mengotomasi serangan siber, seperti *phishing* berbasis AI, serangan *Distributed Denial of Service* (DDoS), atau manipulasi data. Di sisi lain, AI juga memberikan peluang dalam mendeteksi dan mencegah serangan melalui analitik prediktif dan penguatan sistem keamanan.[22]

Kerangka hukum pidana dalam menghadapi *cyber crime* harus mencakup pengaturan teknologi berbasis AI, kolaborasi internasional, serta penguatan kapasitas penegak hukum untuk memahami dan mengatasi kejahatan ini. Kerangka konseptual ini bertujuan untuk memberikan landasan teoritis yang komprehensif dalam analisis kebijakan hukum pidana terhadap kejahatan siber berbasis AI.

[22] Kaplan, A. M., & Haenlein, M. (2019). Siri, Siri in my hand, who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62*(1), 15-25. https://doi.org/10.1016/j.bushor.2018.08.004

F. Kerangka Teoritis

Teori adalah seperangkat konstruk (konsep), defenisi dan proposisi yang berfungsi untuk melihat fenomena secara sistematik, melalui spesifikasi hubungan antar variabel sehingga dapat berguna untuk menjelaskan dan meramalkan fenomena. Teori adalah aluil logika atau penalaran, yang merupakan seperangkat konsep, defenisi, dan proposisi yang disusun secara sistematis. Fungsi teori secara umum mengandung fungsi menjelaskan *(explanation),* meramalkan *(prediction)* digunakan harus sudah jelas karena fungsi teori dalam sebuah penelitian adalah sebagai berikut

1. Untuk memperjelas dan mempertajam ruang lingkup atau konstruksi variable yang akan di telitib.
2. Untuk merumuskan hipotesis dan menyusun instrumen penelitian
3. Memprediksi dan menemukan fakta tentang sesuatu hal yang diteliti.

Kerangka teori untuk menganalisis secara yuridis mengenai Kebijakan Hukum Pidana Dalam Upaya Menanggulangi *Artificial Intelegence* (AI) dalam *Cyber Crime* dengan menggunakan:

1. Teori Negara Hukum

Penelitian ini memilih Teori Negara Hukum sebagai *Grand Theory* dengan alasan bahwa Indonesia adalah Negara Hukum *(rechtsstaat),* sesuai dengan ketentuan Pasal 1 ayat (3) UUD 1945 amandemen ketiga. Selain itu, teori ini menekankan pentingnya kepastian hukum *(rechtszekerheid)* serta perlindungan hak asasi manusia *(human rights).*

Secara teoretis, konsepsi negara hukum yang dianut oleh Indonesia tidak hanya dilihat dari dimensi formal, tetapi juga dalam arti material. Dalam hal ini, istilah yang umum digunakan adalah Negara Kesejahteraan *(welfare state)* atau Negara Kemakmuran. Oleh karena itu, tujuan yang ingin dicapai oleh Negara Indonesia adalah mewujudkan masyarakat yang adil dan makmur, baik secara spiritual

maupun material, berdasarkan Pancasila. Dengan demikian, negara ini juga disebut sebagai negara hukum yang memiliki karakteristik mandiri, yaitu Negara Hukum yang berlandaskan Pancasila.

Pada dasarnya, konsep Negara Hukum merupakan bagian integral dari doktrin *Rule of Law*, di mana dapat disimpulkan bahwa semua tindakan, termasuk yang dilakukan oleh pemerintah, harus berdasarkan hukum dan menjamin hak-hak asasi manusia. Hal ini mencakup prinsip Praduga Tidak Bersalah *(presumption of innocence)* dan Asas Legalitas *(principle of legality)*. Kedua asas ini merupakan bagian dari Hukum Pidana Formil dan Hukum Pidana Materiil, yang berfungsi sebagai sub-sistem dalam sistem hukum pidana. Marc Ancel menyatakan bahwa sistem hukum pidana pada abad XX masih perlu diciptakan. Sistem tersebut hanya dapat dibangun dan disempurnakan melalui usaha bersama dari semua individu yang beritikad baik, serta kontribusi dari para ahli di bidang ilmu sosial.

Sistem Hukum Pidana memiliki empat elemen substantif yang menjadi dasarnya, yaitu nilai-nilai yang mendasari sistem hukum (filosofis), adanya asas-asas hukum *(legal principles)*, norma atau peraturan perundang-undangan *(legal rules)*, serta masyarakat hukum yang mendukung sistem tersebut *(legal society)*. Keempat elemen ini terstruktur dalam sebuah rangkaian yang membentuk piramida, di mana bagian atas terdiri dari nilai-nilai, diikuti oleh asas-asas hukum dan peraturan perundang-undangan di tengah, dan di bagian bawah terdapat masyarakat.

2. Teori Pertanggung Jawaban Pidana

Teori pertanggungjawaban pidana adalah konsep fundamental dalam hukum pidana yang menjelaskan syarat-syarat agar seseorang

dapat dimintai pertanggungjawaban atas perbuatannya yang melanggar hukum. Teori ini berfungsi sebagai dasar untuk menentukan apakah seseorang layak dijatuhi pidana berdasarkan perbuatannya.

Pertanggungjawaban pidana adalah proses hukum di mana seseorang dianggap bertanggung jawab atas perbuatannya yang melanggar hukum dan dapat dijatuhi pidana. Dalam konteks ini, terdapat dua unsur utama yang harus dipenuhi: Unsur Objektif (Actus Reus): Perbuatan yang melanggar hukum yang dilakukan oleh pelaku. Unsur Subjektif (Mens Rea): Kesalahan atau niat jahat dari pelaku saat melakukan perbuatan tersebut.[23]

Seiring dengan perkembangan zaman dan kompleksitas kejahatan, konsep pertanggungjawaban pidana juga mengalami perubahan. Salah satunya adalah penerapan tanggung jawab korporasi (corporate liability), di mana badan hukum seperti perusahaan dapat dimintai pertanggungjawaban atas tindak pidana yang dilakukan oleh individu dalam lingkupnya.

G. Metode Penelitian

Untuk mencapai hasil yang optimal dalam penyusunan karya ilmiah, penting untuk menggunakan metode yang tepat. Menurut Soerjono Soekanto, penelitian hukum merupakan kegiatan ilmiah yang didasarkan pada metode, sistem, dan pemikiran tertentu, dengan tujuan untuk mempelajari gejala hukum melalui analisis. Fradhana Putra Disantara menyatakan dalam artikelnya bahwa penelitian hukum adalah upaya untuk menggali masalah hukum yang disebut isu hukum, berdasarkan karakteristik kajian hukum. Sifat hukum ini bersifat normatif, yang berarti berdasarkan norma atau aturan tertentu, dan harus dibedakan dari pandangan positivistik yang hanya melihat hukum sebagai kumpulan aturan tertulis.

[23] Fadlian, A. (2021). Pertanggungjawaban Pidana dalam Suatu Kerangka Teoritis. *Jurnal Hukum Positum*, 5(2). hal 10-19.

Avrila Anzani, dalam artikelnya, menjelaskan bahwa dalam penelitian ini, pendekatan yang digunakan adalah pendekatan yuridis normatif dengan menganalisis konsep hukum primer dan sekunder, yang kemudian ditinjau melalui pendekatan perundang-undangan dan sejarah. Peneliti mengumpulkan sumber data berdasarkan ketentuan perundang-undangan sebagai bahan hukum primer dan sekunder, serta memperoleh bahan hukum sekunder melalui literatur seperti buku, jurnal, laporan penelitian, dan artikel. Pengumpulan data dalam penelitian ini dilakukan dengan metode penelitian perpustakaan. Teknik analisis data yang digunakan adalah metode berpikir deduktif, dan hasil penelitian disajikan dalam bentuk deskriptif-kualitatif.

Metode penelitian yang digunakan bergantung pada jenis penelitian yang dilakukan. Umumnya, penelitian sosial, termasuk penelitian hukum, dapat ditinjau dari segi sifat, bentuk, tujuan, penerapan, dan disiplin ilmunya. Dari segi sifat, penelitian dapat dibedakan menjadi penelitian eksploratif, deskriptif, dan eksplanatoris.

1. Metode Pendekatan

   Pendekatan yang penulis gunakan pada penelitian ini adalah pendekatan Yuridis Normatif. Pendekatan Yuridis Normatif yaitu suatu penelitian hukum yang menggunakan data skunder, dan dilakukan dengan menekankan serta berpegang pada segi yuridis. Penelitian Yuridis Normatif merupakan kepustakaan, yaitu penelitian data skunder. Pendekatan Yuridis Normatif karena yang diteliti adalah asas hukum, aspek hukum, sekaligus kaidah hukum.

2. Spesifikasi Penelitian

   Penelitian ini menggunakan deskritif analisis, yang berarti menggambar gejala atau peristiwa yang terjadi dalam masyarakat dengan tepat dan tentunya jelas. Dalam buku yang ditulis oleh

Soerjono Soekanto menjelaskan, bahwa penelitian deskritif adalah untuk memberikan data yang seteliti mungkin dengan manusia, keadaan atau gejala-gejala lainnya. Kemudian mampu memberikan data yang lengkap mengenai permasalahan yang terjadi.

3. Sumber dan Jenis Data

Sumber data dari penilitian ini meliputi data primer dan data sekunder yang dijelaskan sebagai berikut:

a. Data Primer

Data Primer adalah data yang dikumpulkan ataupun diperoleh langsung di lapangan oleh orang yang melakukan penelitian atau yang bersangkutan. Data primer ini disebut juga data asli atau baru. Untuk penelitiann ini data primer berupa data hasil wawancara dengan informan. Jadi di dalam wawancara ini terdapat beberapa pertanyaan-pertanyaan yang telah di persiapkan terlebih dahulu sebagai pedoman untuk memudahkan diperolehkan data secara mendalam.

b. Data Sekunder

Data Sekunder adalah data yang diperlukan untuk melengkapi data primer yang di perlukan melalui studi pustaka. Data sekunder meliputi teori-teori, buku-buku, literatur, peraturan perundang-undangan yang berlaku.

1) Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang utama artinya mempunyai otoritas yang di utamakan. Bahan-bahan hukum primer terdiri dari:

a) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
b) Kitab Undang-Undang Hukum Pidana
c) Kitab Undang-Undang Hukum Pidana (Draft Terbaru)
d) Undang-Undang UU Informasi dan Transaksi Elektronik.

2) Bahan Hukum Sekunder

Bahan hukum sekunder, yaitu bahan hukum yang mendukung untuk memperkuat bahan hukum primer sekaligus memberikan penjelasan mengenai bahan hukum primer yang ada sehingga dapat di lakukannya pemahaman yang lebih mendalam, serta adanya penguatan atas dasar hukum menghasilkan analisis hukum yang terbaik. Biasanya bahan hukum sekunder berbentuk literatur buku-buku, jurnal, artikel, makalah, tulisan dan karya ilmiah.

3) Bahan Hukum Tersier

Bahan hukum tersier yaitu bahan hukum yang merupakan perlengkap yang sifatnya memberikan petunjuk dan penjelasan terkait bahan hukum primer dan bahan hukum sekunder. Bahan hukum tersier ini biasanya berbentuk kamus hukum, kamus bahasa indonesia, kamus bahasa Inggris, dan ensiklopedia.

4) Alat Pengumpulan Data

Untuk memperoleh data yang diperlukan dalam penelitian ini yang berhubungan dengan permasalahan yang di bahas, maka penelitian menggunakan alat pengumpulan data sebagai berikut:

a. Studi Kepustakaan

Sumber data yang diperoleh kepustkaan dengan membaca dan mengkaji kepustakaan untuk memperoleh informasi baik dalam bentuk dokumen, dan bukti yang telah di arsipkan sehubung dengan masalah yang akan di teliti.

b. Analisis data

Dalam melekukan analisis data digunakan metode analisis kualitatif, yaitu suatu tata cara penelitian yang menghasilkan data deskriptif analisis. Data

deskriptif analisis adalah data yang terkumpul tindak menggunakan angka-angka dan pengukuran, sehingga apa yang ditanyakan responden secara tertulis atau lisan yang diteliti dan dipelajari sebagai sesuatu yang utuh.

Dari hasil penelitian terhadap data yang diperoleh, maka dilakukan pengelolahan data dengan teknik editing, yaitu meneliti, mencocokan data yang di dapat, serta merapikan data tersebut.

H. Sistematika Penulisan

Penulisan tesis ini agar mempermudah dan memperjelas pembahsan, penulis akan menyusun secara sistematika sebagai berikut:

BAB I : Dalam bab ini dikemukakan mengenai latar belakang, perumusan masalah, tujuan penelitian, kegunaan/manfaat penelitian, keaslian penelitian, kerangka teo dan konsep, metode penelitian, dan sistematika penelitian

BAB II : Dalam bab ini berisi tentang tinjauan pustaka, yang terdiri dari yang berisikan Tinjauan Umum Kebijakan, Tinjauan Pustaka terkait Perlindungan Hukum, Tinjauan Pustaka mengenai *Artificial Intelligence*, dan Tinjauan Pustaka mengenai *Cyber Crime.*

BAB III : Dalam bab ini, akan membahas hasil penelitian dan pembahasan serta jawaban dari rumusan masalah yang terdapat pada bab pendahuluan, yaitu (1) Bagaimana Kebijakan Hukum Pidana Dalam Upaya Menanggulangi *Artificial Intelegence Cyber Crime* Dalam Hukum Positif Saat Ini?, (2) Bagaimana Kebijakan Hukum Pidana Dalam Upaya Menanggulangi

Artificial Intelegence Cyber Crime Hukum Pidana Positif Yang Akan Datang?

BAB IV : Penutup Bab ini merupakan penulis ingin memberikan kesimpulan dan saran pada bab penutup, bab ini berisi kesimpulan yang dibuat oleh penulis dari hasil penelitian dan Saran yang diberikan dan berhubungan dengan masalah yang timbul dalam penelitian tersebut.

