

**PERTANGGUNGJAWABAN PIDANA PENGGUNAAN TEKNOLOGI  
*ARTIFICIAL INTELLIGENCE* PADA TINDAK PIDANA PEMALSUAN  
IDENTITAS DIGITAL**

**Skripsi**

Diajukan Sebagai Salah Satu Persyaratan untuk memperoleh  
Gelar Sarjana Strata Satu (S-1) Ilmu Hukum  
Program Kekhususan Hukum Pidana



Diajukan Oleh:

**Ela Zuyinatul Ilma**

**NIM: 30302200099**

**PROGRAM STUDI (S.1) ILMU HUKUM  
FAKULTAS HUKUM  
UNIVERSITAS ISLAM SULTAN AGUNG (UNISSULA)  
SEMARANG**

**2025**

**HALAMAN PERSETUJUAN**

**ANALISIS YURIDIS MENGENAI PERTANGGUNGJAWABAN PIDANA**  
**DALAM PENGGUNAAN TEKNOLOGI *ARTIFICIAL INTELLIGENCE***  
**(AI) UNTUK TINDAK PIDANA PEMALSUAN IDENTITAS DIGITAL**  
**(DEEPPFAKE)**



Telah disetujui oleh:

Pada Tanggal, 14 November 2025

Dosen Pembimbing:



**Dr. Andi Aina Ilmih, S.H., M.H.**  
**NIDN. 0906068001**

**HALAMAN PENGESAHAN**  
**PERTANGGUNGJAWABAN PIDANA PENGGUNAAN TEKNOLOGI**  
**ARTIFICIAL INTELLIGENCE PADA TINDAK PIDANA PEMALSUAN**  
**IDENTITAS DIGITAL**

Diperiapkan dan disusun oleh

**Ela Zuyinatul Ilma**

**NIM: 30302200099**

Telah dipertahankan didepan Tim Penguji

Pada tanggal: 19 November 2025

Dan dinyatakan telah memenuhi syarat dan lulus

**Tim Penguji:**

**Ketua**

**Dr. Ratih Mega Puspa Sari, S.H, M.Kn**

**NIDN:0624108504**

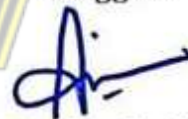
**Anggota**



**Dr. Denny Suwondo, S.H, M.H**

**NIDN : 0617106301**

**Anggota**



**Dr. Andi Aina Ilmih, S.H, M.H**

**NIDN : 0906068001**

Mengetahui,

Dekan Fakultas Hukum Unissula


**Prof. Dr. H. Jawade Hafidz, S.H, M.H.**  
**NIDN : 06.2004.6701**

## **MOTTO DAN PERSEMBAHAN**

### **MOTTO**

**Kelak kamu akan mengingat apa yang kukatakan kepadamu. Aku menyerahkan urusanku kepada Allah. Sesungguhnya Allah Maha Melihat hamba-hamba-Nya**

**(QS. Ghafir40: Ayat 44)**

**Balas dendam yang terbaik adalah mengubah dirimu menjadi lebih baik**

**(Ali Bin Abi Thalib)**

**“Untuk menggapai apa yang kamu inginkan, kamu harus terus mengejar dan berjuang untuk mewujudkannya. Kemudian pada saat yang sama juga jaga dirimu dan kesehatanmu”**

**(Park Chanyeol-EXO)**

### **PERSEMBAHAN**

Tiada lembar yang paling indah dari karya ini selain ucapan Alhamdulillah, dengan segala rasa Syukur atas kehadiran Allah SWT yang telah memberikan rahmat serta karunia-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi ini. Serta sebagai ucapan terimakasih karya ini dipersembahkan untuk:

1. Kedua Orang tua saya, yaitu Bapak Abdul Ghofir dan Ibu Nur Fitriyah yang sangat saya banggakan dan sangat saya sayangi karena tiada hentinya melangitkan doa baiknya serta memberikan dukungan dalam memperjuangkan masa depan dan kebahagiaan putrinya. Terimakasih sudah mengantarkan saya sampai ke tempat ini. Saya persembahkan karya tulis sederhana ini dan gelar ini untuk Bapak dan Ibu tercinta.
2. Adik saya yaitu Dhinni Apriliani dan keluarga saya, karena telah memberikan doa, semangat, serta dukungan materiil maupun moral agar saya dapat terus meraih apa yang saya cita-citakan.
3. Diri saya sendiri, Ela Zuyinatul Ilma. Terima kasih sudah bertahan sejauh ini, memilih untuk bangkit dan menyelesaikan semua ini. Terima kasih karena memutuskan untuk tidak menyerah sesulit apapun proses penyusunan karya ini dan telah menyelesaikannya sebaik dan semaksimal mungkin walaupun ada berbagai tekanan di luar keadaan, ini merupakan pencapaian yang patut dirayakan untuk diri sendiri. Berbahagialah selalu di manapun berada, kamu hebat, Ela. Apapun kurang dan lebihmu mari meryakan diri sendiri.



## SURAT PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda tangan dibawah ini :

Nama : Ela Zuyinatul Ilma

NIM : 30302200099

Program Studi : S-1 Ilmu Hukum

Fakultas : Hukum

Dengan ini menyerahkan karya ilmiah berupa Skripsi dengan

**“PERTANGGUNGJAWABAN PIDANA PENGGUNAAN TEKNOLOGI  
ARTIFICIAL INTELLIGENCE PADA TINDAK PIDANA PEMALSUAN  
IDENTITAS DIGITAL”** dan menyetujui menjadi hak milik Universitas Islam  
Sultan Agung serta memberikan Hak Bebas Royalty Non Eksklusif untuk disimpan,  
dialih mediakan, dalam pangkalan data, dan dipublikasinya 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 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.

Semarang, 19 November 2025

Yang Menyatakan

  
Ela Zuyinatul Ilma  
30302200099

## **SURAT PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH**

Saya yang bertanda tangan dibawah ini :

Nama : Ela Zuyinatul Ilma

NIM : 30302200099

Program Studi : S-1 Ilmu Hukum

Fakultas : Hukum

Dengan ini menyerahkan karya ilmiah berupa Skripsi dengan

**“PERTANGGUNGJAWABAN PIDANA PENGGUNAAN TEKNOLOGI  
ARTIFICIAL INTELLIGENCE PADA TINDAK PIDANA PEMALSUAN  
IDENTITAS DIGITAL”** dan menyetujui menjadi hak milik Universitas Islam  
Sultan Agung serta memberikan Hak Bebas Royalty Non Eksklusif untuk disimpan,  
dialih mediakan, dalam pangkalan data, dan dipublikasinya 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 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.

Semarang, 19 November 2025

Yang Menyatakan



Ela Zuyinatul Ilma  
30302200099

## KATA PENGANTAR

Assalamualaikum Wr.Wb

Bsimillahirrohmanirrohim. Segala puji dan Syukur penulis haturkan kepada Allah SWT atas kehadiran-Nya, atas limpahan Rahmat dan Hidayah serta Karunia-Nya, sehingga Penulis dapat menyelesaikan skripsi yang berjudul **“PERTANGGUNGJAWABAN PIDANA PENGGUNAAN TEKNOLOGI *ARTIFICIAL INTELLIGENCE* PADA TINDAK PIDANA PEMALSUAN IDENTITAS DIGITAL”** tanpa kesulitan sedikitpun.

Shalawat serta salam tidak lupa Penulis sampaikan kepada, Nabi Agung Muhammad SAW. Yang telah membawa kita semua umat manusia dari gelapnya dunia, menuju dunia yang terang seperti sekarang ini, Nabi Muhammad SAW yang telah dinantikan syafaatnya di yaumul qiyamah nanti. Adapun tujuan dari penyusunan skripsi ini guna untuk memenuhi persyaratan dalam memperoleh gelar Sarjana Hukum Satu (S-1) serta merupakan persyaratan akhir Penulis untuk menyelesaikan Program Studi Ilmu Hukum di Universitas Islam Sultan Agung (UNISSULA) Semarang.

Penulis menyadari bahwa dalam penyusunan skripsi ini, ada banyak pihak yang berkontribusi untuk memberikan dukungan dan semangat penuh kepada Penulis atas penyelesaian studi dan tugas akhir ini. Oleh karena itu, dengan tulus dan rasa penuh hormat Penulis mengucapkan terimakasih dan mendoakan semoga Allah memberikan balasan yang terbaik kepada:

1. Bapak Prof. Dr. H. Gunarto, S.H., S.E., Akt., M.Hum. selaku Rektor Universitas Islam Sultan Agung Semarang.
2. Bapak Prof. Dr. H. Jawade Hafidz, S.H., M.H. selaku Dekan Fakultas Hukum Universitas Islam Sultan Agung Semarang
3. Ibu Dr. Hj. Widayati, S.H., M.H. selaku Wakil Dekan I Fakultas Hukum Universitas Islam Sultan Agung Semarang
4. Bapak Dr. Denny Suwondo, S.H., M.H. selaku Wakil Dekan II Fakultas Hukum Universitas Islam Sultan Agung Semarang
5. Bapak Dr. Muhammad Ngaziz, S.H., M.H. selaku Ketua Program Studi S1 Fakultas Hukum Universitas Islam Sultan Agung Semarang
6. Ibu Dr. Ida Musofiana, S.H., M.H. selaku Sekretaris Program Studi S1 Fakultas Hukum Universitas Islam Sultan Agung Semarang
7. Ibu Dini Amalia Fitri, S.H., M.H. selaku Sekretaris Program Studi S1 Fakultas Hukum Universitas Islam Sultan Agung Semarang
8. Ibu Dr. Hj. Widayati, S.H., M.H. selaku Dosen Wali Studi Fakultas Hukum Universitas Islam Sultan Agung Semarang
9. Ibu Dr. Andi Aina Ilmih, S.H., M.H. selaku Dosen Pembimbing Skripsi Fakultas Hukum Universitas Islam Sultan Agung Semarang



Sebagai manusia Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari kata kesempurnaan karena keterbatasan kemampuan dan ilmu pengetahuan yang dimiliki Penulis. Oleh karena itu atas kesalahan ataupun kekurangan, Penulis memohon maaf dan bersedia menerima masukan/kritikan.

Kemudian Penulis berharap besar skripsi ini dapat bermanfaat bagi kalangan siapapun yang membaca dan menyerap isi yang ada di dalamnya. Sekian dan Terimakasih.