BAB II
TINJAUAN PUSTAKA

A. Tinjauan Umum Kebijakan

1. Pengertian Kebijakan

Kebijakan pada dasarnya adalah suatu keputusan yang dipermasalahkan untuk memecahkan masalah tertentu, untuk melaksanakan kegiatan tertentu, yang melakukan kegiatan tertentu, atau untuk mencapai tujuan tertentu, dilakukan oleh instansi pemerintah yang berwenang dalam rangka melaksanakan tugas pemerintahan negara dan pembangunan bangsa.[24]

Menurut Fredrich dalam Agustino (2017: 166) kebijakan adalah serangkaian tindakan atau kegiatan yang diusulkan oleh seseorang, kelompok, atau pemerintah dalam suatu lingkungan tertentu dimana terdapat hambatan-hambatan (kesulitan-kesulitan) dan kemungkinan-kemungkinan (kesempatan-kesempatan) dimana kebijakan tersebut diusulkan agar berguna dalam mengatasinya untuk mencapai tujuan yang dimaksud.

Menurut Kamus Besar Bahasa Indonesia Kebijakan adalah rangkaian konsep dan asas yang menjadi pedoman dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak. Istilah ini dapat diterapkan pada pemerintahan, organisasi dan kelompok sektor swasta, serta individu.[25]

Secara umum, kebijakan juga dipandang sebagai pedoman dasar dalam pengambilan keputusan dan kebijakan dalam suatu organisasi ataupun kelompok. Thomas R. Dye (1978) menyatakan bahwa “Kebijakan publik merupakan apapun yang pemerintah pilih untuk dilakukan ataupun tidak dilakukan.”

[24] http://repositori.unsil.ac.id/770/3/3.%20BAB%20II.pdf pada 16 September 2023
[25] KBBI, diakses dari https://kbbi.kemdikbud.go.id/entri/kebijakan pada September 2023

Kebijakan juga dapat dipandang sebagai suatu sistem. Sistemnya adalah serangkaian bagian yang saling berkaitan dan bergantung serta diatur dalam aturan tertentu untuk menghasilkan satu unit. Menurut Dunn (1994) sistem kebijakan mencakup hubungan timbal balik dari tiga unsur yaitu kebijakan publik, pelaku kebijakan dan lingkungan hidup kebijakan. Dalam konteks yang lebih luas, kebijakan dianggap sebagai kebijakan formal meliputi undang-undang dan peraturan, serta kebijakan informal seperti norma-norma sosial atau praktik internal.

Jika dijabarkan, penjelasan di atas mengenai pengertian dan hakikat kebijakan, maka akan didapati berkaitan dengan unsur-unsur dari kebijakan. Kebijakan berdasarkan beberapa penjelasan di atas secara umum terdiri atas:

a. Masalah atau isu yang hendak diselesaikan
b. Tujuan atau sasaran yang ingin dituju
c. Tindakan atau langkah-langkah yang diinginkan atau direncanakan
d. Pelaku yang terlibat
e. Lingkungan tempat kebijakan dilaksanakan.

Dengan demikian maka kebijakan seharusnya bukan hanya sebagai keputusan yang dituangkan dalam dokumen formal saja, namun juga sebagai instrumen strategis yang dirancang untuk menyelesaikan isu-isu mendasar dalam suatu masyarakat.

2. Implementasi Kebijakan

Implementasi kebijakan secara umum dapat dimaknai sebagai proses menerapkan keputusan yang telah dibuat dalam tindakan nyata yang telah direncanakan. Menurut Grindle (1980:7) bahwa implementasi merupakan proses umum tindakan administratif yang dapat diteliti pada tingkat program tertentu. Proses implementasi baru akan dimulai apabila tujuan dan sasaran telah ditetapkan, program

kegiatan telah tersusun dan dana telah siap dan disalurkan untuk mencapai sasaran.[26] Jika pemahaman ini diarahkan pada lokus dan fokus (perubahan) dimana kebijakan diterapkan akan sejalan dengan pandangan Van Meter dan van Horn yang dikutip oleh Parsons (1995: 461) dan Wibawa, dkk., (1994: 15) bahwasannya implementasi kebijakan merupakan tindakan yang dilakukan oleh (organisasi) pemerintah dan swasta baik secara individu maupun secara kelompok yang dimaksudkan untuk mencapai tujuan.[27]

Sedangkan menurut Daniel A. Mazmanian dan Paul Sabatier, implementasi adalah peristiwa atau kegiatan yang timbul setelah disahkannya pedoman kebijakan negara (Solihin Abdul Wahab, 2008: 65). Menurut Carl J Federick seperti dikutip Leo Agustino mendefinisikan kebijakan sebagai serangkaian tindakan/kegiatan yang diusulkan oleh seseorang atau kelompok atau pemerintahan dalam lingkungan tertentu yang terdapat hambatan (kesulitan) dan peluang untuk mengimplementasikan usulan kebijakan agar dapat dicapai tujuan tertentu (Leo Agustino, 2008: 7). Jadi implementasi kebijakan merupakan suatu kegiatan atau tindakan yang diambil setelah berlakunya peraturan tersebut yang dapat menimbulkan dampak positif dan dampak negatif, serta dapat menimbulkan hambatan dalam pelaksanaannya.[28]

Sementara itu menurut Edward III, implementasi kebijakan dapat dipengaruhi oleh empat variabel yaitu ada komunikasi, sumber daya, dalam hal ini ada sumber daya dan juga sumber daya keuangan dapat mendukung pelaksanaan, perilaku pelaksana itu sendiri, dan juga adanya struktur birokrasi (Subarsono, 2011: 90-92.[29] Proses

[26] Haedar Akib, *Implementasi Kebijakan*, 2010, hlm.2

[27] Rita Novianti, dkk, *Implementasi Kebijakan Perlindungan Anak (Telaaah Uu No 35 Tahun 2014 Pasal 9 Ayat 1)*, 2020, hlm. 142

[28] *Ibid* hlm. 143

[29] *Ibid*, hlm. 143

dalam implementasi kebijakan di sini mencakup beberapa tahapan penting, diantaranya:

a. Perumusan kebijakan *(Policy Formulation)*

   Pada tahap perumusan, akan dilibatkan beberapa instrumen diantaranya seperti identifikasi terhadap masalah, analisis opsi solusi, dan penetapan keputusan dalam bentuk peraturan perundang-undangan.

b. Diseminasi *Kebijakan (Policy Dissemination)*

   Pada tahapan ini, kebijakan yang telah dirumuskan harus dikomunikasikan dengan pemangku kepentingan, pemerintahan yang memimpin, masyarakat, pihak swasta yang terkena dampak, pelaku industri. Pada tahap ini pula dilakukan sosialisasi peraturan perundang-undangan kepada masyarakat luas.

c. Pelaksanaan Kebijakan *(Policy Implementation)*

   Pada tahap ini akan dilibatkan aktor-aktor yang menjadi subjek hukum publik untuk menjalankan peraturan dan kebijakan yang telah dibuat.

d. Evaluasi Kebijakan *(Policy Evaluation)*

   Evaluasi dalam pelaksanaan kebijakan publik diperlukan agar dapat diketahui apa yang menjadi hambatan dan kekuranngan dari peraturan yang telah dibuat. Dengan mengetahui celah hukum yang ada, maka dapat dilakukan perbaikan sehingga peraturan atau kebijakan yang telah dibuat dapat dilaksanakan dengan baik oleh semua pihak dan memberikan keuntungan bagi semua orang dan instansi yang ada.

Selanjutnya menurut Mulyadi (2015:12), implementasi mengacu pada tindakan untuk mencapai tujuan-tujuan yang telah ditetapkan dalam suatu keputusan. Tindakan ini berusaha untuk mengubah keputusan-keputusan tersebut menjadi pola-pola operasional serta berusaha mencapai perubahan-perubahan besar atau kecil sebagaimana yang telah diputuskan sebelumnya. Implementasi

pada hakikatnya juga merupakan upaya pemahaman apa yang seharusnya terjadi setelah program dilaksanakan.[30] Dalam tataran praktis, implementasi adalah proses pelaksanaan keputusan dasar. Proses tersebut terdiri atas beberapa tahapan yakni:

a. Tahapan pengesahan peraturan *Cyber Crime* dan AI.
b. Pelaksanaan keputusan oleh instansi pelaksana.
c. Kesediaan kelompok sasaran untuk menjalankan keputusan.
d. Dampak nyata keputusan baik yang dikehendaki maupun tidak.
e. Dampak keputusan sebagaimana yang diharapkan instansi pelaksana.
f. Upaya perbaikan atas kebijakan atau peraturan *Cyber Crime* dan AI.

Proses persiapan implementasi setidaknya menyangkut beberapa hal penting yakni:

a. Penyiapan sumber daya, unit dan metode.
b. Penerjemahan kebijakan menjadi rencana dan arahan yang dapat diterima dan dijalankan.
c. Penyediaan layanan, pembayaran dan hal lain secara rutin.

Selain itu komunikasi dan sumber-sumber, faktor-faktor lain dapat mempengaruhi implementasi Kebijakan tersebut sesuai dengan harapan yaitu perilaku. Perilaku ini dapat berupa sikap komitmen serta sikap demokratis. Ketika para pelaksana mempunyai pandangan, sikap dan cara pandang yang berbeda berbeda dengan pengambil kebijakan, dalam hal ini pemerintah, adalah proses penerapan kebijakan tersebut menjadi kurang efektif.

[30] https://repositori.uma.ac.id/bitstream/123456789/1657/5/141801061_file%205.pdf diakses pada 16 September 2024

B. Tinjauan Pustaka Terkait Perlindungan Hukum

1. Pengertian Perlindungan Hukum

Secara terminologi, perlindungan hukum dapat diartikan dari gabungan dua definisi, yakni "perlindungan" dan "hukum". KBBI mengartikan perlindungan sebagai hal atau perbuatan yang melindungi. Lalu, hukum dapat diartikan sebagai peraturan atau adat yang secara resmi dianggap mengikat, yang dikukuhkan oleh penguasa atau pemerintah. Merujuk dari definisi tersebut, perlindungan hukum dapat diartikan dengan upaya melindungi yang dilakukan pemerintah atau penguasa dengan sejumlah peraturan yang ada. Singkatnya, perlindungan hukum adalah fungsi dari hukum itu sendiri; memberikan perlindungan.[31]

Satjipto Rahardjo mendefinisikan perlindungan hukum sebagai memberikan pengayoman terhadap hak asasi manusia yang dirugikan oleh orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum.[32] Sedangkan C.S.T. Kansil berpendapat bahwa perlindunngan hukum sebagai berbagai upaya hukum yang harus diberikan oleh aparat penegak hukum untuk memberikan rasa aman, baik secara pikiran maupun fisik dari segala gangguan dan berbagai ancaman dari pihak manapun.[33]

Menurut Muchsin, Perlindungan Hukum merupakan suatu hal yang melindungi subyek-subyek hukum melalui peraturan perundang-undangan yang berlaku dan dipaksakan pelaksanaannya dengan suatu sanksi. Sedangkan menurut Philipus M. Hadjon berpendapat bahwa Perlindungan Hukum adalah perlindungan akan harkat dan martabat, serta pengakuan terhadap hak-hak asasi manusia yang dimiliki oleh

---

[31] "Perlindungan Hukum: Pengertian, Unsur, dan Contohnya", https://www.hukumonline.com/berita/a/perlindungan-hukum-lt61a8a59ce8062/, 16 September 2023

[32] Satjipto Rahardjo, 2000, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, hlm.54.

[33] C.S.T. Kansil, 1989, *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*, Balai Pustaka, Jakarta, hlm.102.

subyek hukum berdasarkan ketentuan hukum dari kesewenangan.[34] Perlindungan hukum dapat dibedakan menjadi dua, yaitu:

a. Perlindungan Hukum Preventif, yaitu perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan maksud untuk mencegah suatu pelanggaran serta memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu kewajiban.
b. Perlindungan Hukum Represif, merupakan perlindungan akhir berupa sanksi seperti denda, penjara, dan hukuman tambahan yang diberikan apabila sudah terjadi sengketa atau telah dilakukan suatu pelanggaran.

Perlindungan hukum preventif ini terdapat dalam banyak peraturan perundang-undangan yang berlaku guna memberikan pencegahan tindak pidana kejahatan dan menjadi batasan dalam melaksanakan kewajiban dalam hukum, sedangkan perlindungan hukum represif secara umum berfungsi menyelesaikan sengketa yang telah muncul akibat adanya pelanggaran hukum.

2. Tujuan, Unsur, dan Tantangan Perlindungan Hukum

Perlindungan hukum dalam sistem hukum nasional di berbagai negara khususnya di Indonesia pada dasarnya diciptakan untuk memberikan kepastian. Namun, bukan hanya memberikan kepastian hukum saja, perlindungan hukum juga memiliki tujuan lain, diantaranya:[35]

[34] Di akses dari http://portaluniversitasquality.ac.id:55555/143/4/BAB%20II.pdf, 16 September 2023, hlm. 8

[35] Satjipto Rahardjo. 2000. *Hukum dan Perubahan Sosial: Suatu Tinjauan Teoritis serta Pengalaman-Pengalaman di Indonesia.* Jakarta: Genta Publishing, hlm. 87.

a. Menciptakan kepastian hukum, hal ini bertujuan agar masyarakat dapat memahami hak dan kewajibannya berdasarkan aturan hukum yang berlaku di suatu negara[36]
b. Menjamin keadilan, yaitu dengan melindungi hak individu ahar tidak dirugikan oleh tindakan yang melanggar hukum dan kesusilaan
c. Memberikan pemulihan, yakni menyediakan mekanisme penyelesaian hukum atas pelanggaran yang dilakukan.