*Wassalamualaikum Wr. Wb.*



## DAFTAR ISI

Cover .....	i
HALAMAN PERSETUJUAN .....	Error! Bookmark not defined.
HALAMAN PENGESAHAN .....	Error! Bookmark not defined.
MOTTO DAN PERSEMBAHAN .....	iii
SURAT PERNYATAAN KEASLIAN SKRIPSI...Error! Bookmark not defined.	
SURAT PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH Error! Bookmark not defined.	
KATA PENGANTAR .....	vii
ABSTRAK .....	xii
ABSTRAK .....	xiii
BAB I PENDAHULUAN .....	1
A. Latar Belakang .....	1
B. Rumusan Masalah .....	11
C. Tujuan Penelitian .....	11
D. Kegunaan Penelitian .....	12
E. Terminologi .....	14
F. Metodologi Penelitian .....	25
G. Sistematika Penulisan .....	28
BAB II TINJAUAN PUSTAKA .....	31
A. Tinjauan Umum Pertanggungjawaban Pidana .....	31
1. Pengertian Pertanggungjawaban Pidana .....	31
2. Dasar Pertanggungjawaban Pidana .....	34
3. Unsur-unsur Pertanggungjawaban Pidana .....	35
4. Subjek Pertanggungjawaban Pidana dalam Konteks Tindak Pidana Siber .....	48
B. Tinjauan Umum Teknologi <i>Artificial Intelligence</i> .....	49
1. Pengertian Umum <i>Artificial Intelligence</i> .....	49
2. Regulasi Mengenai <i>Artificial Intelligence</i> .....	52

3. Sejarah <i>Artificial Intelligence</i> .....	53
4. Cabang <i>Artificial Intelligence</i> .....	57
5. Penerapan <i>Artificial Intelligence</i> dalam Berbagai Bidang.....	62
C. Tinjauan Umum Tindak Pidana Pemalsuan .....	65
1. Pengertian Umum Tindak Pidana Pemalsuan.....	65
2. Peraturan Perundang-Undangan dan Jenis-jenis Tindak Pidana Pemalsuan .....	67
3. Unsur-Unsur Dalam Tindak Pidana Pemalsuan .....	69
4. Perkembangan Tindak Pidana Pemalsuan Dalam Era Digital.....	72
D. Tinjauan Umum Identitas Digital.....	74
1. Konsep dan Pengertian Identitas Digital .....	74
2. Dasar Hukum Identitas Digital di Indonesia .....	77
E. Tinjauan Umum Pemalsuan Identitas Digital atau <i>Deepfake</i> .....	78
1. Pengertian dan Mekanisme <i>Deepfake</i> .....	78
2. Regulasi Hukum Terkait Teknologi <i>Deepfake</i> .....	82
BAB III HASIL PENELITIAN DAN PEMBAHASAN.....	84
A. Bentuk Tindak Pidana Pemalsuan Identitas Digital <i>Deepfake</i> di Ruang Digital Menggunakan Teknologi <i>Artificial Intelligence</i> Menurut Hukum Positif di Indonesia .....	84
B. Bentuk Pertanggungjawaban Pidana Terhadap Pelaku yang Menggunakan Teknologi <i>Artificial Intelligence</i> Untuk Melakukan Pemalsuan Identitas Digital <i>Deepfake</i> Menurut Hukum Positif di Indonesia? .....	97
A. Kesimpulan .....	127
B. Saran.....	128
DAFTAR PUSTAKA.....	129

## ABSTRAK

Perkembangan teknologi kecerdasan buatan atau *Artificial Intelligence* telah membawa dampak signifikan terhadap kehidupan manusia, termasuk munculnya fenomena baru berupa tindak pidana pemalsuan identitas digital atau *deepfake*, yaitu teknologi yang memanfaatkan algoritma pembelajaran mendalam menggunakan sistem deep learning untuk memanipulasi identitas seseorang melalui gambar, video, atau suara sehingga tampak autentik. Penggunaan identitas yang ada di ruang digital tanpa izin yang mengarah pada pemalsuan identitas digital menimbulkan berbagai permasalahan hukum, terutama terkait perlindungan data pribadi, keaslian identitas, dan pertanggungjawaban pidana pelaku. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis bentuk tindak pidana pemalsuan identitas digital atau *deepfake* menggunakan teknologi *Artificial Intelligence* dalam perspektif hukum positif Indonesia serta memahami dan menganalisis bentuk pertanggungjawaban pidana bagi pelaku tindak pidana pemalsuan identitas digital yang menggunakan teknologi *Artificial Intelligence* menurut hukum positif Indonesia.

Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan atau *statute approach*, dan *konseptual conceptual approach*. Sumber bahan hukum terdiri atas bahan hukum primer, sekunder, dan tersier yang dianalisis melalui studi pustaka.

Hasil penelitian menunjukkan bahwa tindak pidana yang memalsukan identitas digital dapat dikategorikan sebagai tindak pidana manipulasi data elektronik sebagaimana diatur dalam Pasal 35 Jo. Pasal 51 ayat (1) UU ITE, serta dapat dijerat dengan Pasal 27A, 27B, 28 UU Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE, Pasal 263 dan 378 KUHP, serta Pasal 65 sampai 68 UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pertanggungjawaban pidana dapat dibebankan kepada pelaku langsung baik pembuat maupun penyebar *deepfake*, dengan mempertimbangkan unsur kesengajaan atau *mens rea* dan perbuatan melawan hukum atau *actus reus*. Penelitian ini merekomendasikan perlunya pembentukan aturan khusus mengenai manipulasi identitas digital berbasis *Artificial Intelligence* untuk memberikan kepastian hukum, memperjelas tanggung jawab korporasi dan pengembang teknologi, serta memperkuat mekanisme penegakan hukum melalui peningkatan kapasitas forensik digital dan kerja sama internasional. Serta pendekatan preventif bagi masyarakat dengan literasi digital dan etika dalam berteknologi. Sehingga hukum pidana diharapkan mampu beradaptasi terhadap kemajuan teknologi tanpa mengabaikan prinsip keadilan dan perlindungan hak asasi manusia.

**Kata Kunci:** *Artificial Intelligence, Deepfake, Pertanggungjawaban Pidana.*

## **ABSTRAK**

*The development of artificial intelligence (AI) technology has had a significant impact on human life, including the emergence of a new phenomenon in the form of digital identity forgery, or deepfake. This technology utilizes deep learning algorithms to manipulate a person's identity through images, videos, or voices to appear authentic. The unauthorized use of identities in the digital space, leading to digital identity forgery, raises various legal issues, particularly related to personal data protection, identity authenticity, and the criminal liability of perpetrators. This study aims to identify and analyze the forms of digital identity forgery, or deepfake, using AI technology from the perspective of Indonesian positive law. It also aims to understand and analyze the forms of criminal liability for perpetrators of digital identity forgery using AI technology under Indonesian positive law.*

*The research method used is a normative juridical approach with a statute approach, and a conceptual approach. The legal sources consist of primary, secondary, and tertiary legal materials analyzed through literature review.*

*The research results show that the crime of deepfake that falsifies digital identity can be categorized as a crime of electronic data manipulation as regulated in Article 35 Jo. Article 51 paragraph (1) of the ITE Law, and can be charged with Articles 27A, 27B, 28 of Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, Articles 263 and 378 of the Criminal Code, and Articles 65 to 68 of Law Number 27 of 2022 concerning Personal Data Protection. Criminal liability can be imposed on the direct perpetrator, both the creator and disseminator of deepfake, by considering the elements of intent or mens rea and unlawful acts or actus reus. This research recommends the need to establish special regulations regarding Artificial Intelligence-based digital identity manipulation to provide legal certainty, clarify the responsibilities of corporations and technology developers, and strengthen law enforcement mechanisms through increased digital forensic capacity and international cooperation. As well as a preventive approach for the community with digital literacy and ethics in technology. Thus, criminal law is expected to be able to adapt to technological advances without ignoring the principles of justice and protection of human rights.*

**Keywords: Artificial Intelligence, Deepfake, Criminal Liability.**



# BAB I

## PENDAHULUAN

### A. Latar Belakang

Pada era digitalisasi ini pertumbuhan teknologi informasi dan komunikasi di Indonesia berjalan dengan sangat cepat dan dinamis. Seiring waktu, terdapat inovasi yang memberikan perbedaan konkrit dalam kehidupan masyarakat di dalam ranah teknologi serta informasi, yang berlangsung tanpa henti dan tanpa batasan. Teknologi ini membawa berbagai manfaat yang besar bagi peningkatan kesejahteraan dan kemajuan bangsa, serta memudahkan penyaluran informasi dan pengetahuan dari seluruh negara di dunia dengan melampaui batas waktu dan ruang. Namun, terdapat hal yang harus diwaspadai mengenai dampak negatif. Peningkatan kejahatan yang memanfaatkan berbagai metode dalam kemajuan teknologi dan informasi telah menyebabkan pergeseran nilai-nilai moral, dan norma sosial, yang kerap kali bertolak belakang dengan tatanan kehidupan masyarakat yang berlaku.

Dampak negatif dari perkembangan teknologi salah satunya berupa tindak pidana yang dilakukan di ruang digital. Kejahatan siber adalah salah satu wujud pelanggaran hukum yang semakin marak terjadi dan meluas di dunia maya. Kejahatan siber ini, yang dikenal sebagai *Cyber Crime*, yakni bentuk baru dari kriminalitas di era digital yang sangat bergantung pada kemajuan teknologi. Kejahatan siber bersifat universal dan multidimensi, meliputi berbagai aspek kegiatan di dunia maya, serta memberikan dampak negatif yang nyata terhadap kehidupan manusia sehari-hari. Banyak tindak kejahatan siber

digunakan sebagai alat untuk melakukan pelecehan seksual, penyebaran berita palsu atau *hoax*, penipuan dan pemalsuan identitas digital, serta tindak pidana dalam bidang pornografi. Fenomena ini telah menjadi ancaman serius terhadap stabilitas keamanan nasional, sehingga pemerintah menghadapi tantangan besar dalam mengimbangi teknik-teknik kriminal yang semakin canggih dan dilakukan menggunakan teknologi komputer.

Perkembangan teknologi di negara lain maupun di Indonesia sangat cepat dan menimbulkan berbagai perubahan dalam kehidupan manusia. Pada era revolusi industri 5.0, fokus utama peradaban tidak lagi bertumpu pada aspek *cyber physical* semata, melainkan beralih pada fungsi manusia sebagai agen kegiatan yang menggunakan teknologi, informasi, dan komunikasi di berbagai aspek kehidupan. Era ini tidak hanya menitikberatkan pada interaksi antar mesin dan sistem robotik atau *machine to machine*, tetapi juga menekankan hubungan timbal balik antara manusia dan mesin.<sup>1</sup> Teknologi kecerdasan buatan atau yang biasa disebut dengan istilah *Artificial Intelligence* merupakan salah satu hasil dari perkembangan di era digitilasisasi.

Di Indonesia, teknologi ini disebut sebagai kecerdasan buatan, sebuah bidang ilmu komputer yang terfokus pada perancangan sistem dan mesin yang dapat menjalankan tugas-tugas yang memerlukan kecerdasan manusia. *Artificial Intelligence* atau sering disebut dengan AI mempergunakan algoritma dan model matematis untuk memungkinkan komputer dan sistem lain belajar

---

<sup>1</sup> Ahmad M. Ramli “Pentingnya Bangsa Ini Mulai Adaptif Dengan Industri 5.0”, <https://www.republika.co.id/berita/qynv2n371/pentingnya-bangsa-ini-mulai-adaptif-dengan-industri-50> diakses pada 26 Januari 2025.

dari data, mengidentifikasi pola, dan mengambil keputusan yang cerdas. AI yang dilengkapi dengan kemampuan *deep learning* dirancang untuk belajar dari data yang spesifik dan eksak, dan diharapkan dapat diterapkan pada berbagai aktivitas dan tugas yang umumnya dikerjakan oleh manusia, di antaranya pemahaman bahasa, pengenalan pola, pemrosesan data, dan analisis. Tingkat akurasi bahkan dapat melebihi kemampuan manusia.<sup>2</sup>

Perkembangan teknologi kecerdasan buatan atau AI memberikan perbedaan yang mendasar dalam beragam sektor kehidupan, terutama di ranah komunikasi maupun media digital. Namun, pemanfaatan teknologi ini juga sering disalahgunakan oleh penjahat siber dalam praktik yang dikenal sebagai *Artificial Intelligence-Crime*.<sup>3</sup>

Salah satu bentuk inovasi yang muncul akibat dari praktik kejahatan siber yaitu teknologi *deepfake* yang bermakna suatu teknik manipulasi media berbasis AI yang mampu mengganti wajah, suara, dan gerakan seseorang dengan tingkat realisme yang sangat tinggi. Oleh karena itu, sulit untuk menentukan apakah suatu konten tersebut asli atau palsu.