Selain tujuan di atas, perlindungan hukum juga melibatkan banyak unsur penting yang saling berkesinambungan dan bekerja satu sama lain. Sehingga unsur-unsur dalam perlindungan hukum diantaranya ialah:

a. Peraturan hukum yang jelas dan tegas yang berfungsi sebagai dasar dalam melindungi hak-hak hukum individu
b. Penegak hukum yang memiliki kompetensi (polisi, jaksa, hakim, pengacara, dan pihak-pihak hukum lainnya)
c. Mekanisme penegakan hukum, yaitu sistem yang mengatur bagaimana seharusnya hukum dilaksanakan termasuk mekanisme dalam pengadilan dan institusi lainnya
d. Kesadaran hukum masyarakat

Di Indonesia secara umum hingga saat ini, perlindungan hukum masih menemui masalah dalam implementasinya. Beberapa masalah yang kerap kali dihadapi dalam upaya mencapai perlidungan hukum untuk menciptakan kepastian hukum diantaranya ialah:

a. Ketidakpastian hukum dengan banyaknya peraturan perundang-undangan yang tidak jelas dan bertentangan

   Ketidakpastian hukum yang disebabkan oleh peraturan yang tumpang tindih atau inkonsisten, sehingga membingungkan

[36] Philipus M. Hadjon. 2007. *Perlindungan Hukum bagi Rakyat Indonesia: Sebuah Studi tentan Prinsip-Prinsipnya, Penanganannya oleh Peradilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara*. Surabaya: Peradaban, hlm. 98.

aparat dan masyarakat dalam pelaksanaannya. Selain itu, perubahan regulasi yang cepat tanpa sosialisasi memadai juga menambah ketidakpastian ini.

b. Ketimpangan akses dimana tidak semua individu memiliki kemampuan atau sarana untuk mengakses perlindungan hukum

Kurangnya akses ke keadilan juga menjadi tantangan besar. Biaya litigasi yang mahal membuat masyarakat miskin sulit membawa kasus mereka ke pengadilan. Di daerah terpencil, keterbatasan infrastruktur hukum seperti pengadilan dan layanan bantuan hukum menyebabkan banyak masyarakat tidak mendapatkan perlindungan hukum. Selain itu, rendahnya literasi hukum membuat banyak orang tidak memahami hak-hak mereka, sehingga sulit untuk menuntut keadilan.

c. Penyalahgunaan wewenang oleh aparat penegak hukum

Korupsi dalam penegakan hukum memperburuk situasi. Penyalahgunaan wewenang oleh aparat hukum melalui praktik suap atau gratifikasi menghambat penerapan hukum yang adil. Misalnya, kasus kriminal yang melibatkan "uang pelicin" sering kali berakhir dengan bebasnya pelaku dari hukuman. Kurangnya pengawasan dan integritas aparat penegak hukum memperparah masalah ini.

d. Ketimpangan sosial dan ekonomi

Ketimpangan sosial dan ekonomi juga menjadi faktor penghambat. Kelompok rentan seperti masyarakat adat, perempuan, dan penyandang disabilitas sering menghadapi diskriminasi. Dalam banyak kasus, pihak yang memiliki kekuatan ekonomi atau politik lebih mudah memenangkan sengketa hukum meskipun tidak memiliki dasar hukum yang kuat.

e. Penegakan hukum yang lambat dan tidak konsisten

Penegakan hukum yang lambat dan tidak konsisten menjadi tantangan serius. Banyak kasus membutuhkan waktu bertahun-tahun untuk diselesaikan, sehingga keadilan tertunda. Selain itu, keputusan pengadilan yang berbeda dalam kasus serupa menunjukkan kurangnya standar yang konsisten dalam sistem peradilan.

f. Masyarakat juga menghadapi kendala budaya seperti rendahnya kesadaran hukum.

Banyak orang tidak mengetahui hak dan kewajiban hukum mereka, sehingga sering menjadi korban pelanggaran. Di beberapa daerah, masyarakat lebih memilih menyelesaikan masalah melalui jalur informal seperti kekerasan atau perjanjian lisan, yang sering tidak memberikan perlindungan hukum formal.

g. Intervensi politik

Intervensi politik dalam penegakan hukum juga menjadi tantangan. Aparat penegak hukum sering mendapat tekanan politik dalam menangani kasus tertentu, terutama yang melibatkan tokoh penting. Selain itu, regulasi yang dibuat sering kali lebih menguntungkan kelompok elit daripada masyarakat umum.

h. Globalisasi dan perkembangan teknologi

Globalisasasi turut memperburuk tantangan ini. Kejahatan transnasional seperti perdagangan manusia dan kejahatan siber semakin sulit ditangani karena melibatkan yurisdiksi lintas negara. Di sisi lain, perkembangan teknologi seperti kecerdasan buatan belum diatur secara memadai oleh hukum, sehingga memberikan celah untuk pelanggaran.

Dengan tantangan-tantangan ini, diperlukan reformasi hukum yang komprehensif, penguatan kapasitas aparat penegak hukum, dan peningkatan kesadaran masyarakat agar perlindungan hukum dapat dijalankan dengan lebih baik dan efektif.

C. Tinjauan pustaka *Artificial Intelligence*

1. Pengertian *Artificial Intelligence*

AI dapat diartikan sebagai penelitian dan perancangan agen cerdas, di mana agen cerdas merupakan sistem yang memantau lingkungannya dan mengambil tindakan untuk meningkatkan kemungkinan mencapai tujuannya. Secara lebih rinci, AI mencakup pengembangan algoritma dan teknologi yang memungkinkan komputer meniru fungsi kognitif manusia. Saat ini, AI dibedakan menjadi dua kategori utama, yaitu AI sempit (atau AI lemah) yang dirancang dan dilatih untuk menyelesaikan tugas tertentu, dan AI umum (AGI atau AI kuat) yang memiliki kemampuan intelektual setara manusia dan mampu menjalankan berbagai tugas kognitif.

AI saat ini sidah menjadi bagian penting dalam kehidupan manusia di semua lini kehidupan. Pemanfaat kecerdasan buatan dalam berbagai bidang saat ini terus digenjot pemerintah untuk membantu masyarakat dan pemerintah dalam pelayanan publik. Pemanfaatan kecerdasan buatan dalam penegakkan hukum di Indonesia saat ini dapat ditengok di bidang lalu lintas dengan penggunaan tilang elektronik (e-tilang). Dalam sistem e-tilang ini pelaksanaan penertiban lalu lintas sudah tidak lagi melibatkan petugas secara langsung, Namun dengan memanfaatkan kamera pemantau (CCTV) yang dipantau secara otomatis melalui sistem elektronik yang sudah dirancang dengan memanfaatkan *artificial intellegence* atau komputerisasi.

AI sempit berfokus pada penerapan dalam bidang-bidang tertentu, seperti pengenalan suara, pemrosesan gambar, atau permainan catur, di mana ia sangat terampil namun terbatas pada fungsi yang telah ditentukan. Di sisi lain, AI umum bertujuan untuk meniru kemampuan berpikir dan memahami yang lebih luas, memungkinkan sistem untuk belajar dan beradaptasi dalam berbagai

situasi tanpa harus diprogram secara khusus untuk setiap tugas. Perkembangan kedua kategori ini terus berlanjut, dengan tujuan meningkatkan efisiensi dan efektivitas dalam menyelesaikan berbagai masalah kompleks yang dihadapi oleh manusia.

Dengan kemajuan teknologi, AI sempit semakin banyak diterapkan dalam berbagai industri, seperti kesehatan, keuangan, dan transportasi, untuk meningkatkan produktivitas dan akurasi. Contohnya, dalam bidang kesehatan, AI digunakan untuk menganalisis data pasien dan membantu dalam diagnosis penyakit. Sementara itu, AI umum masih dalam tahap penelitian dan pengembangan, dengan banyak tantangan yang perlu diatasi, termasuk aspek etika dan keamanan.

Seiring dengan peningkatan kemampuan AI, penting untuk mempertimbangkan implikasi sosial dan ekonomi yang mungkin muncul, termasuk dampak pada tenaga kerja dan privasi data. Dengan demikian, pemahaman yang mendalam mengenai kedua kategori AI ini sangat penting untuk merumuskan kebijakan yang tepat dan bertanggung jawab dalam penerapan teknologi ini di masyarakat.

Selain itu, integrasi kecerdasan buatan ke dalam kehidupan sehari-hari memunculkan tantangan baru terkait regulasi dan tanggung jawab. Pertanyaan mengenai siapa yang bertanggung jawab atas keputusan yang diambil oleh sistem AI, apakah itu pengembang, pengguna, atau bahkan algoritma itu sendiri menjadi semakin relevan. Ini menggarisbawahi pentingnya penelitian yang lebih lanjut mengenai aspek etis dan legal dari AI.

Secara umum saat ini kecerdasan buatan sudah banyak membantu manusia dalam berkegiatan. Namun pemanfaatan yang meluas ini pada akhirnya menimbulkan suatu pertanyaan, bagaimana pertanggungjawaban atas apa yang dilakukan oleh kecerdasan buatan ini?.

Berbicara pertanggungjawaban hukum maka akan berbicara pula mengenai subjek hukum. Menurut L.J. Van Apeldoorn dijelaskan "Diperlukan syarat-syarat untuk dapat melakukan perbuatan hukum, yaitu subjek hukum yang memiliki kemampuan memegang hak." Dari sini maka dapat ditarik kesimpulan bahwa untuk dapat dikategorikan sebagai subjek hukum, maka rujukannya ialah peraturan perundang-undangan yang berlaku.

Kecerdasan buatan memiliki hak dan kewajiban yang pelaksanaannya diatur sehingga harus sesuai dengan norma-norma hukum yang berlaku dalam masyarakat. Namun, kecerdasan buatan di sini tentunya tidak dapat disamakan dengan manusia, sebab manusia memiliki akal dan nafsu sedangkan kecerdasan buatan dirancang untuk membantu manusia yang mana tentu tidak memiliki kedua hal tersebut meskipun memiliki hak dan kewajiban yang sama. Kesamaan di sini ialah kesamaan status hukum sebagai subjek hukum.[37] Dalam konteks ini, maka apabila kecerdasan buatan melakukan kesalahan, ia akan dianggap melanggar hukum dan diharuskan bertanggungjawab atas kesalahannya. Pertanggungjawaban ini akan dikembalikan pada aturan dasarnya, apakah karena kesengajaan pihak pengembang atau karena adanya gangguan sistem ayng dikembangkan oleh pengembang kecerdasan buatan.

Di masa depan, pengembangan AI yang lebih cerdas dan beradaptasi diharapkan dapat membawa manfaat besar, seperti peningkatan efisiensi di berbagai sektor dan kemampuan untuk memecahkan masalah kompleks yang sebelumnya sulit diatasi oleh manusia. Namun, keberhasilan tersebut harus sejalan dengan upaya untuk memastikan bahwa teknologi ini digunakan secara adil dan bertanggung jawab, serta memberikan manfaat bagi seluruh lapisan

[37] Febri Jaya dan Wilton Goh, "Analisis Yuridis Terdahap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia", *Jurnal Supremasi Hukum*, Edisi Vol. 17 No.02, Juli 2021, hlm. 2

masyarakat. Oleh karena itu, penting untuk menciptakan dialog yang berkelanjutan antara ilmuwan, pembuat kebijakan, dan masyarakat agar perkembangan AI dapat diarahkan untuk kebaikan bersama.[38]

2. Pengaturan Artificial Intellegence di Indonesia

Indonesia mengenal 2 jenis subjek hukum, yakni subjek hukum orang atau *"naturalijk person"* dan subjek hukum badan atau *"recht person"*.[39] Kedua jenis subjek hukum tersebut memiliki karakteristik yang berbeda. Dalam konteks subjek hukum kecerdasan buatan atau *artificial intellegence* masih menimbulkan perdebatan di kalangan ahli hukum. Sebab meskipun dianggap sebagai subjek hukum, tetapi antara manusia dan kecerdasan buatan memiliki banyak sekali perbedaan dan dalam hal ini tentu AI bukanlah makhluk hidup, melainkan sebuah sistem. Tetapi yang menimbulkan pertanyaan ialah fakta bahwa kecerdasan buatan ini hidup berdampingan dengan manusia dan memiliki banyak dampak nyata bagi manusia.

Pada hakekatnya, *Artificial Intelligence* dan manusia merupakan 2 hal yang berbeda. Perbedaan paling mendasar ada pada sifat alami dalam proses lahirnya.[40] Apabila *Artificial Intelligence* dianalogikan sebagai manusia khususnya pekerja, dapat dihubungkan dengan pasal 1367 ayat (1) dan (3) Kitab Undang-Undang Hukum Perdata (KUHPER) yang berisi:[41]

> *(1) "Seseorang tidak saja bertanggung jawab untuk kerugian yang disebabkan perbuatannya sendiri, tetapi juga untuk kerugian yang disebabkan perbuatan orangorang yang menjadi*

[38] Di akses melalui https://medium.com/@hidayatkampai/definisi-kecerdasan-buatan-ai-menurut-para-ahli-11a6eba95ef4 pada tanggal 23 Oktober 2024

[39] Dudu Duswara Machmudin, Pengantar Ilmu Hukum (Sebuah Sketsa), PT Refika Aditama, Bandung, 2010, hlm. 32.

[40] FL. Yudhi Priyo Amboro, Khusuf Komarhana, "Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata di Indonesia", terdapat dalam https://ojs.uph.edu/index.php/LR/article/view/3513/pdf, Diakses tanggal 7 Juni 2024.

[41] Subekti dan R. Tjitrosubidio, Kitab Undang-Undang Hukum Perdata, Pradnya Paramita, Jakarta, 2008, hlm. 346.

tanggung jawabnya atau disebabkan oleh barang-barang yang berada di bawah pengawasannya."

(3) "Majikan-majikan dan orang yang mengangkat orang lain untuk mewakili urusan-urusan mereka adalah bertanggung jawab tentang kerugian yang diterbitkan oleh pelayan-pelayan atau bawahan-bawahan mereka di dalam melakukan pekerjaan untuk mana orang-orang ini dipakainya."

Dengan dianalogikannya *Artificial Intelligence* sebagai pekerja atas dasar karakteristik yang ada dalam sistem. Tidak dapat dipungkiri lagi bahwa pekerjaan yang dapat dilakukan *Artificial Intelligence* sejauh ini merupakan pekerjaan yang dapat dilakukan manusia atau bisa lebih dalam beberapa kasus tertentu. Apabila *Artificial Intelligence* dianalogikan sebagai pekerja, maka secara otomatis pencipta dan pengembang *Artificial Intelligence* adalah pemberi kerja.[42]

Kecerdasan buatan merupakan hasil karya manusia maka sebetulnya mereka lebih masuk akal jika dikategorikan sebagai subjek hukum badan. Sebab kecerdasan buatan adalah sistem elektronik yang manusia ciptakan, dan secara lahiriyah mereka tidak memiliki naturalitas seperti manusia yang memiliki fisik dan emosional. Kesamaan *Artificial Intelligence* dengan entitas hukum yang menguatkan posisi *Artificial Intelligence* termasuk ke dalam subjek hukum badan ini tidak lantas menjadikan peraturan-peraturan yang diberlakukan harus sama. Meskipun terdapat berbagai kesamaan, namun di sisi lain *Artificial Intelligence* dengan entitas badan hukum lain seperti contohnya perusahaan tentu memiliki perbedaan dari segi keamanan dan resiko hingga transparansi dan akuntabilitas.[43]

Regulasi yang mengatur secara rinci mengenai kecerdasan buatan hingga saat ini belum ada di Indonesia. Hingga sekarang,

[42] Fatimah Nada, et.al. Op. cit. Hlm. 154.
[43] Fatimah Nada, et.al. Op. cit. Hlm. 155.

pengaturan mengenai kecerdasan buatan masih diasosiasikan dengan sistem elektronik dalam Undang-Undang Informasi dan Transaksi Elekronik dan berbagai peraturan perundang-undangan lainnya yang mengatur sistem informasi dan kejahatannya. Kekosongan hukum yang mengatur kecerdasan buatan ini jika terus dibiarkan akan menimbulkan potensi penyalahgunaan *Artificial Intellegence*, seperti diskriminasi algoritma, pelanggaran privasi, dan kejahatan siber berbasis kecerdasan buatan. Oleh sebab itu, maka diperlukan kebijakan yang tepat guna dalam pengaturan AI di Indonesia untuk menghindari berbagai pelanggaran seperti di atas. Pendekatan multistakeholder dan harmonisasi pada regulasi internasional menjadi penting untuk dikaji penerapannya.

D. Tinjauan Pustaka *Cyber Crime*

1. Pengertian *Cyber Crime*

Di zaman yang serba digital seperti sekarang, kejahatan terjadi dengan berbagai macam cara. Kejahatan melalui ruang-ruang digital menjadi salah satu kejahatan yang banyak terjadi saat ini. *Cyber Crime* menjadi istilah yang umum digunakan untuk menyebut kejahatan yang terjadi di ruang-ruang digital. *Cyber Crime* merupakan kegiatan yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit *(carding)*, *confidence fraud*, penipuan identitas, pornografi anak, dan sebagainnya.

Semakin maraknya kasus kejahatan siber membuat pemerintah harus bergerak dengan cepat dalam menaggulangi merebaknya kejahatan siber di Indonesia. Pembentukan peraturan perundang-undangan menjadi fokus utama saat itu, hingga terbentuklah Undang-Undang Nomr 11 Tahun 2008 tentang Informasi dan

Transaksi Elektronik. Di dalam undang-undang tersebut, pemerintah turut memasukkan *cyber crime* sebagai salah satu hal yang diatur, dengan harapan agar kejahatan siber yang saat itu baru mulai marak terjadi dapat diatasi, dikurangi, dan dihentikan.

Di Indonesia, pengaturan mengenai kejahatan siber tertuang dalam beberapa peraturan perundang-undangan seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diperbaharui melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Undang-Undang ini mengatur mengenai transaksi elektronik dan kejahatan siber berupa penyebarluasan informasi yang tidak benar, pencemaran nama baik melalui internet, dan peretasan *(hacking).*

2. Jenis, Sifat, dan Karakteristik Cyber Crime

Kejahatan siber atau *Cyber Crime* terdiri atas 2 (dua) jenis, yaitu kejahatan yang menggunakan teknologi informasi sebagai fasilitas, serta kejahatan yang menggunakan teknologi informasi sebagai sasaran, berikut penjelasannya[44]:

1. Kejahatan yang menggunakan teknologi informasi sebagai fasilitas, seperti kejahatan pembajakan hak cipta, pornografi, pemalsuan dan pencurian kartu kredit *(carding),* dan penipuan berbasis online, serta penyebaran informasi palsu dan *hatespeech* atau ujaran kebencian.

2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran, seperti peretasan *(hacking)*, merusak situs internet dan data *(cracking),* serta penyebarluasan informasi rahasia *(defecting).*

[44] Sutanto, H.S., & Sugiarto. Cybercrime – Motif dan Penindakan. Jakarta: Pensil 324.

Kejahatan dunia maya atau kejahatan siber dikategorikan dalam 2 (dua) sifat, yakni kejahatan siber sebagai tindakan kriminal, dan kejahatan siber sebagai kejahatan abu-abu:[45]

1. *Cyber Crime* sebagai tindakan kejahatan

   Menurutnya, kejahatan siber dianggap sebagai tindakan kejahatan karena dilakukan dengan melakukan tindakan kriminal melalui internet atau dunia maya sebagai fasilitas dan medianya. *Carding* (pencurian kode kartu anjungan tarik tunai), hacking (peretasan sistem elektronik), *scam* (penipuan menggunakan jaringan internet) menjadi beberapa contoh kejahatan yang dilakukan dengan menggunakan internet sebagai medianya.

2. *Cyber Crime* sebagai kejahatan abu-abu

   Kejahatan siber kerap kali terjadi secara abu-abu atau didefiniskan sebagai kejahatan yang sebenarnnya secara hukum aktifitas tersebut bukanlah kejahhatan. Namun, aktifitas abu-abu dalam dunia maya ini sering kali juga menimbulkan kerugian bagi orang lain, dan pelaku yang melakukan aktifitas kejahatan abu-abu ini melakukannya untuk tujuan tertentu tanpa adanya izin dari orang lain yang pada akhirnya merasa dirugikan dan menjadi korban. *Probing* atau *portscanning* (memantau sistem orang lain tanpa izin) menjadi contoh kejahatan siber abu-abu.

Kejahatan siber terjadi dengan tujuan dan motif yang bermacam-macam. Beberapa karakteristik kejahatan siber yang dipaparkan oleh Freddy Haris terdiri atas *Unauthorized Access* (dengan maksud untuk memfasilitasi kejahatan), *Unauthorized alteration or destruction of data*, serta mengganggu dan merusak operasi komputer. Selanjutnya Barda Nawawi Arief dalam bukunya memaparkan kualifikasi kejahatan dunia maya berdasarkan

[45] Fiorida Mathilda, "Cyber Crime dalam Sistem Hukum Indonesia," *SigmaMu* 4, no. 2 (September 2012): 36.

Convention on Cyber Crime di Budapest, Hungaria pada 2001 terdiri atas[46]:

1. *Illegal interception*, yaitu sengaja dan diam-diam melakukan pengiriman data komputer yang bersifat rahasia
2. *Data interference*, yaitu perusakan, penghapusan, perubahan, dan penghapusan data komputer
3. *System interference*, yaitu gangguan serius terhadap berfungsinya komputer
4. *Misuses of device*, yaitu penyalahgunaan perlengkapan komputer
5. *Computer related forgery*, yaitu pemalsuan data
6. *Computer related fraud*, yaitu penipuan dengan tujuan memperkaya diri dengan mengganggu fungsi komputer
7. *Content-related offences,* yaitu delik-delik pornografi anak
8. *Offence related to infringements of copyright and related rights*, yaitu delik-delik pelanggaran hak cipta.

Selain karakteristik di atas, kejahatan siber juga terdiri atas beberapa karaktersitik unik lainnya, diantaranya yaitu:[47]

1. Perbuatan dilakukan secara ilegal dilakukan dan terjadi di ruang digital, sehingga tidak dimungkinkan untuk mengetahui yurisdiksi hukum negara dan daerah mana yang berlaku untuk kejahatan tersebut
2. Perbuatan tersebut dilakukan dengan menggunakan perangkat internet
3. Kerugian materil dan non-materil atas tindakan kejahatan siber sering kali lebih besar daripada kejahatan konvensional lainnya
4. Pelakunya adalah orang yang mengetahui dan paham penggunaan perangkat komputer dan sistem informasi

[46] Barda Nawawi Arief. (2006). *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia.* Raja Grafindo Persada.

[47] Miftakhur Rokhman Habibi, Isnatul Liviani. *Op. cit. hlm. 411.*

5. Perbuatan kejahatan siber dilakukan secara transnasional (antar negara).

3. Regulasi *Cyber Crime* di Indonesia

Sebagai negara yang besar dengan jumlah penduduk yang amat besar, Indonesia menjadi negara dengan tingkat kejahatan siber yang masih sangat tinggi. Kejahatan siber yang umum terjadi di Indonesia ialah peretasan, *scamming* (penipuan), dan *carding*. Meski kejahatan siber sangat sering terjadi, namun upaya penvegahan yang pemerintah lakukan melalui upaya-upaya pembentukan kebijakan hukum dan upaya *defence* masih sangat minim dan jauh tertinggal dari negara lain. Sering kali terdengar data-data pemerintah dan perusahaan swasta dibobol oleh sekelompok *hacker* yang selanjutnya mereka jual atau di-*lock* guna meminta tebusan dari pemilik data tersebut.

Hingga saat ini kebijakan yang mengatur mengenai kejahatan siber masih sangat minim. Namun selain karena perundang-undangan yang belum lengkap, karakteristik kejahatan siber yang dilakukan secara transnasional juga menyulitkan pemerintah dan pihak berwajib untuk menanggulangi kejahatan ini. Tingginya angka kejahatan siber di Indonesia melahirkan ancaman serius bagi pemerintah dan masyarakat. Indonesia hingga saat ini masih menjadi salah satu negara dengan tingkat kejahatan siber tertinggi di dunia.

Tingginya angka ini menjadi bukti bahwa Indonesia belum memiliki kemampuan yang baik dalam menciptakan keamanan data dan keamanan ruang digital di negarannya. Badan Siber dan Sandi Negara (BSSN) saat ini menjadi salah satu badan pemerintah yang secara khusus menangani keamanan siber dan dunia maya di Indonesia. Sedangkan untuk kejahatan siber, saat ini Divisi Siber yang dimiliki Kepolisian Republik Indonesia menjadi pihak yang bertugas memantau dan memastikan ruang digital masyarakat aman.

Pengaturan kejahatan siber di Indonesia tidak secara khusus mengatur mengenai *Cyber Crime*. Beberapa peraturan perundang-undangan yang saat ini berlaku sudah mengatur pencegahan kejahatan siber seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Terorisme, serta Undang-Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Undang-Undang di atas telah mengatur secara detail memgenai jenis, karakteristik, dan ancaman hukuman bagi pelaku kejahatan siber di Indonesia.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau UU ITE yang saat ini menjadi salah satu kebijakan hukum uutama dalam penanganan kejahatan siber telah mengatur beberapa jenis kejahatan di ruang digital. Beberapa jenis kejahatan siber yang diatur dalam undang-undang ini diantaranya:

1. Tindakan yang melanggar kesusilaan, seperti pornografi, pornoaksi, dan prostitusi secara online
2. Perjudian online
3. Penghinaan dan pencemaran nama baik melalui media digital
4. Pemerasan dan pengancaman
5. Penguntitan secara online *(cyberstalking)*
6. Penyebaran berita palsu *(hoax)*
7. Ujaran kebencian dan *cyber bullying*
8. Akses ilegal sistem informa

BAB III
HASIL PENELITIAN DAN PEMBAHASAN

A. Kebijakan Hukum Pidana dalam upaya menanggulangi AI *(Artificial Intelegence) Cyber Crime* dalam Hukum Positif Saat Ini

Seiring dengan meningkatnya ancaman kejahatan dunia maya, seperti penipuan kartu kredit (carding), skimming pada ATM/EDC, peretasan (hacking), pembobolan sistem (cracking), phishing, penyebaran malware (seperti virus, worm, trojan, dan bot), cybersquatting, pornografi, perjudian online, serta kejahatan transnasional yang melibatkan perdagangan narkoba, kejahatan terorganisir (mafia), terorisme, pencucian uang, perdagangan manusia, dan ekonomi bawah tanah, sangat penting untuk diterapkannya perlindungan data yang komprehensif. Dalam hal ini, diperlukan adanya aturan hukum yang bersifat mengikat dan ditegakkan secara konsisten untuk melindungi informasi pribadi. Aturan ini juga bertujuan untuk memastikan bahwa subjek data tetap memiliki kendali penuh terhadap informasi pribadi mereka, menghindari penyalahgunaan, dan memberikan jaminan keamanan serta privasi di dunia digital.[48]

Pada era digital saat ini, penyalahgunaan teknologi dan media sosial semakin sering terjadi di tengah masyarakat. Salah satu kasus yang baru-baru ini menjadi sorotan adalah kasus penyebaran konten menyimpang melalui platform Facebook, yang dilakukan oleh akun dengan nama "Fantasi Sedarah." Dalam grup tersebut, disebarkan berbagai konten bermuatan seksual yang menyimpang, khususnya bertema incest (hubungan sedarah) dan eksploitasi seksual, yang secara jelas bertentangan dengan norma hukum, etika, dan kesusilaan publik.

Tindakan semacam ini merupakan bentuk kejahatan siber yang dapat dikenakan sanksi pidana berdasarkan peraturan perundang-undangan yang berlaku. Pelaku dalam kasus tersebut dapat dijerat dengan Pasal 27 ayat (1)

[48] Zainuddin Kasim, "Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia, Vol.2, No.1,Juli 2023,hlm.20

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang mengatur tentang larangan distribusi atau transmisi konten yang melanggar kesusilaan. Selain itu, dapat dikenakan pula Pasal 45 ayat (1) UU ITE, yang mengatur sanksi pidana bagi siapa pun yang dengan sengaja dan tanpa hak mendistribusikan atau membuat dapat diaksesnya konten tersebut.