Pemalsuan identitas digital atau sering dikenal *deepfake*, awalnya dikembangkan untuk tujuan positif seperti industri perfilman, hiburan, atau edukasi. Namun, dalam perkembangannya, teknologi ini banyak

---

<sup>2</sup> Ranti Fauza Mayana, et.al, 2024, Legal Issues of *Artificial Intelligence* – Generated Works: Challenges on Indonesian Copyright Law, *Law Reform*, Vol, 20, No. 1, hlm. 55.

<sup>3</sup> Dwi Fitri. Ade Nur Hidayah. Et al., 2025, Deepfake Dan Krisis Kepercayaan; Analisis Hukum Terhadap Penyebaran Konten Palsu di Media Sosial, *JIIIC: Jurnal Intelek Insan Cendekia*, Vol. 2, No 6, hlm. 1157.

disalahgunakan untuk kepentingan yang merugikan, seperti penyebaran hoaks, pemerasan, fitnah, hingga pornografi non-konsensual.

Di Indonesia, kejadian ini muncul tidak hanya di ranah entertainment, melainkan dalam modus kejahatan, seperti pemalsuan suara tokoh publik hingga konten ekstremis yang mendistorsi identitas asli seseorang.<sup>4</sup> Kondisi tersebut menunjukkan bahwa *deepfake* memiliki potensi besar dan akan terus meningkat sebagai sarana pemalsuan identitas digital yang membahayakan integritas informasi dan reputasi seseorang.

Perkembangan teknologi AI yang tidak bisa dihindari oleh semua lapisan di masyarakat dalam setiap negara tentu menjadi alasan utama bagi suatu negara untuk menetapkan regulasi hukum khusus yang mengatur penggunaan AI. Saat ini ketentuan hukum pidana Indonesia belum mengatur secara rinci tentang tindak pidana di ruang siber, khususnya penyalahgunaan teknologi AI yang dipakai dalam tindak pidana *deepfake*.

Di Indonesia regulasi mengenai teknologi secara spesifik didalam ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau kerap disebut UU ITE. Namun,UU ITE tidak secara jelas mendefinisikan AI. Dengan pertumbuhan teknologi AI yang cukup cepat,

---

<sup>4</sup> Desty Aster Yansen. B et al, 2025 Kriminalisasi Pelanggaran Protokol Digital Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake di Media Sosial, *INNOVATIVE: Journal Of Social Science Research*, Vol. 5, No. 4 Page 386-398.

berbagai pendapat muncul di berbagai bidang mengenai definisi AI yang sesuai dengan ketentuan teknis UU ITE sebagaimana diterapkan di Indonesia.<sup>5</sup>

Dalam proses penegakan hukum terhadap kejahatan *deepfake* menggunakan teknologi kecerdasan buatan (AI), instrumen hukum lain yang dapat dijadikan acuan meliputi Kitab Undang-Undang Hukum Pidana (KUHP) yang lama, Kitab Undang-Undang Hukum Pidana Nasional (UU No. 1 Tahun 2023), dan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP Act). Meskipun peraturan-peraturan ini dapat digunakan sebagai dasar hukum, mereka masih dianggap belum cukup untuk mengatasi berbagai hambatan yang timbul akibat perkembangan pesat teknologi AI, utamanya dalam memberantas tindak pidana yang melibatkan penggunaan teknologi AI.<sup>6</sup>

Dalam penerapannya kasus *deepfake* sering menimbulkan interpretasi yang beragam, baik dalam menentukan unsur delik, mengidentifikasi pelaku, maupun menjatuhkan sanksi. Beberapa permasalahan utama meliputi ketidakjelasan pertanggungjawaban pidana, di mana pelaku sering kali sulit dilacak karena teknik *deepfake* melibatkan banyak pihak, seperti pengembang AI, pengguna, dan penyedia platform. Lebih jauh lagi, kompleksitas teknologi ini memunculkan kesulitan dalam pembuktian di pengadilan, karena dibutuhkan keahlian forensik digital yang memadai untuk memastikan keaslian atau manipulasi suatu konten. Hal ini mengakibatkan proses penegakan hukum

---

<sup>5</sup> Shofika Hardiyanti.Q. Safira Ayuni. et al., 2024, Kedudukan dan Konsep Pertanggungjawaban *Artificial Intelligence* Dalam Hukum Positif Indonesia, *UNES Law Review*, Vol. 6, No. 4 hlm. 12690.

<sup>6</sup> Gayatri Kusuma. et.al., 2024 “Ius Constituendum: Pengaturan *Artificial Intelligence* sebagai Upaya Anti Cyber Laundering dalam Mekanisme Central Bank Digital Currency (CBDC),” *Jurnal Pendidikan Tambusai*, Vol. 8, no. 2 hlm. 23887.



berjalan lambat dan seringkali korban tidak memperoleh perlindungan hukum yang optimal. UU ITE juga yang menjadi dasar hukum penanganan kejahatan siber perlu ditinjau kembali dan disesuaikan dengan perkembangan teknologi, termasuk AI.<sup>7</sup>

Seiring berjalannya waktu, masyarakat akan semakin terpapar pada informasi yang tidak dapat dipercaya, yang dapat merusak reputasi individu dan mengganggu kepercayaan masyarakat. Fenomena ini memerlukan perhatian dari beragam pemangku kepentingan, terutama pemerintah, penegak hukum, dan masyarakat sipil, untuk bersama-sama mencari solusi yang dapat melindungi individu dari inovasi teknologi tanpa mengorbankan inovasi dan kemajuan teknologi. Fenomena ini telah menjadi perhatian global, terutama setelah beberapa kasus penyalahgunaan teknologi *deepfake* yang merugikan individu dan masyarakat.

Di Indonesia, kasus penyalahgunaan teknologi *deepfake* semakin kerap terjadi. Terdapat beberapa contoh tindak pidana yang menggunakan teknologi *deepfake* yang pernah muncul di Indonesia yaitu kejahatan penipuan yang dialami beberapa artis seperti Melaney Ricardo, Rafi Ahmad, dan Najwa Shihab.<sup>8</sup>

Kasus pemalsuan identitas juga pernah diungkap oleh Wakil Presiden Direktur PT Bank Central Asia (BCA), Hendra Lembong. Dalam wawancara

---

<sup>7</sup> Dwi Fitri, Ade Nur Fidayah. et al., 2025, Deepfake Dan Krisis Kepercayaan; Analisis Hukum Terhadap Penyebaran Konten Palsu Di Media Sosial, *JIIC: Jurnal Intelek Insan Cendekia*, Vol. 2 No. 6, hlm. 1158.

<sup>8</sup> Nila Tiara.A.M.J., 2024, Analisis Pendekatan Ekonomi Hukum Terhadap Kriminalisasi *Deepfake*, *Literasi Sintaks: Jurnal Ilmiah Indonesia*, Jilid. 9

yang dilakukan pada 26 Juli 2023, ia menjelaskan bahwa seseorang yang menggunakan teknologi AI untuk memanipulasi foto pada KTP yang dijadikan alat verifikasi dalam proses pengajuan kredit.

Menyadari semakin maraknya penggunaan teknologi *deepfake* yang dapat mengancam privasi, reputasi, dan keamanan finansial masyarakat. Maka penelitian tentang pertanggungjawaban pidana dalam penggunaan teknologi *deepfake* untuk pemalsuan identitas digital menjadi sangat mendesak untuk segera dilakukan. Kondisi ini juga berkaitan dengan kesenjangan hukum yang terjadi, dimana UU ITE dan KUHP kita belum secara spesifik mengatur tentang pertanggungjawaban hukum terhadap pelaku pemalsuan identitas digital melalui *deepfake*.

Apabila dilihat dari aspek filosofis, teknologi ini telah melanggar prinsip keadilan substantif karena mempersulit pembuktian unsur kesalahan dalam hukum pidana. Penggunaan *deepfake* berseberangan dengan asas-asas hak dasar manusia menuntut perlindungan martabat, kejujuran, dan keadilan. Konten palsu yang dibuat tanpa izin dapat merusak harga diri dan reputasi korban, sehingga mewajibkan sistem hukum untuk mampu melindungi hak-hak esensial tersebut.

Konsep keadilan sebagai pilar utama dalam filsafat hukum menjadi landasan penting dalam mengatur pertanggungjawaban pidana terhadap pelaku kejahatan ini, agar keadilan sosial tetap ditegakkan dan hak-hak warga negara terlindungi secara adil. Sedangkan dalam aspek sosiologis, dampaknya telah merusak tatanan sosial melalui penyebaran informasi palsu yang masif.

Keberadaan *deepfake* mampu mempengaruhi norma-norma sosial mengenai kepercayaan dan keaslian informasi di masyarakat. Fenomena ini berpotensi menimbulkan keresahan, menurunkan tingkat kepercayaan terhadap media dan informasi, serta memperparah penyebaran disinformasi yang dapat mengancam stabilitas sosial dan kepercayaan publik terhadap institusi dan individu. Hal ini menuntut adanya penelitian mengenai pertanggungjawaban pidana dalam tindakan penyalahgunaan AI dalam tindak pidana teknologi *deepfake*. Tidak hanya normatif formal namun juga responsif terhadap realitas sosial dan budaya masyarakat, agar tercipta harmoni yang berkesinambungan antara perlindungan untuk hak individu dan kepentingan sosial secara umum.

Hingga saat ini, studi akademik mengenai aspek yuridis *deepfake* dan pertanggungjawaban pidana dalam konteks hukum Indonesia masih sangat terbatas. Banyak kajian yang lebih banyak membahas aspek teknologi dan etika, namun minim penelitian yang secara khusus mengkaji bagaimana sistem hukum pidana Indonesia mampu menghadapi dan mengatur pertanggungjawaban pidana terhadap pelaku kejahatan *deepfake* melalui teknologi AI.

Dalam studi yang dilakukan oleh Bogren dan Hussein, penelitian ini hanya mengkaji mengenai adanya kesenjangan dalam wacana media sosial serta pandangan terkait isu-isu etika yang muncul dalam penggunaan teknologi *deepfake*. Penelitian tersebut menempatkan fenomena *deepfake* dalam kerangka etika AI yang lebih luas.

Hasil studi menunjukkan banyak kekhawatiran, antara lain terkait penyebaran informasi palsu, ketidakpercayaan yang semakin meningkat, dan

kekhawatiran akan penyalahgunaan teknologi dan aplikasi berbahaya. Selain itu, studi ini juga menunjukkan terdapat kekhawatiran terhadap pelanggaran prinsip-prinsip etika yang telah ditetapkan, seperti martabat manusia, transparansi, privasi, dan prinsip non-kejahatan, yang berpotensi dilanggar oleh penggunaan teknologi *deepfake*. Dalam penelitian sebelumnya juga terdapat penelitian yang membahas mengenai penyalahgunaan teknologi AI dan pertanggungjawaban pidananya.