Peningkatan kejahatan dunia maya, yang semakin beragam dan canggih, menuntut adanya upaya sistematis dalam penyusunan kebijakan yang dapat mengakomodasi kebutuhan perlindungan data pribadi. Kejahatan seperti penipuan kartu kredit (carding), peretasan sistem (hacking), dan penyebaran malware memiliki dampak yang merugikan bagi individu, organisasi, dan bahkan negara. Oleh karena itu, undang-undang yang mengatur perlindungan data pribadi menjadi sangat relevan dan mendesak untuk diterapkan guna memitigasi risiko yang ditimbulkan.

Meskipun demikian, kurangnya regulasi yang jelas mengenai perlindungan data pribadi menyebabkan meningkatnya kasus penyalahgunaan sistem informasi dan data pribadi. Oleh karena itu, sangat penting untuk mengembangkan sebuah sistem yang dapat mengatasi permasalahan tersebut. Saat ini, Indonesia masih belum memiliki undang-undang yang secara spesifik mengatur perlindungan data pribadi. Peraturan yang ada selama ini hanya tersebar di berbagai undang-undang yang berbeda, sehingga diperlukan pembentukan undang-undang yang lebih komprehensif, terperinci, dan tegas untuk mengatur perlindungan hak milik pribadi tersebut.[49]

Pentingnya perlindungan data pribadi semakin dirasakan seiring dengan meningkatnya penggunaan teknologi informasi dalam kehidupan sehari-hari. Tanpa adanya regulasi yang jelas dan memadai, potensi penyalahgunaan data pribadi semakin besar, baik itu untuk kepentingan komersial maupun kejahatan siber. Hal ini menuntut negara untuk segera

[49] Zainuddin Kasim, *Ibid*, .hlm.20

mengambil langkah konkret dalam menyusun undang-undang yang tidak hanya mengatur hak-hak individu atas data pribadinya, tetapi juga memberikan sanksi yang tegas bagi pelaku penyalahgunaan. Keberadaan undang-undang yang komprehensif ini diharapkan dapat memperkuat kepercayaan masyarakat terhadap sistem digital dan mencegah terjadinya eksploitasi data yang merugikan pihak-pihak yang tidak bertanggung jawab.

Kitab "Undang-Undang Hukum Pidana" (KUHP) merupakan fondasi utama bagi peraturan-peraturan hukum pidana di Indonesia. Meskipun KUHP ini berasal dari zaman penjajahan Belanda, hingga saat ini, karena belum ada perubahan atau penerimaan terhadap pembaruan yang telah diusulkan oleh para ahli hukum pidana Indonesia sejak tahun 1963, KUHP yang ada masih tetap digunakan untuk memastikan eksistensi hukum pidana dalam masyarakat Indonesia.[50]

Meski begitu, penggunaan KUHP yang masih bersumber dari produk hukum kolonial ini tidak lepas dari kritik, terutama terkait dengan relevansi dan kesesuaiannya dengan kondisi sosial, politik, dan budaya Indonesia yang terus berkembang. Proses pembaharuan KUHP telah menjadi perhatian serius bagi kalangan akademisi dan praktisi hukum Indonesia sejak lama. Berbagai upaya untuk memperbarui KUHP ini telah dilakukan, namun perubahan yang diharapkan hingga saat ini belum terlaksana secara menyeluruh. Pembaharuan KUHP dianggap sebagai langkah penting untuk menyelaraskan hukum pidana Indonesia dengan nilai-nilai dan kebutuhan masyarakat modern, termasuk dalam hal perlindungan terhadap hak asasi manusia dan keadilan sosial.

Kebijakan pencegahan kejahatan siber melalui hukum pidana termasuk dalam cakupan kebijakan penal, yang merupakan bagian dari kebijakan kriminal secara keseluruhan. Dari perspektif kebijakan pidana, upaya pencegahan terhadap kejahatan, termasuk penanggulangan cybercrime, tidak bisa dilakukan hanya dengan mengandalkan hukum pidana secara terpisah.

[50] Dwila Annisa Rizki Amalia, *et.al*. "Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism", Vol.3, No.2, 2021, hlm.232

Sebaliknya, pencegahan tersebut perlu dilakukan dengan pendekatan yang lebih sistematik dan terpadu.

Secara mendasar, politik atau kebijakan hukum pidana bertujuan untuk merumuskan hukum pidana dengan cara yang tepat, memberikan pedoman bagi pembuat undang-undang, serta memastikan penerapan hukum pidana yang efektif. Kebijakan legislatif memegang peranan penting dalam menentukan arah peraturan perundang-undangan pidana, karena tujuan yang ingin dicapai sudah harus ditetapkan sejak awal. Misalnya, dalam Pasal 26 ayat (2) UU ITE, ketentuan tersebut tidak memberikan sanksi pidana kepada pelaku, yang mana korban hanya bisa mengajukan gugatan secara perdata. Selain itu, Pasal 26 UU ITE hanya mencakup perlindungan dasar terhadap data pribadi. Para ahli teknologi informasi mengkritik Pasal 26 ini karena memiliki kekurangan, yaitu tidak memberikan perlindungan yang memadai bagi pengguna data pribadi yang digunakan untuk kepentingan tertentu oleh perusahaan. Keamanan data bertujuan untuk meningkatkan perlindungan data dengan cara: 1) Melindungi data agar tidak dapat diakses oleh pihak yang tidak berwenang; dan 2) Mencegah pihak yang tidak berwenang untuk memasukkan atau menghapus data.

Dalam kejahatan ini Indonesia memerlukan instrumen hukum yang lebih spesifik. Karena untuk saat ini hukum yang ada di indonesia terkhususnya dalam KUHP (Kitab Undang Undnag Hukum Pidana) hanya mengatur tentang kejahatan Pencurian, Penipuan, pemerasan dan pengamcan. Dalam hal tersebut telah diatur didalam Pasal 335, 362, 378 KUHP.

Pasal 335 KUHP mengatur mengenai tindak pidana perbuatan tidak menyenangkan, khususnya yang berkaitan dengan pemaksaan kehendak secara melawan hukum, yang disertai ancaman atau kekerasan. Pasal ini sering digunakan dalam konteks hukum pidana untuk menindak tindakan-tindakan seperti pengancaman, intimidasi, atau pemaksaan, yang tidak secara eksplisit masuk ke dalam pasal-pasal khusus lainnya dalam KUHP. Namun, penerapan pasal ini sering menjadi sorotan karena dianggap memiliki unsur yang luas dan multitafsir, sehingga harus diterapkan secara hati-hati agar tidak menimbulkan

kriminalisasi yang berlebihan terhadap ekspresi atau perbedaan pendapat. Bunyi Pasal 335 KUHP:

"*Barang siapa secara melawan hukum memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu, dengan memakai kekerasan, sesuatu ancaman kekerasan, atau perbuatan lain, baik terhadap orang itu sendiri maupun orang lain, dihukum penjara selama-lamanya satu tahun atau denda sebanyak-banyaknya empat ribu lima ratus rupiah.*"

Dalam konteks kejahatan siber yang menggunakan *Artificial Intelligence* (AI), Pasal 335 KUHP bisa dikaitkan jika AI digunakan untuk: Mengirimkan ancaman otomatis kepada seseorang; Memaksa seseorang memberikan data pribadi melalui ancaman digital.

Kebijakan kriminalisasi sendiri adalah kebijakan yang menetapkan suatu tindakan yang sebelumnya tidak dianggap sebagai tindak pidana, menjadi tindak pidana. Keputusan untuk melakukan kriminalisasi atau dekriminalisasi harus didasarkan pada pertimbangan kebijakan tertentu yang memperhitungkan berbagai faktor, antara lain: 1) Keseimbangan antara metode yang digunakan dan hasil yang ingin dicapai; 2) Analisis biaya yang dikeluarkan dibandingkan dengan hasil yang diperoleh dalam mencapai tujuan yang ditetapkan; 3) Penelitian atau penafsiran terhadap tujuan yang ingin dicapai, dengan memperhatikan prioritas lain dalam pengalokasian sumber daya manusia; 4) Dampak sosial dari kriminalisasi dan dekriminalisasi, yang juga mempertimbangkan efek sekunder yang mungkin timbul.

Kebijakan hukum pidana dalam hukum positif Indonesia saat ini masih berada pada tahap awal dalam merespons perkembangan kejahatan siber berbasis Artificial Intelligence (AI). Instrumen utama yang digunakan dalam menangani cyber crime adalah Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang terakhir diubah dengan UU No. 1 Tahun 2024.

Secara umum, regulasi tersebut memang telah mengatur beberapa bentuk kejahatan siber seperti akses ilegal, peretasan, penyebaran informasi palsu, hingga pelanggaran data pribadi. Namun, dalam konteks AI-based cyber crime, hukum positif yang ada belum secara eksplisit mengatur mengenai peran, tanggung jawab hukum, atau batasan penggunaan kecerdasan buatan dalam tindak pidana siber. Misalnya, kejahatan dengan menggunakan deepfake, automated phishing, atau AI-driven malware masih sulit untuk diklasifikasikan secara tegas dalam kategori delik yang diatur KUHP atau UU ITE.

Dalam hal ini Indonesia masis memiliki kekosongan hukum yang mana *Artificial Intellegance* (AI) adalah entitas digital yang tidak memiliki status hukum yang jelas, sehingga sulit untuk menentukan siapa yang bertanggung jawab secara pidana atas tindakannya. Hal ini menimbulkan ketidakpastian hukum dan dapat menghambat upaya penegakan hukum.

Dari sudut pandang penulis, hal ini menunjukkan bahwa kebijakan hukum pidana yang ada masih belum memadai secara substansi dan teknis dalam menjawab kompleksitas kejahatan siber berbasis AI. Kekosongan hukum (legal vacuum) muncul karena sistem hukum Indonesia belum mengantisipasi perkembangan teknologi digital yang sangat cepat, khususnya dalam hal subjek hukum, pertanggungjawaban pidana, dan model pencegahan kejahatan digital yang menggunakan AI sebagai alat atau aktor.

Oleh karena itu, menurut penulis, diperlukan reformulasi kebijakan hukum pidana yang meliputi:Penyusunan regulasi baru atau revisi UU ITE yang secara eksplisit mengatur tindak pidana dengan keterlibatan AI; Penguatan kapasitas aparat penegak hukum dalam memahami teknologi AI dan cara kerjanya dalam kejahatan siber; Pembuatan standar etik dan legal terhadap penggunaan AI, termasuk dalam sektor publik dan korporasi; Pembentukan lembaga atau unit khusus yang menangani kejahatan digital berbasis teknologi tinggi. Dengan langkah-langkah tersebut, kebijakan hukum pidana diharapkan dapat lebih adaptif, komprehensif, dan efektif dalam menghadapi ancaman baru dari cyber crime berbasis AI di era transformasi digital.

B. Kebijakan Hukum Pidana dalam Upaya Menanggulangi *Artificial Intelegence Cyber Crime* dalam Hukum Positif yang Akan Datang

Teknologi yang ada dan terus berkembang menjadi bukti peradaban manusia maju dengan sangat pesat. Kehadiran teknologi tentu saja telah banyak membantu manusia dalam menjalankan kehidupan sehari-hari. Bahkan, kehadiran teknologi berangsur dapat menggantikan tugas manusia, sehingga tugas-tugas dapat dilakukan dengan efisien menggunakan bantuan teknologi. Kemampuan manusia dalam mengembangkan teknologi kemudian membawa perusahaan teknologi terus berinovasi menciptakan piranti-piranti baru dalam dunia teknologi. *Artificial Intelegence* atau kecerdasan buatan menjadi salah satu teknologi paling mutakhir dalam peradaban manusia saat ini. Kecerdasan buatan membawa masyarakat dapat mengerjakan pekerjaan secara mudah, sebab semua pekerjaan dapat dikerjakan oleh sistem tanpa harus dikendalikan secara manual oleh manusia. Namun, perkembangan teknologi termasuk masuknya piranti *Artificial Intelegence* bukan tanpa masalah. Perkembangan teknologi juga membawa masalah baru dalam ranah hukum pidana. Di mana perkembangan teknologi yang ada turut membawa jenis dan modus baru dalam kejahatan berbasis teknologi siber, atau *Cyber Crime*.

Terlepas dari tujuan teknologi dalam rangka meningkatkan efisiensi kehidupan masyarakat, namun kehadirannya bukan tak menimbulkan kejahatan baru. Saat ini, teknologi tidak selalu digunakan untuk kebaikan oleh masyarakat. Teknologi yang terus berkembang ditambah dengan kehadiran piranti automatisasi semacam *Artificial Intelegence* memungkinkan para pelaku kejahatan melakukan kejahatan siber dengan memanfaatkan *Internet of Things* dan media teknologi lainnya.[51] Kejahatan siber atau *Cyber Crime* mencakup berbagai tindakan ilegal yang dilakukan dengan menggunakan jaringan komputer dan internet, seperti *hacking*, penyebaran *malware*, pencurian data, penipuan internet, penyalahgunaan *Artificial Intelegence*, dan lain sebagainya.

[51] Intan Permata Sari, *et.al*. "Analisis Kebijakan Cyber Crime dalam Hukum Positif di Indonesia". *Journal of Law and Nation (JOLN)*. Vol. 3, No. 2. Mei 2024, hlm. 396.

Peningkatan angka kejahatan siber di Indonesia setiap tahunnya sangat tinggi. Hal ini kemudian mendorong Pemerintah Republik Indonesia membangun kerangka hukum yang lebih kuat dan relevan dalam rangka mengurangi angka kejahatan siber di Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi salah satu kerangka hukum awal dalam penanggulangan kejahatan siber. Undang-Undang tersebut kemudian diperbaharui pada 2016 karena beberapa pasalnya sudah tidak relevan dan butuh penambahan pasal baru melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Meskipun landasan hukumnya telah ada, namun implementasi undang-undang tersebut menghadapi berbagai tantangan.[52] Oleh sebab itulah perlu ada rekonstruksi terhadap produk hukum penanggulangan kejahatan siber yang ada dengan menyinkronkannya pada perkembangan hukum dan jenis kejahatan siber yang ada.