Beberapa penelitian sebelumnya antara lain, sebuah studi yang berjudul “Pengaturan Hukum Pidana di Indonesia Terhadap Penyalahgunaan Teknologi *Artificial Intelligence Deepfake* Dalam Melakukan Tindak Pidana *Cybercrime*” yang ditulis oleh Patricia Morisa Banfatin, Karolus Kopong Medan, Debi F.Ng. Fallo.<sup>9</sup>

Kedua penelitian yang memiliki judul Kedudukan dan Konsep Pertanggungjawaban *Artificial Intelligence* Dalam Hukum Positif Indonesia yang ditulis oleh Shofika Hardiyanti Qurrahman, Safira Ayunil, Tsabita Aurelia Rahim.<sup>10</sup> Terakhir, yaitu penelitian berjudul “Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan *Artificial Intelligence* di Indonesia” yang ditulis oleh Muhammad Tan Abdul Rahman Haris dan Tantimin<sup>11</sup>.

---

<sup>9</sup> Patricia Morisa Banfatin, et al., 2025, Pengaturan Hukum Pidana di Indonesia Terhadap Penyalahgunaan Teknologi *Artificial Intelligence Deepfake* Dalam Melakukan Tindak Pidana *Cybercrime*, *Jurnal Pemuliaan Keadilan*, Vol. 2, No. 1.

<sup>10</sup> Shofika Hardiyanti.Q., et al., 2024, Kedudukan dan Konsep Pertanggungjawaban *Artificial Intelligence* Dalam Hukum Positif Indonesia, *UNES Law Review*, Vol. 6, No. 4

<sup>11</sup> Muhammad Tan Abdul Rahman Haris & Tantimin, 2022, Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan *Artificial Intelligence* di Indonesia, *Jurnal Komunikasi Hukum*, Vol. 8 No. 1.

Namun didalam penelitian-penelitian tersebut hanya membahas pertanggung jawaban AI secara luas dan lebih umum. Sedangkan dalam penelitian ini akan mengkaji fenomena penyalahgunaan *Artificial Intelligence* yang lebih difokuskan pada pertanggungjawaban pidananya dalam penindakan tindak kejahatan *deepfake*.

Penelitian ini memiliki tujuan untuk menjabarkan dan menganalisis bentuk serta karakteristik tindak pidana pemalsuan identitas digital atau *deepfake* melalui teknologi *Artificial Intelligence* dalam perspektif hukum positif Indonesia. Serta menganalisis dasar hukum pertanggungjawaban pidana yang bisa dipakai dalam menjerat pelaku penyalahgunaan *deepfake* untuk tindak pidana pemalsuan identitas digital, termasuk unsur delik, bentuk kesalahan atau *mens rea*, dan subjek hukum yang bertanggung jawab. Bahkan dapat mengidentifikasi kelemahan regulasi yang ada mengenai penyalahgunaan teknologi *Artificial Intelligence* dalam *deepfake* dan juga membandingkan dengan kebijakan Internasional yang berguna untuk melihat regulasi dan kebijakan yang diterapkan di negara lain terkait aturan penyalahgunaan *Artificial Intelligence* dan *deepfake*, sehingga dapat memberikan pandangan yang lebih menyeluruh dan membantu Indonesia dalam merumuskan kebijakan yang lebih efektif.

Peneliti memiliki harapan agar riset mengenai fenomena ini dapat menghasilkan sebuah pemahaman yang semakin mendalam. pesifik mengenai pertanggung jawaban pidana dalam penyalahgunaan teknologi *Artificial Intelligence* yang digunakan untuk tindak pidana *deepfake*. Selain itu, peneliti



juga mengharapkan dengan adanya penelitian ini bisa memberikan panduan bagi para pengemban kebijakan, para penegak hukum, maupun para peneliti khususnya peneliti yang berfokus pada bidang teknologi dan hukum. Maka dari itu, peneliti akan membahas dan mengkaji fenomena ini melalui penelitian dengan judul “Pertanggungjawaban Pidana Penggunaan Teknologi *Artificial Intelligence* pada Tindak Pidana Pemalsuan Identitas Digital”.

## **B. Rumusan Masalah**

Berdasarkan penjelasan pada bagian latar belakang tersebut, penulis kemudian memberikan rumusan masalah sebagai berikut:

1. Bagaimana bentuk tindak pidana pemalsuan identitas digital *deepfake* di ruang digital menggunakan teknologi AI menurut hukum positif Indonesia?
2. Bagaimana bentuk pertanggungjawaban pidana terhadap pelaku yang menggunakan teknologi *Artificial Intelligence* untuk melakukan pemalsuan identitas digital *deepfake* menurut hukum positif di Indonesia?

## **C. Tujuan Penelitian**

Dengan melihat latar belakang serta rumusan masalah yang telah diuraikan sebelumnya, penelitian ini bertujuan untuk mencapai hasil akhir yang diharapkan oleh penulis, antara lain:

1. Untuk mengidentifikasi dan menganalisis bentuk tindak pidana pemalsuan identitas digital atau *deepfake* menggunakan teknologi *Artificial Intelligence* dalam perspektif hukum positif Indonesia
2. Memahami dan menganalisis bentuk pertanggungjawaban pidana bagi pelaku tindak pidana pemalsuan identitas digital yang menggunakan teknologi *Artificial Intelligence* menurut hukum positif Indonesia.

#### **D. Kegunaan Penelitian**

Hasil penelitian ini diharapkan dapat memberikan kontribusi yang bermanfaat baik secara teoritis ataupun praktis, antara lain:

1. Manfaat Teoritis
  - a. Memberikan kontribusi pada ilmu hukum, utamanya dalam perkembangan hukum pidana dan hukum siber. Dengan penelitian ini, maka pengetahuan akan bertambah mengenai tantangan hukum yang dihadapi akibat perkembangan teknologi *Artificial Intelligence*.
  - b. Menambah literatur akademik mengenai kejahatan berbasis teknologi informasi, yang hingga kini masih relatif minim dibahas secara mendalam terkait konteks hukum pidana di Indonesia. Serta memperkaya teori pertanggungjawaban pidana dengan menganalisis unsur-unsur delik dan bentuk kesalahan atau *mensrea* dalam konteks pemalsuan identitas digital, sehingga dapat menjadi referensi dan dasar konseptual bagi penelitian selanjutnya.
  - c. Memberikan peningkatan pemahaman tentang hukum positif di Indonesia. Dengan menganalisis regulasi yang ada, penelitian ini akan

membantu memperjelas pemahaman mengenai hukum positif Indonesia terkait dengan kejahatan siber dan penggunaan teknologi *Artificial Intelligence* dalam pergeseran paradigma kejahatan di era digital, serta memberikan dasar bagi pengembangan regulasi yang lebih baik.

## 2. Manfaat Praktis

- a. Memberikan pengertian yang lebih jelas untuk para aparat penegak hukum seperti polisi, jaksa, hakim saat mengatasi kasus-kasus yang berkaitan teknologi *Artificial Intelligence* khususnya dalam tindak pidana pemalsuan identitas digital atau *deepfake* melalui pemberian pemahaman yang lebih baik mengenai pertanggungjawaban pidana beserta cara penegakan hukumnya yang tepat.
- b. Menjadi rekomendasi kebijakan yang konkret untuk pemerintah dan pembuat undang-undang dalam merumuskan peraturan yang lebih efektif, adaptif, dan adaptif mengenai perkembangan teknologi khususnya dalam menangani kejahatan berbasis *Artificial Intelligence*, sehingga dapat melindungi masyarakat dari penyalahgunaan teknologi.
- c. Memberikan edukasi hukum kepada masyarakat agar lebih waspada terhadap modus kejahatan berbasis teknologi *Artificial Intelligence* dan memahami pentingnya perlindungan identitas digital.
- d. Menjadi rekomendasi materi dalam pelatihan dan pendidikan bagi mahasiswa hukum, praktisi hukum, dan pihak terkait lainnya, untuk

meningkatkan pemahaman mereka tentang isu-isu hukum dan tindak kejahatan yang berkaitan dengan teknologi *Artificial Intelligence*.

## E. Terminologi

### 1. Pertanggungjawaban pidana

Dalam ranah hukum pidana, dikenal istilah pertanggungjawaban pidana yang dalam bahasa Inggris disebut *responsibility* atau *criminal liability*, sedangkan dalam bahasa Belanda dikenal sebagai *toereken*. Konsep ini memegang peranan penting dalam sistem hukum pidana karena tidak hanya berkaitan dengan aspek yuridis, tetapi juga berhubungan dengan nilai-nilai moral serta norma kesusilaan yang hidup dalam masyarakat. Dengan demikian, penerapan pertanggungjawaban pidana bertujuan untuk mewujudkan keadilan yang sejalan dengan prinsip hukum dan etika sosial.<sup>12</sup>

Roeslan Saleh menyebut “pertanggungjawaban pidana”, di sisi lain Moeljatno mengemukakan “pertanggungjawaban dalam hukum pidana”, Para ahli hukum lainnya telah lebih sering membahas hal tersebut dengan “pertanggungjawaban pidana”.<sup>13</sup> Pada dasarnya, pertanggungjawaban pidana menjadi konsep dasar dalam hukum pidana yang berhubungan dengan dapat tidaknya seseorang dipidana karena perbuatan yang dilakukannya. Menurut Roeslan Saleh, tidak setiap perbuatan pidana secara

---

<sup>12</sup> Hanafi, Mahrus, 2015, *Sistem Pertanggung Jawaban Pidana*, Cetakan pertama, Rajawali Pers, Jakarta, hlm.16.

<sup>13</sup> Sampur Dongan Simamora dan Mega Fitri Hertini, 2015, *Hukum Pidana Dalam Bagan*, FH Untan Press, Pontianak, hlm.166.

otomatis berkaitan dengan pertanggungjawaban pidana. Istilah perbuatan pidana hanya menegaskan adanya larangan terhadap suatu tindakan.

Seseorang yang mengerjakan perbuatan terlarang tidak selalu dikenakan tanggung jawab pidana. Hal ini karena tanggung jawab pidana bergantung dari apakah ada unsur kesalahan pada saat perbuatan tersebut dilakukan. Apabila orang yang berbuat tindakan pidana itu memenuhi unsur-unsur kesalahan yang dikaitkan dengan tindak pidana yang dilakukan, maka tentu dia akan dipidana.<sup>14</sup> Dengan kata lain, penentuan apakah terdakwa dijatuhi pidana atau dibebaskan bergantung pada terpenuhinya unsur-unsur pertanggungjawaban pidana. Apabila terdakwa dipidana, hal tersebut menunjukkan bahwa perbuatannya terbukti bersifat melawan hukum, dan ia memiliki kemampuan untuk mempertanggungjawabkan tindakannya.

Kemampuan tersebut menjadi dasar yang menunjukkan adanya unsur kesalahan dari pelaku, baik dalam bentuk kesengajaan maupun kealpaan. Dengan demikian, pertanggungjawaban pidana pada dasarnya adalah pemberian beban hukum untuk pembuat tindak pidana yang dalam keadaan sadar dan dapat dipertanggungjawabkan dalam mengerjakan tindak pidana, sehingga layak untuk dikenai sanksi pidana. Sehingga yang dimaksud dengan kemampuan bertanggungjawab merupakan suatu keadaan batin seseorang yang normal dan sehat.

---

<sup>14</sup> Fadillah Sabri, 2021, *Pertanggungjawaban Pidana Dokter Atas Kesalahan Dalam Praktik Kedokteran*, PT Raja Grafindo Persada, Depok, hlm. 92



Menurut Mulyatno, dalam doktrin hukum pidana, pertanggungjawaban muncul apabila memenuhi 3 unsur utama yaitu:

a. Kesalahan

Menurut Moelyatno, kesalahan adalah keadaan psikis pelaku yang berhubungan dengan perbuatannya, yaitu unsur kesengajaan atau *dolus* dan kealpaan atau *culpa*. Kesalahan dipahami sebagai keadaan psikis atau sikap batin pelaku terhadap perbuatan yang dilakukannya, yang menunjukkan adanya hubungan antara pelaku dengan tindak pidana tersebut. Dengan kata lain, kesalahan adalah dasar bagi adanya pidana, sebagaimana ditegaskan dalam asas tiada pidana tanpa kesalahan atau dalam bahasa latin *geen straf zonder schuld*.