Produk hukum yang mengatur mengenai kecerdasan buatan hingga saat ini belum tersedia. Kekosongan hukum pada pengaturan mengenai kecerdasan buatan dan regulasi khusus mengenai penanggulangan kejahatan berbasis *Artificial Intelegence* menyebabkan kejahatan yang ada kemudian tidak dapat diakomodir dan diatur secara khusus dan rinci sesuai dengan porsi dan jenis kejahatannya.[53]

Perkembangan kecerdasan buatan dewasa ini telah merambah ke berbagai piranti dan digunakan dalam hampir semua sektor kehidupan mulai dari keuangan dan bisnis, teknik, gawai, penerbangan, transportasi, dan lain sebagainya. Akses kecerdasan buatan yang semakin mudah dan umum digunakan saat ini mulai digunakan dengan tujuan kejahatan. Beberapa bentuk kejahatan siber berbasis *Artificial Intelegence* yang marak terjadi saat ini antara lain seperti *Deepfake Fraud* (penggunaan algoritma AI untuk membuat video

[52] Mahrina, Joko Sasmito, Candra Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation", *Jurnal Pena Justisia: Media Komunikasi dan Kajian Hukum*, Vol. 21, No. 2, December 2022, hlm. 345.

[53] Nugroho, H.T. Wahyuni. "Tantangan Regulasi Kejahatan Siber di Indonesia: Perspektif Perkembangan Teknologi Kecerdasan Buatan". *Jurnal Hukum dan Teknologi.* Vol. 7, No. 2, hlm. 129.

palsu yang menyerupai seseorang), *AI- Generated Phising Emails* (pembuatan phising melalui email dengan tingat personalisasi yang sangat tinggi), dan *Identify Theft* (pencurian data pribadi dari media sosial untuk membuat identitas palsu menggunakan AI).[54] Tantangan utama dalam pemberantasan kejahatan siber berbasis kecerdasan buatan diakibatkan karena kurangnya regulasi yang spesifik, keterbatasan kemampuan dan pengetahuan aparat penegak hukum, serta minimnya infrastruktur teknologi dalam mendeteksi dan mencegah serangan siber.

Regulasi hukum pidana mengenai penanggulangan kejahatan siber berbasis *Artificial Intelegence* khususunya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi instrumen utama yang sangat penting. Namun, meskipun undang-undang sudah ada, tetapi pelaksanaannya belum mampu mengakomodir permasalahan yang ada. Beberapa keterbatasan dalam hukum positif dalam rangka penanggulangan kejahatan siber berbasis AI diantaranya ialah:

1. Ketiadaan regulasi khususnya AI *Cyber Crime*
2. Definisi dan ruang lingkup kejahatan siber dalam UU ITE cenderung bersifat umum, sehingga belum mampu mencakup kejahatan berbasis AI
3. Kurangnya kapasitas kemampuan aparat penegak hukum khususnya berkaitan dengan identifikasi dan penanganan kejahatan siber berbasis kecerdasan buatan.

Pembaharuan kebijakan hukum mengenai penanggulangan kejahatan siber dengan basis kecerdasan buatan saat ini sangat mendesak. Hal ini tentunya disebabkan karena adanya kekosongan hukum di mana belum ada regulasi yang mengatur secara detail dan rinci mengenai permasalahan kejahatan siber berbasis kecerdasan buatan di Indonesia. Kekosongan hukum yang mengatur mengenai kecerdasan buatan di Indonesia ini khususnya yang berkaitan dengan kedudukan tanggung jawab *Artificial Intelegence* dalam industri hukum di Indonesia. Kekosongan hukum dalam bidang AI inilah yang

[54] Smith, J. "AI and Fraud: The Rise of Deepfake Scams". *Cybersecurity Review*. Vol. 15, No. 3, hlm. 45-50.

menyebabkan banyak praktisi hukum masih memanfaatkan pengaturan yang berkaitan dengan regulasi bidang teknologi untuk menanggapi permasalahan di bidang kecerdasan buatan, salah satunya melalui Undang-Undang Informasi dan Transaksi Elektronik atau UU ITE.[55]

Berdasarkan permasalahan kekosongan hukum di bidang AI, perlu antisipasi dari segala kemungkinan yang bisa muncul akibat kurangnya regulasi di bidang kecerdasan buatan. Dalam regulasi baru ini nantinya diharapkan ada pertimbangan yang rinci dan jelas berkaitan dengan kedudukan *Artificial Intelegence* dalam pertanggungjawaban hukum. Secara eksplisit, kecerdasan buatan memang dapat melakukan perbuatan hukum layaknya subjek hukum yang ada. Namun dalam praktiknya, kecerdasan buatan merupakan sistem yang dibangun manusia dan tidak dapat berperan sebagai subjek hukum. Oleh sebab itulah diperlukan adanya penafsiran secara terperinci dalam regulasi hukum baru yang mengatur secara jelas mengenai kecerdasan buatan, khususnya dalam rangka penanggulangan kejahatan siber berbasis *Artificial Intelegence* dalam hukum Indonesia.[56]

Seperti yang diketahui bersama, *Artificial Intelegence* kedudukannya masih sangat kabur di Indonesia. Hanya Undang-Undang Informasi dan Transaksi Elektronik serta Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik saja yang mengatur bidang kecerdasan buatan. Pengaturan dalam dua produk hukum ini pun tidak menyebutkan kecerdasan buatan secara jelas, hanya diksi "Agen Elektronik" saja yang dijelaskan dalam kedua peraturan tersebut.

Regulasi mengenai *Artificial Intelegence* atau kecerdasan buatan belum diatur dalam Kitab Undang-Undang Hukum Pidana terbaru. Dalam KUHP terbaru, yang diatur hanyalah mengenai kejahatan siber atau *Cyber Crime* saja. Namun instrumen kejahatan siber dalam KUHP terbaru yang sudah disusun juga sangat penting sebagai salah satu instrumen hukum yang mengatur

[55] Ni Made Yordha Ayu Astiti. "*Strict Llliability of Artificial Intelegence*: Pertanggungjawaban Kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban". *Jurnal Magister Hukum Udayana.* Vol. 12, No. 4, Desember 2023, hlm. 969.

[56] Ni Made Yordha Ayu Astiti. *Op.cit*, hlm. 967.

kejahatan dengan menggunakan media teknologi dan internet. Regulasi baru dalam menghadapi kejahatan siber dalam Undang-Undang Nomor 1 Tahun 2023 tentang Hukum Pidana diantaranya seperti *hacking*, pencurian data, hingga penyebaran *malware*. Ini menunjukkan bahwa Undang-Undang Nomor 1 Tahun 2024 memiliki landasan hukum yang lebih kuat dibandingkan regulasi sebelumnya dengan menjelaskan unsur-unsur tindak pidana secara lebih rinci.[57]

Pasal-pasal dalam undang-undang tersebut mencakup berbagai kejahatan siber, termasuk akses ilegal dalam Pasal 332, serangan terhadap sistem informasi negara dalam Pasal 333, hingga pelanggaran pada sistem keuangan dan perbankan dalam Pasal 334. Sanksi yang ditetapkan tergolong berat, baik dalam bentuk pidana penjara hingga denda besar, guna menciptakan efek jera. Sebagai contoh, akses ilegal yang melibatkan pelanggaran sistem pengamanan dapat dipidana hingga 8 tahun, sementara pelanggaran yang berkaitan dengan informasi rahasia pemerintah dapat mencapai hukuman penjara 12 tahun.[58]

Penelitian ini menyoroti bahwa regulasi dalam Undang-Undang Nomor 1 Tahun 2024 dirancang untuk menghadapi kompleksitas dan dinamika kejahatan siber yang terus berkembang. Selain itu, perlindungan terhadap sektor keuangan dan perbankan juga diperkuat melalui sanksi yang signifikan. Analisis yuridis menunjukkan bahwa undang-undang ini memberikan landasan hukum yang lebih jelas untuk menangani kejahatan siber yang memiliki sifat lintas batas dan berkembang pesat. Ini artinya bahwa Undang-Undang Nomor 1 Tahun 2023 yang direncanakan akan segera berlaku telah memberikan kerangka hukum yang lebih komprehensif dalam melindungi masyarakat dari kejahatan siber. Dengan revisi dan reformasi hukum yang berkelanjutan, regulasi ini diharapkan mampu mengikuti perkembangan teknologi dan modus

[57] Yosua Hia. "Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan Siber dalam KUHP Baru (UU Nomor 1 Tahun 2023)". *Jurnal SELISIK*. Vol. 10, No. 1, Juni 2024, hlm. 158.

[58] Yosua Hia. *Op.cit*, hlm. 161-163.

kejahatan modern, sehingga menciptakan lingkungan digital yang lebih aman di Indonesia.

Kehadiran Undang-Undang Nomor 1 Tahun 2024 yang mengatur kejahatan siber secara komprehensif menjadi pijakan penting untuk pengembangan regulasi di masa depan, khususnya dalam menghadapi tantangan baru terkait kejahatan yang melibatkan *Artificial Intelligence* (AI). Dengan pesatnya perkembangan teknologi AI, modus operandi kejahatan siber semakin kompleks, mulai dari serangan otomatis melalui bot hingga manipulasi data menggunakan algoritma cerdas. Dalam konteks ini, pembaharuan hukum positif menjadi sangat mendesak agar sistem hukum dapat mengantisipasi dan menanggulangi ancaman yang muncul.

Urgensi pembaharuan regulasi terkait AI dalam *Cyber Crime* terletak pada kemampuan teknologi ini untuk mempercepat, memperluas, dan menyembunyikan jejak kejahatan. AI dapat digunakan untuk menciptakan *malware* adaptif, *deepfake*, hingga manipulasi data yang sangat sulit dideteksi. Dalam hukum positif yang ada, seperti UU ITE atau KUHP baru, belum ada pengaturan eksplisit mengenai penggunaan AI untuk tujuan kriminal. Hal ini menciptakan kekosongan hukum yang dapat dimanfaatkan oleh pelaku kejahatan. Oleh karena itu, revisi regulasi yang ada harus memasukkan elemen-elemen spesifik tentang AI dalam tindak pidana siber.

Pembaharuan yang diperlukan meliputi penambahan ketentuan mengenai kejahatan yang melibatkan pengembangan, penggunaan, atau distribusi teknologi AI untuk tujuan ilegal. Misalnya, regulasi perlu mengatur secara khusus tentang pembuatan *Deepfake* untuk penipuan, penggunaan AI untuk serangan pada infrastruktur kritis, dan manipulasi pasar melalui algoritma cerdas. Selain itu, penting untuk mendefinisikan tanggung jawab hukum bagi pengembang dan pengguna AI yang tidak bertanggung jawab, termasuk mekanisme audit algoritma dan sanksi pidana yang sesuai.

Gambaran pembaharuan hukum juga harus mencakup kolaborasi internasional, mengingat sifat lintas batas dari kejahatan siber berbasis AI. Indonesia dapat belajar dari negara-negara lain yang telah mulai mengatur

teknologi ini, seperti Uni Eropa dengan *Artificial Intelligence Act* atau pendekatan Amerika Serikat melalui undang-undang yang mengatur keamanan data berbasis AI. Pembaharuan hukum di Indonesia harus menekankan pada integrasi standar global, pemantauan algoritma, dan pengembangan kapasitas penegak hukum untuk menangani kasus AI *Cyber Crime.* Dengan pembaharuan ini, sistem hukum Indonesia tidak hanya menjadi responsif terhadap tantangan teknologi modern, tetapi juga menciptakan kerangka hukum yang adil dan relevan. Hal ini sejalan dengan tujuan Undang-Undang Nomor 1 Tahun 2024, yaitu memberikan perlindungan hukum yang lebih kuat bagi masyarakat di era digital. Langkah ini juga mencerminkan visi hukum progresif yang tidak hanya bereaksi terhadap ancaman, tetapi juga proaktif dalam menciptakan ruang digital yang aman dan adil.

Meskipun pengaturan mengenai kejahatan siber telah ada dan dibuat dengan lebih rinci dalam KUHP terbaru. Namun hal tersebut tidak membuat kecerdasan buatan tidak perlu dibuatkan regulasinya. Produk hukum undang-undang dan turunannya tetap diperlukan hadir dalam mengatur *Artificial Intelegence Cyber Crime* atau kejahatan siber berbasis kecerdasan buatan. Kekosongan hukum yang saat ini terjadi sangat berdampak terhadap penegakan hukum dan upaya preventif yang bisa dilakukan oleh pemerintah, penegak hukum, serta praktisi hukum. Kekosongan hukum juga dikhawatirkan dapat menyebabkan terjadinya peningkatan angka penyalahgunaan *Artificial Intelegence* untuk berbagai jenis kejahatan siber dan kejahatan lainnya di Indonesia. Oleh sebab itulah diperlukan rekonstruksi hukum yang bertujuan menghadirkan pembaharuan hukum pidana yang mengatur secara jelas, rinci, dan lengkap mengenai *Artificial Intelegence* dan penegakan hukumnya.