Oleh karena itu, kesalahan dalam hukum pidana bukan sekadar pelanggaran terhadap norma hukum, tetapi merupakan penilaian menyeluruh terhadap keadaan batin pelaku, kapasitasnya untuk bertanggung jawab, serta kondisi yang melatarbelakangi tindakannya yang artinya, hanya dapat dipidana seseorang apabila ia melakukan perbuatan yang dilarang, memiliki kesalahan dalam arti hukum, dan tidak dilindungi penyebab dihapuskannya pertanggungjawaban pidana karena suatu alasan.

b. Kemampuan Bertanggungjawab

Dalam Kitab Undang-Undang Hukum Pidana atau kerap disebut juga dengan KUHP tidak mengatur tentang pertanggung jawaban melainkan kemampuan untuk bertanggungjawab. Hal tersebut diatur

dalam Pasal 44 KUHP, yang mengemukakan bahwa seseorang yang menjalankan suatu perbuatan pidana tidak bisa dipidana apabila ia mempunyai gangguan jiwa atau cacat perkembangan mental, sehingga tidak mempunyai kemampuan untuk menyadari sifat tindakannya atau tidak dapat menguasai kehendaknya. Maka dari itu, orang yang mengalami gangguan jiwa, anak-anak yang belum memiliki kecakapan penuh, atau orang dalam keadaan tidak sadar, dianggap tidak mempunyai kemampuan bertanggung jawab secara penuh.

c. Tidak ada alasan pemaaf.

Konsep hukum pidana, alasan pemaaf merupakan dasar yang dapat menghapus kesalahan pelaku, sehingga meskipun secara formil ia telah berbuat tindakan yang unsur tindak pidananya terpenuhi, pelaku tidak dapat dijatuhi hukuman. Dengan kata lain, perbuatannya tetap tergolong melawan hukum, namun karena adanya kondisi pribadi atau keadaan tertentu, pelaku tidak dapat dipersalahkan atas tindakannya. Alasan pemaaf ini berbeda dengan alasan pembenar, yang berfungsi menghapus sifat melawan hukum dari suatu tindakan. Dalam teori hukum pidana, alasan pembenar dianggap sebagai dasar yang menghilangkan unsur melanggar hukum dari tindakan, sedangkan alasan pemaaf berfokus pada penghapusan kesalahan pelaku. Keduanya memiliki perbedaan mendasar alasan pembenar memberikan “pembenaran” terhadap suatu perbuatan melawan hukum, sementara

alasan pemaaf memberikan “pemaafan” bagi pelaku yang berbuat tindak pidana tersebut.<sup>15</sup>

Pertanggungjawaban pidana pada dasarnya adalah pemberian beban hukum kepada pembuat yang dengan sadar, dapat dipertanggungjawabkan mengerjakan tindak pidana, sehingga layak untuk dikenai sanksi pidana. Dalam konteks kejahatan berbasis teknologi, termasuk penggunaan *Artificial Intelligence* untuk melakukan tindak pidana pemalsuan identitas digital *deepfake*, pertanggungjawaban pidana menjadi semakin kompleks karena melibatkan persoalan teknis pembuktian, identifikasi pelaku, serta perluasan subjek hukum, tidak hanya kepada individu tetapi juga kemungkinan kepada korporasi atau penyelenggara platform digital yang turut memfasilitasi terjadinya kejahatan tersebut.

## 2. *Artificial Intelligence*

*Artificial Intelligence* atau bisa disebut juga dengan AI merupakan sebuah tanda dimulainya era revolusi industri 4.0 yang dipercaya memberikan kemudahan kepada penggunanya, baik itu di ranah pemerintahan ataupun di ranah industri.

AI adalah program berbasis media digital, seperti komputer, yang dirancang agar mampu berfokus pada data dan dapat memproses informasi dan bertindak layaknya manusia dalam mengambil keputusan maupun

---

<sup>15</sup> Hanafi Amrani, dan Mahrus Ali, 2015, *Sistem Pertanggungjawaban Pidana*, Jakarta, Rajawali Pers, hlm. 45.

melakukan tindakan tertentu.<sup>16</sup> AI dapat dipahami sebagai bentuk simulasi kecerdasan manusia yang dijalankan oleh mesin, khususnya sistem komputer. Melalui penerapan AI, komputer memiliki kemampuan untuk belajar dari pengalaman, mengenali pola tertentu, mengambil keputusan secara mandiri, serta menyelesaikan berbagai jenis tugas dengan tingkat kecepatan dan efisiensi yang tinggi, meskipun tugas tersebut bersifat kompleks dan memerlukan analisis mendalam.<sup>17</sup> Sejak masa itu, teknologi Hal ini sudah banyak digunakan dalam tugas-tugas pengolahan bahasa alami, seperti perilaku manusia.<sup>18</sup>

Di Indonesia, perkembangan AI semakin pesat seiring dengan transformasi digital di berbagai sektor, seperti keuangan, kesehatan, pendidikan, hingga pemerintahan. Pemerintah telah menerbitkan Strategi Nasional Kecerdasan Artifisial 2020–2045 yang menjadi peta jalan pengembangan AI di Indonesia melalui Kementerian Komunikasi dan Informatika. Strategi ini mengfokuskan pada lima aspek prioritas, yakni penelitian, ketahanan pangan, serta mobilitas dan kota cerdas.

Penerapan AI dalam berbagai bidang tersebut diharapkan dapat meningkatkan efisiensi dalam hal kualitas layanan publik, serta daya saing bangsa di era digital. Pemanfaatan AI diperkirakan dapat meningkatkan dan

---

<sup>16</sup> Endang Irawan Supriyadi & Dianing Banyu Asih, 2020, "Implementasi *Artificial Intelligence* (AI) di Bidang Administrasi Publik Pada Era Revolusi Industri 4.0", *Jurnal Sosial dan Humaniora Universitas Muhammadiyah Bandung*, Vol. 02 No.02

<sup>17</sup> Moh. Ayub Ismail, "Apa Itu AI (*Artificial Intelligence*): Pengertian, Kelebihan, Dan Kekurangan", universitas stekom, <https://stekom.ac.id/artikel/apa-itu-ai-kecerdasan-buatan-pengertian-kelebihan-kekurangan> di akses tanggal 20 September 2023

<sup>18</sup> Ayu Annisa, 2024, "Persepsi Mahasiswa Terhadap Pemanfaatan *Artificial Intelligence* (AI) Chat GPT Sebagai Sumber Informasi Tugas Kuliah", *Skripsi Fakultas Dakwah UIN Prof. K.H. Saifuddin Zuhri, Purwokerto*, hlm. 47.

memastikan mutu kehidupan manusia. solusi terhadap berbagai persoalan sosial melalui integrasi dengan kemajuan teknologi yang terus berkembang. Selain itu, ketertarikan masyarakat Indonesia dalam memanfaatkan teknologi AI menjadi fokus utama, hal ini disebabkan dalam mengingat peluang, potensi dan efek yang dihasilkan.<sup>19</sup>

Berkaitan hasil analisis yang sudah dilaksanakan, disimpulkan bahwa perkembangan AI saat ini menunjukkan kemajuan pesat, baik dalam aspek perangkat keras maupun perangkat lunak. Teknologi tersebut dianggap berhasil menghasilkan sistem dan produk yang dapat dimanfaatkan dalam berbagai aktivitas kehidupan bermasyarakat. AI bekerja melalui empat teknik utama, yaitu *searching* yang berarti proses pencarian, *reasoning* yang mencakup kemampuan berpikir logis, *planning* yang berhubungan dengan perencanaan tindakan, serta *learning* yang mengacu pada proses pembelajaran..<sup>20</sup>

AI terbagi dalam beberapa cabang penting. Salah satunya adalah *machine learning*, yaitu metode yang mengharapkan komputer belajar dari data tanpa instruksi pemrograman eksplisit. Bentuk yang lebih konkrit adalah *deep learning*, yang memakai aringan saraf tiruan atau *neural networks* berlapis yang berguna dalam mengolah data dalam jumlah besar, termasuk data visual dan audio.

---

<sup>19</sup> Selly Anastassia Amellia Kharis. et al., 2023, Analisis Tren Minat Masyarakat Indonesia terhadap *Artificial Intelligence* dalam Menyongsong Society 5.0: Studi Menggunakan Google Trends,|, *G-Tech: Jurnal Teknologi Terapan*, Vol.7, No. 4, hlm. 1346.

<sup>20</sup> Endang Irawan Supriyadi dan Dianing Banyu Asih, 2021, Implementasi *Artificial Intelligence* (AI) di Bidang Administrasi Publik Pada Era Revolusi Industri 4.0,| *Jurnal RASI* Vol. 2, No. 2 hlm. 15



Selain itu, terdapat *natural language processing* atau NLP yang diharapkan komputer bias mengerti dan mengelola bahasa manusia, serta *computer vision* yang memberi kemampuan bagi mesin untuk mengenali dan menafsirkan konten visual. Perkembangan cabang-cabang AI ini telah melahirkan berbagai aplikasi dalam kegiatan sehari-hari, dimulai dari asisten virtual, pengenalan wajah, kendaraan otonom, hingga teknologi manipulasi digital seperti *deepfake*.

Namun, peran manusia disegala bidang tidak dapat digantikan sepenuhnya oleh teknologi AI, termasuk dalam bidang pendidikan. Hanya saja AI berguna dalam program atau sistem yang menyokong dan membantu kegiatan manusia untuk menuntaskan tugasnya.<sup>21</sup> Selain itu, pemanfaatan AI di Indonesia juga menimbulkan tantangan hukum, khususnya terkait penyalahgunaannya dalam tindak pidana. Contoh nyata adalah penggunaan teknologi *deepfake* untuk pemalsuan identitas digital, penyebaran hoaks, pornografi non-konsensual, maupun penipuan berbasis rekayasa suara dan video. Hal ini memberikan tanda bahwa regulasi mengenai AI di Indonesia perlu diperkuat. Walaupun Indonesia memiliki Undang-Undang Informasi dan Transaksi Elektronik dan saat ini Indonesia baru mengesahkan Undang-Undang Perlindungan Data Pribadi, namun belum terdapat aturan yang secara khusus membahas aturan pertanggungjawaban pidana dalam kasus penyalahgunaan AI.

---

<sup>21</sup> Yudo Devianto dan Saruni Dwiasnati, 2020, Kerangka Kerja Sistem Kecerdasan Buatan dalam Meningkatkan Kompetensi Sumber Daya Manusia Indonesia, *Jurnal Telekomunikasi dan Komputer* Vol. 10, No. 1, hlm. 20.

Kondisi ini menunjukkan bahwa urgensi pembaruan hukum di Indonesia sangat diperlukan agar mampu mengantisipasi perkembangan kejahatan berbasis AI. Sistem hukum pidana perlu beradaptasi dengan memasukkan aturan yang lebih spesifik mengenai penyalahgunaan teknologi AI, baik dalam hal pencegahan maupun penindakan. Pembaruan hukum tersebut bukan hanya penting dalam melindungi kepentingan masyarakat, namun juga dalam memberikan kepastian bahwa kemajuan teknologi tetap dalam koridor perlindungan hukum yang adil dan bertanggung jawab.