Berdasarkan penjelasan di atas dan dengan melihat fakta hukum dan fakta dalam masyarakat yang saat ini terjadi, terdapat beberapa rekomendasi hukum untuk melakukan pembaharuan hukum penanggulangan *Artificial Intelegence Cyber Crime* khususnya di wilayah hukum Indonesia. Pembaharuan hukum dan tindakan yang dapat dilakukan secepatnya antara lain sebagai berikut:

1. Pembentukan Undang-Undang *Artificial Intelegence*

   Hingga saat ini, Indonesia masih belum memiliki produk hukum yang secara spesifik mengatur mengenai *Artificial Intelegence*. Tanpa adanya regulasi khusus yang mengatur mengenai kecerdasan buatan, sangat sulit untuk membedakan penggunaan *Artificial Intelegence* yang sah dan diperbolehkan serta yang dilarang dalam konteks kejahatan siber. Dalam Undang-Undang *Artificial Intelegence* tersebut, nantinya terdapat beberapa hal yang harus diatur. Beberapa hal yang direkomendasikan untuk diatur dalam undang-undang tersebut diantaranya:

   a. Definisi dan ruang lingkup *Artificial Intelegence*
   b. Tanggung jawab hukum jika AI digunakan sebagai media dan alat melakukan kejahatan
   c. Pengawasan dan audit teknologi yang memerlukan lembaga atau badan negara khusus guna memastikan pengembangan dan penggunaan AI berjalan sesuai dengan norma hukum yang berlaku.

2. Revisi Undang-Undang Informasi dan Transaksi Elektronik

   Sebagai payung hukum utama dalam penegakan hukum dan penanggulangangan kejahatan siber, undang-undang ini memerlukan revisi dan pembaharuan hukum di dalamnya. UU ITE yang saat ini ada dan berlaku tidak secara khusus mengatur mengenai kecerdasan buatan. Hal inilah yang kemudian menyebabkan adanya kekosongan hukum dalam penegakan *Artificial Intelegence* dalam konteks kejahatan siber. Dalam perubahan yang dilakukan terhadap Undang-Undang ITE harus ada pengaturan yang lebih jelas lagi mengenai pasal yang menjelaskan tentang jenis kejahatan siber berbasis AI sekaligus bentuk penegakan hukumnya.

3. Peningkatan Teknologi Forensik Digital

   Kejahatan siber sangat sulit untuk dilacak, apalagi kejahatan siber yang menggunakan *Artificial Intelegence* sebagai media kejahatannya. Oleh sebab itulah teknologi forensik digital di Indonesia perlu mendapatkan *upgrade.* Kejahatan siber dengan kecerdasan buatan sangat sulit untuk dideteksi, hal ini berkaitan erat dengan sifat dari *Artificial*

Intelegence yang anonim, sehingga sangat sulit untuk mengetahui siapa yang bertanggung jawab atas kejahatan yang terjadi. Beberapa hal yang dapat dilakukan dalam rangka meningkatkan kemampuan forensik digital aparat penegak hukum di Indonesia diantaranya dengan:

a. Peningkatan infrastruktur digital forensik di Indonesia. Hal ini dapat dilakukan dengan menyediakan perangkat lunak dan perangkat keras yang mampu mendeteksi, menganalisis, dan melacak aktivitas *Artificial Intelegence* dalam suatu kejahatan siber yang terjadi.[59]
b. Kerja sama dengan lembaga internasional guna mengadopsi teknologi digital forensik yang mereka gunakan sehingga Indonesia bisa mendapatkan transfer teknologinya.

4. Kerja Sama Internasional

Kerja sama internasional dengan negara lain sangat diperlukan dalam penegakan hukum dan penanggulangan kejahatan siber berbasis kecerdasan buatan. Hal ini didasarkan karena kejahatan siber seringkali bersifat lintas negara dan lintas bangsa. Oleh sebab itulah penanganan kejahatan siber berbasis kecerdasan buatan membutuhkan kolaborasi antarnegara. Pembuatan perjanjian ekstradisi pelaku kejahatan siber serta ikut berpartisipasi secara aktif dalam forum internasional misalnya melalui *Global Forum on Cyber Expertise* menjadi strategi kerja sama yang dapat dilakukan oleh Indonesia ke depannya.

5. Penguatan Edukasi dan Literasi Digital

Penguatan literasi dan edukasi digital kepada masyarakat menjadi langkah yang sangat penting untuk dilakukan. Hal ini disebabkan karena masyarakat yang kurang memahami teknologi khususnya *Artificial Intelegence* seringkali menjadi korban kejahatan siber. Sehingga strategi penguatan literasi digital bagi masyarakat sangat penting dilakukan dengan cara melakukan kampanye nasional tentang literasi digital dan

[59] Casey, E. 2011. *"Digital Evidence and Computer Crime: Forensic Science, Computers, and The Internet (3rd edision)"*. Academic Press.

Artificial Intelegence serta dengan membuat modul *Artificial Intelegence* di sekolah untuk mengedukasi masyarakat sejak usia dini.[60]

Rekomendasi di atas dapat dituangkan dalam kebijakan-kebijakan pemerintah baik melalui pembaharuan hukum dan peraturan perundang-undangan maupun melalui program pemerintah. Tujuan dari dilakukannya tindakan dan pembaharuan hukum terhadap penanggulangan dan penegakan hukum *Artificial Intelegence Cyber Crime* di atas pada dasarnya ialah untuk menciptakan regulasi yang adaptif dengan perkembangan teknologi yang semakin maju di tengah-tengah masyarakat saat ini. Dengan langkah-langkah di atas, harapannya Indonesia akan semakin *melek* dengan perkembangan teknologi yang terjadi serta mampu mengatasi dan menanggulangi kejahatan siber berbasis kecerdasan buatan yang semakin banyak kejadiannya.

Pengaturan mengenai penyalahgunaan kecerdasan buatan (AI) dalam kejahatan siber telah menjadi perhatian di beberapa negara maju. Di Uni Eropa, *Artificial Intelligence Act* dirancang untuk mengatur penggunaan AI berdasarkan tingkat risikonya, dengan kategori khusus untuk teknologi berisiko tinggi yang dapat membahayakan keamanan masyarakat atau hak asasi manusia.[61] Regulasi ini mewajibkan audit menyeluruh terhadap algoritma, transparansi pengoperasian, serta pemberlakuan sanksi berat bagi pelanggaran yang terjadi. Sementara itu, Amerika Serikat melalui *Algorithmic Accountability Act* menekankan tanggung jawab pengembang AI untuk memastikan teknologi mereka tidak disalahgunakan, termasuk perlindungan terhadap diskriminasi data atau eksploitasi keamanan digital.[62] Di Tiongkok, pemerintah memiliki regulasi ketat mengenai keamanan data dan penggunaan teknologi AI, seperti kewajiban perusahaan untuk menyertakan mekanisme pencegahan risiko dalam setiap produk berbasis AI.

---

[60] Livingstone, S., Helsper, E.J. "Gradations in Digital Inclusion: Children, Young People, and the Digital Devide". *New Media & Society.* Vol. 9, No. 4, hlm. 671-696.

[61] European Commission. *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://eur-lex.europa.eu. Dikutip pada 7 Desember 2024.

[62] U.S. Congress. *Algorithmic Accountability Act of 2019*. https://www.congress.gov. Dikutip pada 7 Desember 2024.

Indonesia dapat mengadaptasi beberapa elemen penting dari regulasi di negara-negara tersebut. Pertama, penerapan audit menyeluruh untuk teknologi AI sebelum diluncurkan, sebagaimana dilakukan Uni Eropa, dapat membantu memastikan bahwa teknologi yang beredar aman dari potensi penyalahgunaan. Kedua, pengembangan kebijakan tanggung jawab pengembang AI, seperti di Amerika Serikat, memungkinkan sanksi hukum diterapkan pada produsen teknologi yang gagal mengantisipasi celah keamanan atau penyalahgunaan produk mereka. Terakhir, pendekatan Tiongkok yang terpusat pada perlindungan data dan keamanan digital dapat menjadi inspirasi dalam membentuk regulasi yang komprehensif untuk mencegah eksploitasi data oleh teknologi AI.

Selain itu, Indonesia perlu mendorong kerja sama internasional dalam merancang regulasi ini, seperti inisiatif *Global Partnership on Artificial Intelligence* (GPAI) yang bertujuan memperkuat kolaborasi global untuk pengaturan dan pengembangan teknologi AI secara etis dan aman. Dengan adaptasi yang tepat dari praktik internasional, Indonesia dapat membentuk kerangka hukum yang lebih responsif terhadap risiko kejahatan siber berbasis kecerdasan buatan.

Pemerintah Republik Indonesia sejatinya telah mengeluarkan Surat Edaran Nomor 9 Tahun 2023 tentang Etika Kecerdasan Buatan yang di dalamnya berisi mengenai pengaturan penggunaan kecerdasan buatan secara khusus serta pedoman dalam penggunaan AI di Indonesia.[63] Selain itu, beberapa hal mengenai kecerdasan buatan juga telah diatur dalam Undang-Undang Perlindungan Data Pribadi yang bisa mempengaruhi penggunaan kecerdasan buatan. Kemudian terdapat pula pada Strategi Nasional Kecerdasan Buatan (SNKI).[64]

---

[63] Hukum Online, Menakar Prospek Pengaturan Artificial Intelligence di Indonesia https://www.hukumonline.com/berita/a/menakar-prospek-pengaturan-artificial-intelligence-diindonesia/ Diakses 7 Desember 2024.

[64] Nur Aliya. R, Muhammad Aksay, Muhammad Firdaus. A. "Urgensi Pembuatan Regulasi Penggunaan AI (Artificial Intelegence) di Indonesia". *Jurnal Penegakan Hukum Indonesia (JPHI).* Vol. 5, No. 1, hlm. 48.

Dalam rangka menangani dan menegakkan hukum *Artificial Intelegence Cyber Crime* di Indonesia, pemerintah diharapkan dapat segera membentuk regulasi yang secara khusus mengatur mengenai hal tersebut. Jika didasarkan atas permasalahan yang ada, perlu Undang-Undang tentang Penggunaan dan Pengawasan Kecerdasan Buatan dalam sistem hukum nasional Indonesia. Dibuatnya peraturan perundang-undangan ini bertujuan sebagai landasan hukum dan pondasi penting dalam penanganan dan penegakkan hukum *Artificial Intelegence Cyber Crime* di Indonesia yang saat ini belum diatur. Dengan dibentuknya Undang-Undang tentang Penggunaan dan Pengawasan Kecerdasan Buatan diharapkan akan ada landasan hukum yang kuat dalam pengaturan pengembangan, penggunaan, serta pengawasan teknologi AI sekaligus penanggulangan potensi adanya penyalahgunaan kecerdasan buatan untuk membantu manusia melakukan kejahatan.

Undang-Undang tentang Penggunaan dan Pengawasan Kecerdasan Buatan juga diharapkan mencakup berbagai aspek penting. Beberapa aspek penting yang diharapkan diatur dalam undang-undang ini diantaranya ialah:

1. Ketentuan umum

   Ketentuan umum berfungi untuk mendefinisikan konsep utama dari kejahatan siber dengan basis kecerdasan buatan, ruang lingkup kejahatan siber berbasis AI, dan hal-hal lain dalam bidang kecerdasan buatan yang masih membutuhkan definisi secara lebih jelas untuk menghindari kontradiksi dalam memahami kecerdasan buatan dan undang-undang ini.

2. Prinsip-Prinsip Penggunaan AI

   Pengaturan mengenai prinsip penggunaan kecerdasan buatan di sini termasuk juga pengaturan mengenai sertifikasi teknologi AI bagi pengembang atau *Developer* sistem. Selain itu, pengaturan mengenai tanggung jawab hukum penyalahgunaan dan kejahatan dengan kecerdasan buatan juga harus dibuat. Tujuannya ialah untuk memastikan sistem kecerdasan buatan yang dibuat oleh pengembang dapat berjalan dengan baik, aman digunakan, serta dapat diminimalisir kemungkinannya digunakan untuk berbuat kejahatan.

3. Pengawasan terhadap Teknologi Kecerdasan Buatan

Pengawasan pengembangan dan penggunaan kecerdasan buatan harus dilakukan dengan membentuk lembaga khusus yang bertugas melakukan audit secara berkala dalam rangka memastikan kecerdasan buatan yang dibuat dapat dijalankan dengan baik dan sesuai dengan etika hukum dan norma hukum yang dibuat. Keberadaan lembaga pengawas juga penting guna memberikan perlindungan data pribadi masyarakat pengguna sistem, aplikasi, atau piranti yang menggunakan kecerdasan buatan, serta evaluasi terhadap risiko keamanan kecerdasan buatan.

4. Rincian Jenis-Jenis Kejahatan Siber Berbasis AI

Undang-Undang tentang Penggunaan dan Pengawasan Kecerdasan Buatan perlu merinci secara jelas mengenai jenis-jenis kejahatan siber berbasis kecerdasan buatan, seperti pembuatan *deepfake* dalam modus kejahatan penipuan atau pembuatan *malware* dengan memenfaatkan AI, serta lain sebagainya.

5. Sanksi atau Hukuman bagi Pihak yang Menyalahgunakan AI

Sebagai salah instrumen hukum pidana, tentunya Undang-Undang tentang Penggunaan dan Pengawasan Kecerdasan Buatan juga harus mengatur jenis hukuman dan sanksi yang diberikan kepada pihak-pihak yang menyalahgunakan kecerdasan buatan untuk melakukan kejahatan siber dan kejahatan lainnya.

6. Pencegahan dan Penanggulangan Kejahatan Siber

Dalam bidang pencegahan dan penanggulangan kejahatan siber berbasis kecerdasan buatan ini diperlukan pengaturan secara jelas mengenai tanggung jawab perusahaan penyedia layanan kecerdasan buatan jika terjadi penyalahgunaan atau kegagalan dalam mengamakan produk yang dibuatnya.

7. Literasi dan Edukasi Digital

Perlu dilakukan pendidikan, pelatihan, ataupun kampanye mengenai pemanfaatan kecerdasan buatan dalam kehidupan sehari-hari. Bukan

hanya itu, dalam edukasi juga perlu disampaikan mengenai penyalahgunaan kecerdasan buatan dan penanggulangannya agar masyarakat tidak menjadi pelaku ataupun korban dari kejahatan siber berbasis kecerdasan buatan yang semakin marak.