### 3. Pemalsuan identitas Digital (*Deepfake*)

Salah satu fenomena yang saat ini menimbulkan perhatian serius adalah penggunaan teknologi *deepfake*. Istilah *deepfake* berasal dari gabungan kata *deep learning* dan *fake*, *Deep Learning* yakni suatu teknologi yang menghasilkan perangkat lunak untuk sebuah teknologi *deepfake*.<sup>22</sup> Sedangkan kata *fake* berasal dari hasil teknologi *deepfake* dalam bentuk konten palsu yang bukan sebuah hal yang original.<sup>23</sup>

Fitur wajah seseorang dapat dimanipulasi menggunakan teknologi *deepfake*. *Deepfake* bias berupa video seseorang sedang bertindak sesuatu padahal aslinya tidak pernah dilakukannya, hal itu dikerjakan dengan

---

<sup>22</sup> John Brandon, 2018, Terrifying High-Tech Porn: Creepy ‘deepfake’ Videos Are on the Rise, *Fox News*, <https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise>.

<sup>23</sup> Chiquita Thefirstly Noerman & Aji Lukman Ibrahim, 2024, Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Perlindungan Negara, *Jurnal USM Law Review*, Vol. 7 No. 2, hlm. 604.

memakai muka seseorang di sebuah video yang sebenarnya diperbuat orang lain.<sup>24</sup>

Melalui *deepfake*, identitas digital seseorang dapat dipalsukan dengan cara menempelkan wajah, suara, atau gerakan tubuh ke dalam konten lain, sehingga orang tersebut terlihat melakukan tindakan yang sebenarnya tidak pernah dilakukan. *Deepfake* mempunyai kemampuan untuk mengubah ingatan, menciptakan ingatan palsu, atau mengganti karakter seseorang.<sup>25</sup> Teknologi *deepfake* berpotensi menimbulkan kerugian besar bagi berbagai pihak apabila dimanfaatkan untuk melakukan tindak kejahatan seperti penipuan, pornografi, atau kejahatan lainnya, melalui memanipulasi data diri seseorang sehingga tampak individu yang menjadi korban yang melakukan tindakan kejahatan.

Walaupun tindak pidana penipuan sudah ada dalam KUHP, dampak dari penipuan melalui teknologi *deepfake* jauh lebih kompleks dan merugikan dibandingkan dengan penipuan konvensional. Hal tersebut disebabkan *deepfake* bukan hanya mengandung unsur penipuan verbal, tetapi juga penipuan visual yang dapat menciptakan ilusi nyata dan menyesatkan persepsi publik secara lebih efektif dan meyakinkan.<sup>26</sup>

---

<sup>24</sup> John D. Kelleher, Deep Learning, 2019, *The MIT Press Essential Knowledge Series*, Massachusetts, The MIT Press, Cambridge.

<sup>25</sup> Cristian Vaccari and Andrew Chadwick, 2020, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," *Social Media + Society* Vol. 6 No. 1.

<sup>26</sup> Chiquita Thefirstly Noerman & Aji Lukman Ibrahim, 2024, Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Perlindungan Negara, *Jurnal USM Law Review*, Vol. 7 No. 2, hlm. 604.

Menurut Chesney dan Citron, *deepfake* menimbulkan ancaman serius terhadap privasi, reputasi, bahkan stabilitas sosial dan politik, hal itu disebabkan *deepfake* digunakan dalam menyebarkan informasi palsu, pornografi non-konsensual, pemerasan, hingga manipulasi opini publik. Dalam konteks hukum pidana, pemalsuan identitas digital dengan *deepfake* dapat diklasifikasikan sebagai tindak pidana yang melanggar hak privasi, kehormatan, serta berpotensi memenuhi unsur yang ada didalam tindak pidana penipuan, tindak pidana pencemaran nama baik, maupun pelanggaran terhadap perlindungan data pribadi.

Di Indonesia, regulasi yang dapat dipakai untuk menjerat pelaku pemalsuan identitas digital masih mengacu pada Undang-Undang Informasi dan Transaksi Elektronik, khususnya terkait pencemaran nama baik, penyebaran konten palsu, dan manipulasi informasi elektronik, serta terdapat dalam Undang-Undang Perlindungan Data Pribadi, dimana mengatur perlindungan terhadap data pribadi termasuk identitas digital. Sampai saat ini belum terdapat ketentuan khusus yang mengatur secara eksplisit mengenai *deepfake*, sehingga menimbulkan tantangan dalam proses penegakan hukum, terutama dalam aspek pembuktian dan pertanggungjawaban pidana. Sehingga, pemalsuan identitas digital melalui *deepfake* bukan hanya merupakan fenomena teknologi, tetapi merupakan isu hukum yang membutuhkan kajian lebih lanjut. Kehadiran teknologi ini menuntut adanya pembaruan regulasi agar hukum Indonesia dapat mewadahi penegakan hukum yang tepat kepada korban serta memastikan

hukum berlaku adil dan tepat kaitannya dengan pertanggungjawaban pidana orang yang melakukan perbuatan pidana.

## **F. Metodologi Penelitian**

Metode penelitian yang dipakai dalam riset ini yakni yuridis normatif. Penelitian yuridis normatif adalah cara penelitian dalam meneliti serta mengkaji mengenai hukum sebagai aturan, asas hukum, prinsip hukum, norma hukum, doktrin hukum, teori hukum serta kepustakaan lainnya yang bisa digunakan dalam menjawab permasalahan hukum yang diteliti.

### **1. Metode Pendekatan**

Penelitian hukum memakai beragam pendekatan, hal tersebut bertujuan untuk mempunyai informasi dalam beragam aspek tentang masalah yang sedang dikaji. Dalam menyelesaikan permasalahan yang menjadi kunci bahasan, maka penelitian hukum memerlukan pendekatan penelitian hukum. Pendekatan peraturan perundang-undangan atau *statue approach* dan pendekatan konseptual atau *conceptual approach* adalah pendekatan yang digunakan dalam penelitian ini. Pendekatan per-undang-undangan, yakni pendekatan dikerjakan melalui cara mengkaji seluruh peraturan perundang-undangan dan regulasi yang ada dan menjadi acuan terkait dengan masalah hukum yang diteliti.<sup>27</sup> Sementara itu, pendekatan konseptual merupakan metode yang didasarkan pada pemahaman serta teori yang tumbuh dan berkembang dalam disiplin ilmu hukum. Pemilihan

---

<sup>27</sup> Dr. Muhaimin, SH., M.Hum.,2020, *Metode Penelitian Hukum*, Mataram University Press, Mataram, hlm.56.



pendekatan ini dilakukan dengan tujuan untuk mendapatkan jawaban mengenai berbagai persoalan hukum yang muncul dalam suatu riset hukum. Dengan begitu, maka keserasian antara pendekatan dengan masalah hukum ialah pertimbangan yang paling utama dalam melakukan pemilihan pendekatannya.<sup>28</sup>

## **2. Sumber Data**

Data yang dipakai dalam penelitian ini yaitu data sekunder atau bahan hukum yang merupakan bahan yang didapatkan lewat studi kepustakaan. Melalui cara memahami peraturan-peraturan, buku-buku, situs internet, dan data yang berhubungan dengan penelitian yang diklasifikasikan menjadi:

### **a. Bahan Hukum Primer**

Bahan Hukum Primer adalah bahan hukum yang terdiri dari peraturan perundang-undangan, putusan pengadilan, risalah resmi, dan dokumen resmi negara. Dalam bahan hukum primer ini penulis menggunakan peraturan yang menjadi acuan yaitu, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

### **b. Bahan Hukum sekunder**

Penelitian ini memakai sumber bahan sekunder yang relevan dengan topik penelitian, yakni bahan yang berfungsi menjelaskan bahan hukum primer. Sumber tersebut terdiri dari rancangan undang-undang,

---

<sup>28</sup> Ibid, hlm. 57.

hasil penelitian yang dipublikasikan dalam jurnal atau majalah ilmiah, buku-buku teks, pendapat para pakar hukum, serta berbagai publikasi hukum lainnya yang tidak termasuk dalam kategori dokumen resmi. Publikasi mengenai hukum yakni berupa kamus hukum, jurnal hukum, buku teks, dan pendapat atas putusan pengadilan.

c. Bahan Hukum Tersier

Penelitian ini juga mengambil bahan-bahan hukum tersier, antara lain yakni bahan yang menjadi arahan maupun pemahaman mengenai bahan hukum primer ataupun bahan hukum sekunder, seperti kamus hukum, ensiklopedia, kamus bahasa, dan ensiklopedia hukum.

### 3. Metode Pengumpulan Data

Adapun metode pengelompokan data yang dipakai dalam penulisan skripsi ini memakai metode pengumpulan data melalui teknik pengkelompokan bahan hukum atau data sekunder di penelitian hukum normatif dilaksanakan melalui studi pustaka atau *bibliography study* dengan bahan-bahan hukum, yakni bahan hukum primer, bahan hukum sekunder, bahan hukum tersier dan atau bahan yang non-hukum. Pencarian bahan hukum dapat dilakukan melalui membaca, mendengarkan, melihat, maupun pencarian bahan hukum di media internet atau *website*, *e-books*, buku-buku referensi, artikel, dan jurnal-jurnal. Selain itu dalam memperoleh data yang lebih valid, maka pengumpulan data kemudian diinventarisir dan dikelompokkan atau diklasifikasikan sesuai dengan masing-masing

rumusan masalah.

#### **4. Analisis Data**

Penelitian ini memakai metode analisis kualitatif, yaitu pendekatan yang tidak dinilai atau diukur secara numerik, melainkan dilakukan melalui proses interpretasi terhadap berbagai bahan hukum yang telah dikumpulkan dan diolah sebelumnya. Tujuan dari penerapan metode penafsiran ini untuk menelaah hukum dengan menilai apakah dalam bahan hukum yang digunakan, utamanya bahan hukum primer, adanya kekosongan norma, perselisihan antar norma, atau ketidakjelasan dalam norma hukum tersebut.

Oleh karena itu, setelah data sekunder dalam bentuk dokumen didapatkan lengkap, kemudian di analisis dengan peraturan yang berhubungan dengan persoalan yang dikaji. Analisis data kualitatif dibutuhkan untuk menghasilkan data yang dibutuhkan sebagai informasi yang tepat dan seterusnya ditulis secara deskriptif.

#### **G. Sistematika Penulisan**

Agar memudahkan dalam penelusuran dan pemahaman laporan penelitian ini, diperlukan penyusunan sistematika penulisan yang teratur. Skripsi ini dibagi menjadi empat bab yang disusun secara sistematis, di mana setiap bab membahas aspek yang tidak saling berkaitan namun tetap membentuk satu kesatuan yang saling berkaitan.

### **BAB I                      PENDAHULUAN**

Dalam Bab I, penulis menguraikan mengenai latar belakang yang memuat aspek filosofis, yuridis, dan

sosiologis. Kemudian juga memuat rumusan masalah, tujuan penelitian, manfaat penelitian, terminologi, metode penelitian, dan sistematika penelitian yang disajikan sebagai pengantar untuk masuk ke permasalahan yang akan diteliti.

## **BAB II                    TINJAUAN PUSTAKA**

Bab II berisi mengenai tinjauan umum yang juga tentang Penyalahgunaan teknologi *Artificial Intelligence* untuk melakukan tindak pidana pemalsuan identitas digital atau *deepfake*.