Pemerintah Indonesia harus bertindak proaktif dan strategis dalam menghadapi ancaman ini. Langkah pertama adalah meningkatkan kapasitas literasi digital masyarakat. Kampanye edukasi tentang risiko teknologi AI dan cara mengenali ancaman siber harus dilakukan secara luas untuk memperkuat ketahanan masyarakat terhadap serangan. Selanjutnya, pemerintah perlu memperkuat infrastruktur keamanan siber nasional. Pembentukan pusat komando khusus yang memanfaatkan teknologi AI untuk mendeteksi dan merespons ancaman secara *real-time* menjadi kebutuhan mendesak. Kolaborasi dengan sektor swasta dan pakar teknologi juga diperlukan untuk memastikan pertahanan siber yang komprehensif.

Kerangka hukum yang baik untuk menanggulangi kejahatan siber berbasis AI harus mencakup tiga aspek utama: regulasi preventif, penegakan hukum yang efektif, dan perlindungan hak-hak masyarakat. Pertama, regulasi preventif harus mencakup kewajiban bagi pengembang AI untuk memastikan teknologi mereka tidak disalahgunakan. Misalnya, pemerintah dapat mengadopsi pendekatan Uni Eropa yang mewajibkan audit risiko sebelum AI diluncurkan ke pasar. Aturan ini dapat mencakup ketentuan mengenai transparansi algoritma, pengujian keamanan, dan kewajiban pelaporan insiden.

Kedua, kerangka hukum harus memberikan wewenang yang jelas kepada lembaga penegak hukum untuk menangani kejahatan siber berbasis AI. Hal ini mencakup pelatihan khusus bagi aparat penegak hukum untuk memahami teknologi AI, serta pemberian alat dan teknologi yang memadai untuk menyelidiki kasus kejahatan siber. Terakhir, kerangka hukum harus memastikan perlindungan hak asasi manusia, termasuk privasi dan kebebasan informasi. Regulasi harus seimbang,

sehingga tidak menciptakan pengawasan berlebihan yang dapat melanggar hak-hak masyarakat.

Rekonstruksi dan pembaharuan hukum pidana yang mengatur mengenai kejahatan siber yang menggunakan sistem kecerdasan buatan sebagai alat kejahatan menjadi sebuah hal yang penting. Pemerintah harus segera mengambil tindakan untuk mengisi kekosongan hukum tentang kecerdasan buatan yang saat ini terjadi. Jika kekosongan hukum mengenai penanggulangan kejahatan siber menggunakan *Artificial Intelegence* dibiarkan terus terjadi, yang ditakutkan ialah penegakkan hukum terhadap kasus serupa tidak dapat dilakukan dengan baik.

Pembaharuan hukum yang mengatur kecerdasan buatan di Indonesia dilakukan agar sistem hukum nasional lebih responsif dalam menghadapi perkembangan teknologi, masyarakat, dan modus kejahatan yang selalu berkembang setiap saat. Selain itu, dengan kehadiran peraturan perundang-undangan yang mengatur mengenai penggunaan dan pengawasan kecerdasan buatan di Indonesia akan menciptakan kerangka hukum yang lebih adil, bermanfaat, dan relevan dengan kebutuhan masyarakat saat ini dan di masa yang akan datang.

Risiko peningkatan dan perkembangan kejahatan siber berbasis kecerdasan buatan di masa yang akan datang harus diimbangi dengan upaya aktif pemerintah dalam membentuk kebijakan yang mengatur permasalahan tersebut. Bukan hanya pemerintah, aparat penegak hukum juga dituntut terus melakukan *upgrade* terhadap perkembangan jenis kejahatan yang ada agar penanganan kejahatan dapat dilakukan dengan baik dan adil. Selain itu, masyarakat sebagai subjek hukum yang rentan menjadi pelaku ataupun korban juga harus memahami bagaimana pemanfaatan kecerdasan buatan yang baik dan memahami bagaimana norma hukum dalam pemanfaatan kecerdasan buatan tersebut supaya terhindar dari risiko penyalahgunaan kecerdasan buatan baik sebagai korban atau justru sebagai pelaku tindak kejahatan tersebut.


UNIVERSITAS ISLAM SULTAN AGUNG
UNISSULA
جامعة سلطان أجونج الإسلامية

BAB IV
PENUTUP

A. Kesimpulan

Berdasarkan dari hasil penilitian dapat di simpulkan sebagai berikut:

1. Kebijakan hukum pidana dalam hukum positif Indonesia saat ini belum sepenuhnya mampu mengakomodasi kompleksitas dan perkembangan kejahatan siber (cyber crime) yang melibatkan teknologi Artificial Intelligence (AI). Meskipun beberapa ketentuan dalam KUHP dan UU ITE telah mengatur jenis-jenis tindak pidana siber secara umum, namun belum ada pengaturan yang secara spesifik dan komprehensif mengatur peran serta dampak dari penggunaan AI dalam kejahatan digital. Ketiadaan regulasi yang eksplisit mengenai AI sebagai alat maupun subjek yang berkontribusi dalam tindak pidana siber menimbulkan kekosongan hukum yang dapat melemahkan upaya penegakan hukum dan perlindungan terhadap masyarakat.
2. Dalam hukum positif ke depan, diperlukan kebijakan hukum pidana yang secara eksplisit mengatur tentang bentuk, pertanggungjawaban, serta sanksi pidana terhadap kejahatan yang melibatkan teknologi AI, baik sebagai alat maupun sebagai pelaku melalui sistem otomatisasi. Selain itu, penting pula untuk memperkuat kapasitas aparat penegak hukum, memperjelas standar etik penggunaan AI, serta membangun kerangka hukum yang mampu mengantisipasi risiko dan dampak sosial dari penggunaan AI secara tidak bertanggung jawab.

B. Saran

Seiring dengan meningkatnya potensi penyalahgunaan teknologi Artificial Intelligence (AI) dalam kejahatan siber, diperlukan langkah-langkah konkret dari pembentuk undang-undang dan pemangku kepentingan di bidang hukum untuk segera melakukan penyesuaian terhadap kebijakan hukum pidana yang berlaku saat ini. Beberapa saran yang dapat penulis ajukan antara lain:

1. Perlu dilakukan pembaruan regulasi yang secara khusus mengatur kejahatan siber yang melibatkan teknologi AI, baik dalam hal klasifikasi tindak pidana, bentuk pertanggungjawaban pidana, maupun mekanisme pembuktiannya.
2. Penegak hukum perlu diberikan pelatihan dan peningkatan kapasitas agar mampu memahami karakteristik kejahatan berbasis AI serta menerapkan hukum pidana secara tepat, adil, dan sesuai dengan perkembangan teknologi.
3. Kolaborasi antara negara, akademisi, sektor swasta, dan masyarakat harus ditingkatkan guna membangun kesadaran hukum digital serta menciptakan sistem perlindungan hukum yang kuat terhadap risiko AI dalam ruang siber.

SSDAFTAR PUSTAKA

Buku :

Brenner, S. W. 2010. *Cybercrime: Criminal threats from cyberspace*. Praeger.

A. S.T. Kansil, 1989, *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*, Jakarta: Balai Pustaka.

Casey, E. 2011. *"Digital Evidence and Computer Crime: Forensic Science, Computers, and The Internet (3rd edision)"*. Academic Press.

Kaharuddin, & Haq, Z. A. (2024). Kecerdasan buatan dan aspek perlindungan hukum di era digitalisasi. Prenada Media.

Moeljatno. 2002. *Asas-asas Hukum Pidana*. Jakarta: PT Rineka Cipta.

Philipus M. Hadjon. 2007. *Perlindungan Hukum bagi Rakyat Indonesia: Sebuah Studi tentan Prinsip-Prinsipnya, Penanganannya oleh Peradilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara.* Surabaya: Peradaban.

Satjipto Rahardjo. 2000. Hukum dan Perubahan Sosial: Suatu Tinjauan Teoritis serta Pengalaman-Pengalaman di Indonesia. Jakarta: Genta Publishing.

Sutan Remy Sjahdeini. *Kejahatan Siber: Cybercrime*. Jakarta: Pustaka Utama Grafiti, 2003, hlm. 12-15.

Wall, D. S. 2007. *Cybercrime: The transformation of crime in the information age*. Polity Press.

Peraturan Perundang-Undangan

Undang-Undang ITE Nomor 1 Tahun 2024 perubahan atas Undang Undang ITE No 11 Tahun 2008

Pasal 1 ayat (3) Undang Undang Dasar Tahun 1945

UU Nomor 6 Tahun 2023 perubahan atas Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang Nomor 28 Tahun 2014 perubahan atas Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta

Undang-Undang Nomor 5 Tahun 2018 perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Terorisme

Kitab Undang Undang Hukum Pidana (KUHP)

Pasal 335 ayat (1) KUHP tentang Perbuatan Tidak Menyenangkan

Pasal 362 KHP tentang Pencurian

Pasal 378 KUHP tentang Penipuan

Jurnal :

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber crime dalam sudut pandang hukum pidana. Jurnal Kewarganegaraan, 6(1), hlm.2173.

Amalia, D. A. R., et al. (2021). Kebijakan hukum pidana dalam upaya penanggulangan cyber terorism. Jurnal Nama, 3(2), 232.

Bibit Santoso, "Menata Kebijakan Publik Yang Tepat Agar Tidak Terjadi Gejolak Di Masyarakat Bila Diundangkan" vol.13, no.1, hlm.39.

Budianto, Rafi Septia, dan Noenik Soekorini. "Tindak Pidana Cyber Crime dan Penegakan Hukumnya." Binamulia Hukum, vol. 12, no. 2, 2023, hlm.292

Febri Jaya dan Wilton Goh, "Analisis Yuridis Terdahap Kedudukan Kecerdasan Buatan Atau Artificial Intelligence Sebagai Subjek Hukum Pada Hukum Positif Indonesia", *Jurnal Supremasi Hukum*, Edisi Vol. 17 No.02, Juli 2021, hlm. 2

Intan Permata Sari, *et.al*. "Analisis Kebijakan Cyber Crime dalam Hukum Positif di Indonesia". *Journal of Law and Nation (JOLN)*. Vol. 3, No. 2. Mei 2024, hlm. 396.

Izil Hidayat Putra, "Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan Perundang-Undangan", vol.1, no.2, hlm.112

Livingstone, S., Helsper, E.J. "Gradations in Digital Inclusion: Children, Young People, and the Digital Devide". *New Media & Society.* Vol. 9, No. 4, hlm. 671-696.

Mahrina, Joko Sasmito, Candra Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation", *Jurnal Pena Justisia: Media Komunikasi dan Kajian Hukum*, Vol. 21, No. 2, December 2022, hlm. 345.

Marsella, dkk, "Analisis Implementasi Artificial Intelligence Untuk Bisnis: Supanto, dkk "Regulasi Penyimpangan Artificial Intelligence Pada Tindak

Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016", vol.9, no.2, hlm.132

Miftakhur Rokhman Habibi, Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangan dalam Sistem Hukum Indonesia". *Jurnal Al-Qanun: Pemikiran dan Pembaharuan Hukum Islam.* Vol. 23, No.2. Desember 2020. Hlm. 407.

Ni Made Yordha Ayu Astiti. "*Strict Llliability of Artificial Intelegence*: Pertanggungjawaban Kepada Pengatur AI ataukah AI yang Diberikan Beban Pertanggungjawaban". *Jurnal Magister Hukum Udayana.* Vol. 12, No. 4, Desember 2023, hlm. 969.

Nugroho, H.T. Wahyuni. "Tantangan Regulasi Kejahatan Siber di Indonesia: Perspektif Perkembangan Teknologi Kecerdasan Buatan". *Jurnal Hukum dan Teknologi.* Vol. 7, No. 2, hlm. 129.

Nur Aliya. R, Muhammad Aksay, Muhammad Firdaus. A. "Urgensi Pembuatan Regulasi Penggunaan AI (Artificial Intelegence) di Indonesia". *Jurnal Penegakan Hukum Indonesia (JPHI).* Vol. 5, No. 1, hlm. 48.

Yosua Hia. "Analisa Yuridis Pasal-Pasal Khusus Terkait Kejahatan Siber dalam KUHP Baru (UU Nomor 1 Tahun 2023)". *Jurnal SELISIK.* Vol. 10, No. 1, Juni 2024, hlm. 158.

Smith, J. "AI and Fraud: The Rise of Deepfake Scams". *Cybersecurity Review.* Vol. 15, No. 3, hlm. 45-50.

Supanto, dkk "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016", Vol.9, No.2, Hlm.132

Systematic Literature Review", vol.4, no.2, hlm.134

Tri Wahyudi, "Studi Kasus Pengembangan dan Penggunaan Artificial Intelligence (AI) Sebagai Penunjang Kegiatan Masyarakat Indonesia", vol.9, no.1, hlm.29

Kasim, Z. (2023). Kebijakan hukum pidana untuk penanggulangan cyber crime di Indonesia. Jurnal Nama, 2(1), 20.

Website :

Ahmad Sudi Pratikno, "Implementasi Artificial Intelligence Dalam Memetakan Karakteristik, Kompetensi, dan Perkembangan Psikologi Siswa Sekolah Dasar Melalui Platform Offline", terdapat dalam https://scholar.google.co.id/citations?view_op=view_citation&hl=id&use

r=-FbwaL4AAAAJ&citation_for_view=-FbwaL4AAAAJ:d1gkVwhDpl0C

European Commission. *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://eur-lex.europa.eu.

Giovani Dio Prasasti, "Wamenkominfo : 22,1 Persen Pekerja di Indonesia Sudah Mulai Menggunakan AI", https://www.liputan6.com/tekno/read/5467690/wamenkominfo-221-persen-pekerja-diindonesia-sudah-mulai-pakai-ai?page=2.

Hukum Online, Menakar Prospek Pengaturan Artificial Intelligence di Indonesia https://www.hukumonline.com/berita/a/menakar-prospek-pengaturan-artificial-intelligence-diindonesia/.

Kaplan, A. M., & Haenlein, M. (2019). Siri, Siri in my hand, who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62(1), 15-

U.S. Congress. *Algorithmic Accountability Act of 2019*. https://www.congress.gov.