## **BAB III                HASIL PENELITIAN DAN PEMBAHASAN**

Bab III, penulis membahas dan menjawab berbagai rumusan permasalahan yang tertulis dalam Bab I berdasarkan hasil riset atau penelitian yang sudah terhimpun oleh penulis yang kemudian disusun dalam bab ini..

## **BAB IV                PENUTUP**

Bab terakhir yaitu Bab IV, penulis memberikan uraian dari penutup yang memuat kesimpulan dan saran. Kesimpulan berisi uraian dari penulis mengenai hal-hal yang dapat disimpulkan berdasarkan hasil penelitian dan pembahasan pada bab sebelumnya, kemudian saran berisi rekomendasi terkait putusan maupun kebijakan

yang sebaiknya diberikan dan diambil dilihat dari berbagai aspek, baik aspek filosofis, yuridis, maupun sosiologi.





## **BAB II**

### **TINJAUAN PUSTAKA**

#### **A. Tinjauan Umum Pertanggungjawaban Pidana**

##### **1. Pengertian Pertanggungjawaban Pidana**

Pertanggungjawaban pidana adalah kewajiban subjek tindak pidana untuk menerima akibat atas perlakuannya yang telah bertindak dalam tindak pidana yang merugikan.<sup>29</sup> Seseorang yang membuat tindak pidana hanya akan dihukum jika ia bertindak dengan kesalahan. Seseorang dapat dianggap bertindak dengan kesalahan jika, pada saat melakukan tindak pidana tersebut, masyarakat menganggap tindakan tersebut menyimpang dari norma atau aturan dan karenanya layak untuk dikecam.

Menurut Roeslan Saleh, pertanggungjawaban pidana diartikan sebagai bentuk lanjutan dari adanya celaan objektif terhadap suatu perbuatan pidana yang kemudian dilengkapi dengan adanya celaan subjektif pada pelaku, sehingga terpenuhi syarat untuk dijatuhkannya pidana atas perbuatannya tersebut. Celaan objektif adalah ketika seseorang melakukan perbuatan yang tidak boleh dilakukan oleh hukum, untuk hukum formil ataupun hukum materil. Sementara itu, celaan subjektif berkaitan pada kecaman yang diarahkan kepada individu pelaku atas tindakannya yang melanggar ketentuan hukum. Namun, apabila perbuatan tersebut tergolong

---

<sup>29</sup> I Gusti Kade Budhi.H., 2022, *Artificial Intelligence : Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana*, PT Raja Grafindo Persada, Depok, hlm.88

perbuatan tercela atau melanggar hukum, tetapi pelaku tidak memiliki kemampuan untuk bertanggung jawab karena adanya faktor kesalahan atau gangguan dalam dirinya, maka pertanggungjawaban pidana tidak dapat dikenakan kepadanya.<sup>30</sup>

Menurut Soegeng Istanto, pertanggungjawaban sebagai kewajiban dalam memperoleh hasil dan pengklasifikasian atas segala sesuatu yang telah terjadi, termasuk tanggung jawab untuk melakukan pemulihan terhadap masalah yang mungkin timbul akibat perbuatannya. Sementara itu, menurut Titik Triwulan, pertanggungjawaban harus memiliki dasar yang spesifik, yaitu suatu kondisi yang timbul akibat dari hak hukum bagi seseorang dalam menuntut orang lain, serta menciptakan hal yang wajib untuk hukum bagi seseorang dalam memberikan pertanggungjawaban tindakannya.<sup>31</sup>

Pertanggungjawaban juga dimaknai bahwa meskipun seseorang memiliki kebebasan dalam melaksanakan tugas atau peran yang diembannya, tanggung jawab atas konsekuensi dari kebebasan tersebut tidak dapat melepaskan diri dari tanggung jawab atas konsekuensi dari kebebasannya. Selain itu, untuk memastikan bahwa kewajiban yang dijalankan sesuai dengan ketentuan dan tuntutan yang berlaku individu tersebut tetap dapat dimintai pertanggungjawaban atas tindakannya.

---

<sup>30</sup> Fatma, 2023, "Pertanggungjawaban Hukum Terhadap Perintah Jabatan Tanpa Wewenang Melakukan Tindak Pidana Pembunuhan Perspektif Hukum Pidana Islam" *Skripsi Fakultas Syariah dan Ilmu Hukum Isla Institut Agama Islam Negeri Parepare*, Parepare, hlm. 13

<sup>31</sup> Hizkia A. M. Kaunang, 2019, Tanggungjawab Hukum Pemerintah Dalam Ketersediaan Fasilitas Masyarakat Pejalan Kaki dan Penyandang Cacat Menurut Undang-Undang Nomor 22 Tahun 2009, *Lex Et Societatis*, Vol. VII, No. 11, hlm. 81

Pertanggungjawaban pidana berlandaskan pada asas kesalahan atau asas culpabilitas yang berpijak pada aspek keadilan, serta harus berjalan seimbang dengan asas legalitas yang menonjolkan kepastian hukum. Meskipun secara prinsip pertanggungjawaban pidana didasarkan pada adanya kesalahan, namun dalam kondisi tertentu dimungkinkan penerapan pertanggungjawaban pidana pengganti maupun suatu pidana pertanggungjawaban yang bersifat ketat. Contohnya, kekeliruan baik terkait dengan keadaan maupun terhadap hukum dapat menjadi alasan pemaaf, maka pembuat tidak dapat dijatuhi pidana, kecuali jika kekeliruan tersebut dinilai layak untuk dipertanggungjawabkan kepadanya.<sup>32</sup>

Pertanggungjawaban pidana memiliki fungsi sentral dalam hukum pidana karena menjadi mekanisme untuk memutuskan bisa atau tidaknya seseorang dikenai sanksi pidana atas tindakan yang dilakukannya. Fungsi utamanya adalah sebagai penilaian yuridis agar pemidanaan hanya dapat dijatuhkan kepada orang yang benar-benar bersalah dan mampu bertanggung jawab. Dengan begitu, pertanggungjawaban pidana melindungi individu dari kemungkinan kriminalisasi yang sewenang-wenang sekaligus menegakkan asas tiada pidana tanpa kesalahan.

Pertanggungjawaban pidana berfungsi untuk membedakan antara tindakan pidana dengan pertanggungjawaban pidana. Tidak semua perbuatan yang bersifat melawan hukum otomatis mengakibatkan

---

<sup>32</sup> Evi Febryani, Dian Puspa Iwari. et al., 2024, Pertanggung jawaban Pidana sebagai Dampak Penuntutan Terhadap Korporasi Akibat Pailit, *Collegium Studiosum Journal*, Vol. 7, No. 1, hlm. 3

pemidanaan, sebab sebelumnya harus terdapat pembuktian mengenai adanya kesalahan pada diri orang yang berbuat tindak pidana dan kemampuan untuk bertanggung jawab. Dalam hal ini, pertanggungjawaban pidana memastikan bahwa pemidanaan dilakukan secara adil dan proporsional.

Fungsi lainnya adalah sebagai dasar legitimasi bagi pemidanaan. Pemidanaan tidak berdiri sendiri, tetapi lahir dari adanya pertanggungjawaban pidana. Tanpa adanya pertanggungjawaban pidana, pemidanaan kehilangan dasar hukum dan berseberangan dengan prinsip keadilan. Sehingga, pertanggungjawaban pidana dapat dipandang sebagai jembatan yang menghubungkan antara perbuatan pidana dan sanksi pidana.

## **2. Dasar Pertanggungjawaban Pidana**

Dasar utama pertanggungjawaban pidana dalam hukum Indonesia adalah asas tiada pidana tanpa kesalahan *geen straf zonder schuld*. Artinya, orang hanya dapat dipidana jika adanya kesalahan yang melekat pada dirinya, baik dalam bentuk kesengajaan maupun kealpaan. Prinsip ini menjadi fondasi bagi hukum pidana modern, yang membedakan antara tindakan pidana dan pertanggungjawaban pidana.

Asas tiada pidana tanpa kesalahan tidak tercantum dalam Kitab Undang-undang Hukum Pidana atau kerap disebut KUHP, tidak ada di perundang-undangan lainnya, namun ada didalam hukum yang tidak tertulis. Walaupun asas ini tidak secara eksplisit tercantum dalam peraturan perundang-undangan, namun keberadaannya diakui dan berkembang

berkaitan dengan asas yang tertulis di dalam keyakinan masyarakat serta diterima sebagai bagian dari prinsip-prinsip hukum pidana.<sup>33</sup>

Dalam KUHP maupun peraturan perundang-undangan lainnya, masalah pertanggung jawaban pidana sedikit dibahas. Dalam KUHP Wv.S misalnya, masalah pertanggungjawaban pidana dikaitkan dengan alasan-alasan penghapusan pidana, hal tersebut relevan dengan aturan dalam pasal 44 yaitu mengenai seseorang tidak dapat dimintai pertanggungjawaban pidana apabila dapat mengendalikan kehendaknya akibat gangguan kejiwaan, pasal 48 yang mengatur mengenai tidak dapat dipidana apabila perbuatan dilakukan karena adanya daya paksa, pasal 49 membahas mengenai suatu perbuatan tidak dipidana apabila suatu perbuatan tersebut dilakukan untuk suatu pembelaan diri, pasal 50 membahas terkait tidak dipidana suatu perbuatan apabila melakukan tindakan untuk melaksanakan ketentuan undang-undang, dan pada pasal 51 KUHP Wv.S mengatur tentang tindakan yang tidak dapat dipidana apabila tindakan tersebut diperbuat karena perintah jabatan. Sedangkan dalam KUHP Nasional atau Undang-Undang No. 1 Tahun 2023 Pertanggungjawaban pidana tercantum di pasal 36 sampai dengan pasal 50.

### **3. Unsur-unsur Pertanggungjawaban Pidana**

Pertanggungjawaban berfungsi sebagai dasar dalam memilih apakah seseorang yang telah melakukan tindak pidana dapat dipidana atau

---

<sup>33</sup> Karimah, 2020, *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana (Fraud) Kecurangan Dalam Transaksi Perbankan*, Guepedia, DKI Jakarta, hlm. 28



dibebaskan dari hukuman. Untuk dapat menyatakan bahwa seseorang layak dimintai pertanggungjawaban atas perbuatan pidana yang dilakukannya, terdapat sejumlah unsur tertentu yang harus terpenuhi terlebih dahulu.

Secara terperinci, Sudarto menjelaskan bahwa untuk dapat dimintai pertanggungjawaban pidana, sehingga pelaku dapat dijatuhi pidana, sejumlah aspek yang perlu dipenuhi, yaitu:<sup>34</sup>

- a. Adanya suatu tindak pidana yang dilakukan oleh pembuat;

Unsur perbuatan merupakan komponen paling esensial dalam pertanggungjawaban pidana, seseorang tidak dapat dijatuhi pidana kalau ia tidak berbuat suatu tindakan termasuk dalam kategori tindakan terlarang sebagaimana diatur dalam peraturan perundang-undangan. Prinsip ini sesuai dalam asas legalitas yang menjadi dasar dalam sistem hukum pidana Indonesia. Asas legalitas dikenal dalam istilah Latin *Nullum delictum nulla poena sine praevia lege poenali* mengandung makna tiada ada seseorang yang dipidana tanpa adanya aturan hukum yang sudah mengatur dahulu perbuatan tersebut, serta tidak ada hukuman yang dapat dijatuhkan tanpa dasar hukum yang menetapkan larangan atas perbuatan itu.<sup>35</sup>

Dalam sistem hukum pidana Indonesia, hanya tindakan yang nyata atau tampak secara lahiriah yang dapat dijadikan dasar pemidanaan.

Artinya, hukum pidana menuntut adanya tindakan yang dapat

---

<sup>34</sup> Hanafi Amrani dan Mahrus Ali, *Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan*, Rajawali Press, Jakarta, 2015, hlm.22

<sup>35</sup> Mia Amalia, M. Ikhwan Raya. et al., 2024, *Asas-Asas Hukum Pidana*, PT. Sonpedia Publishing Indonesia, Jambi, hlm. 60

diamati secara eksternal, karena seseorang tidak dapat dijatuhi pidana semata-mata berdasarkan keadaan batin atau pikiran internalnya. Prinsip ini sejalan dengan *asas cogitationis poenam nemo patitur*, yang artinya yaitu tiada seorang pun dapat pidana atas yang ada dalam pikirannya saja.<sup>36</sup>

b. Adanya unsur kesalahan berupa kesengajaan atau kealpaan,

Kata “kesalahan” berasal dari terjemahan Bahasa Belanda, yaitu kata *Schuld*. Kesalahan merupakan kondisi psikologi orang yang berkaitan ke tindakan yang diperbuatnya. Dilihat dari keadaannya perbuatan tersebut pembuat dapat dicela atas perbuatannya.<sup>37</sup>

Pendefinisian kesalahan tersebut merupakan pengertian luasnya.

Dalam Kitab Undang-Undang Hukum Pidana atau KUHP, pengertian kesalahan dijabarkan konteks yang sempit, yakni sebagai bentuk kealpaan, sebagaimana tercermin dalam kalimat berbahasa Belanda yang termuat dalam Pasal 359 dan Pasal 360 KUHP. Selain itu, pengertian kesalahan bisa dilihat dari dua sudut, yaitu pengertian psikologis dan pengertian secara yuridis atau normatif. Kesalahan psikologis merupakan bentuk tindak pidana yang bersumber dari diri seseorang, yang berkaitan dengan apa yang dipikirkan dan dirasakan dalam batinnya. Jenis kesalahan ini sulit dibuktikan karena bersifat

---

<sup>36</sup> Jefferson M.H. & Juanrico A.S.T, 2022, Kajian Hukum Pidana Dalam Penipuan Jual Beli Akun Permainan Online Melalui Media Sosial, *TATOHI Jurnal Ilmu Hukum*, Vol. 2, No. 3, hlm. 259

<sup>37</sup> Firdaus Renuat, Padrisan Jamba. et al., 2023, *Pengantar Hukum Pidana*, CV. Gita Lentera, Sumatera Barat, hlm. 68

abstrak dan tidak memiliki bentuk nyata, sehingga keberadaannya tidak dapat diketahui secara langsung.<sup>38</sup>

Konsep hukum pidana Indonesia, kesalahan yang dipakai yakni kesalahan secara arti normatif. Kesalahan normatif dipahami sebagai bentuk kesalahan yang dinilai berdasarkan sisi masyarakat mengenai tindakan orang. Penilaian ini didasarkan pada aturan-aturan hukum pidana, yang mencakup kesalahan karena kesengajaan maupun kealpaan. Dengan demikian, dari tindakan yang telah terjadi, masyarakat atau pihak lain melihat hukum dan norma yang berlaku terdapat unsur kesalahan, baik yang dilakukan dengan sengaja maupun karena kelalaian.

1) Kesengajaan, Kesengajaan atau *dolus* yakni sebuah bentuk kesalahan dalam hukum pidana. Unsur kesengajaan atau *opzettelijk* bukan unsur *culpa* dalam tindak pidana di Indonesia. Hal ini mengacu pada unsur kesadaran atau niat seseorang untuk melakukan tindakan yang melanggar hukum.<sup>39</sup>

Mengenai unsur kesalahan yang bersifat sengaja, tidak perlu membuktikan pelaku mengetahui secara pasti bahwa tindakannya diancam oleh undang-undang. Artinya, tidak perlu dibuktikan bahwa pelaku memahami bahwa perbuatannya merupakan tindakan jahat atau melanggar hukum. Cukup dengan

---

<sup>38</sup> Ibid, hlm. 68

<sup>39</sup> Ecep Nurjamal, 2020, *Hukum Pidana dan Penerapan Hukum Acara Pidana*, Edu Publisher, Jawa Barat, hlm. 31

menunjukkan bahwa pelaku sadar dan mengakui perbuatannya serta memahami konsekuensi dari tindakannya, unsur kesengajaan telah terpenuhi.

Prinsip ini sesuai dengan prinsip hukum fiksi, yang beranggapan setiap orang dianggap mengetahui keberadaan dan isi dari peraturan perundang-undangan. Seseorang tidak dapat menghindar dari tanggung jawab hukum dengan alasan ketidaktahuan terhadap hukum atau larangan atas perbuatannya, karena hukum menganggap bahwa setiap individu telah mengetahui aturan yang berlaku. Kesengajaan terbagi menjadi dua kategori:<sup>40</sup>

a) *Dolus Directus* atau kesengajaan langsung, kesalahan Ini terjadi ketika seseorang sengaja dan secara langsung bertindak dengan perbuatan yang berlawanan dengan hukum dengan memiliki niat yang jelas dan sadar.

Dalam hal ini, pelaku tindakan mempunyai tujuan langsung yaitu untuk mencapai hasil dengan melanggar hukum.

b) *Dolus Indirectus* atau kesengajaan tidak langsung, kesalahan Ini terjadi ketika seseorang dengan sengaja melakukan tindakan yang melanggar hukum namun dengan tujuan lain, tetapi dengan sadar mengetahui hasil

---

<sup>40</sup> Ibid, hlm. 31

perbuatannya yang melanggar hukum merupakan konsekuensi yang tak terhindarkan dari tindakannya. Dalam hal ini, pelaku tindakan mungkin tidak mempunyai niat langsung untuk mencapai hasil yang melanggar hukum, tetapi dirinya sadar dan menerima bahwa hasil tersebut akan terjadi sebagai konsekuensi dari tindakannya.

Kesengajaan atau *dolus* ini sering kali menjadi unsur penting dalam membuktikan kesalahan pidana. Untuk menghukum seseorang atas tindakan pidana yang dilakukannya, maka perlu dibuktikan bahwa pelaku secara sengaja melakukan tindakan tersebut dengan niat atau kesadaran yang jelas disengaja. Definisi dan klasifikasi dari kesengajaan atau *dolus* dapat bervariasi dalam berbagai sistem hukum. Setiap yurisdiksi dapat memiliki standar yang sedikit berbeda terkait dengan bentuk kesengajaan atau *dolus* dalam konteks pidana. Contoh pasal kesengajaan dalam tindak pidana ialah yang membahayakan nyawa yang terdapat dalam pasal 165 KUHP dan menghilangkan nyawa pasal 340 KUHP.<sup>41</sup>

Orang melakukan perbuatan pidana diniatkan atau dilaksanakan timbul akibat dikehendaki dikarenakan ada tiga

---

<sup>41</sup> Ibid, hlm. 32



kesengajaan.<sup>42</sup> Yaitu kesengajaan sebagai kepastian, kesengajaan sebagai diniatkan, dan kesengajaan sebagai kemungkinan

## 2) Kealpaan atau *Culpa*

Kelalaian atau *Culpa* adalah seseorang melakukan tindakan pidana namun tidak diniatkan untuk melakukan, tindakan tersebut terjadi karena adanya kealpaan atau kurangnya kehati-hatian atau lalai. Dalam kealpaan sikap batin seseorang menyadari tindakan yang dilakukannya akan tetapi orang tersebut tidak menyadari terjadinya akibat dari tindakannya.

Dalam KUHP sendiri tidak ditemukan definisi mengenai kealpaan, sehingga pengertian kealpaan dapat didefinisikan dalam ilmu pengetahuan hukum atau doktrin dan yurisprudensi. Terdapat dua syarat kelalaian dari Van Hamel dan Simon yakni tidak mengadakan penduga-dugaan sebagaimana yang diharuskan oleh hukum dan tidak mengadakan penghati-hatian sebagaimana diharuskan oleh hukum bagi suatu kealpaan.<sup>43</sup>

Kelalaian atau *Culpa* merupakan salah satu bentuk dari kesalahan dalam hukum pidana. Hal ini terjadi ketika seseorang gagal memenuhi kewajiban atau standar yang diharapkan dari mereka untuk bertindak dengan hati-hati atau kecermatan yang wajar

---

<sup>42</sup> Ibid, hlm. 32

<sup>43</sup> Faisal Riza & Erwin Amsadi, 2023, Hukum Pidana Indonesia, UMSU Press, Medan, hlm. 74

alam suatu situasi tertentu. Kelalaian dapat dibagi menjadi dua kategori:<sup>44</sup>

1) *Culpa Lata* atau kelalaian berat, Ini terjadi ketika seseorang dengan sengaja atau sangat ceroboh melanggar kewajibannya untuk bertindak dengan hati-hati. Kelalaian berat mencerminkan kecerobohan yang sangat serius yang dampaknya cukup signifikan dan dapat merugikan orang lain.

2) *Culpa Levis* atau kelalaian ringan, Ini terjadi ketika seseorang tidak memenuhi kewajibannya untuk bertindak dengan standar kehati-hatian yang wajar, tetapi tidak seburuk kelalaian berat. Kelalaian ringan biasanya mencerminkan kegagalan untuk mengambil tindakan yang diharapkan atau kekurangan dalam kehati-hatian dalam situasi tertentu.

Dalam kasus kelalaian, tidak ada niat jahat atau kesengajaan untuk melanggar hukum. Namun, kelalaian tersebut masih dapat dianggap sebagai kesalahan apabila seseorang gagal untuk memenuhi kewajibannya dalam bertindak dengan hati-hati atau kecermatan yang wajar, dan dampak dari tindakannya dapat mengakibatkan kerugian atau cedera bagi orang lain. Standar kelalaian cukup beragam di berbagai sistem hukum. Setiap yurisdiksi dapat memiliki interpretasi dan persyaratan

---

<sup>44</sup> Ecep Nurjamal, *Loc. Cit.*, hlm 32

yang sedikit berbeda terkait dengan bentuk kelalaian dalam konteks hukum pidana.<sup>45</sup>

c. Adanya pembuat yang mampu bertanggungjawab;

Kecakapan untuk bertanggung jawab senantiasa terhubung dengan keadaan fisik dan psikis pelaku. Istilah tersebut dapat dimaknai sebagai keadaan kejiwaan yang sehat dan kemampuan intelektual seseorang dalam mengetahui perbedaan antara perbuatan yang benar dan yang salah. Kemampuan bertanggung jawab mencerminkan kapasitas seseorang untuk menyadari sifat melawan hukum dari tindakannya serta menyesuaikan kehendaknya dengan kesadaran tersebut.<sup>46</sup>

Kemampuan untuk bertanggung jawab selalu dikaitkan dengan konsep pertanggungjawaban pidana, menjadi salah satu unsur fundamental dalam menentukan adanya pertanggungjawaban pidana. Kecakapan tersebut berfungsi sebagai dasar dalam memberikan pidana kepada pelaku. Penilaian mengenai ada tidaknya kecakapan bertanggung jawab harus ada bukti di hadapan hakim, karena jika terbukti bahwa seseorang tidak mempunyai kecakapan tersebut, maka hal itu menjadi alasan hapusnya

---

<sup>45</sup> Ibid, hlm. 33

<sup>46</sup> Kamarudin, 2023, "Analisis Pertanggungjawaban Tindak Pidana Korupsi Di Wilayah Kabupaten Mamasa (Studi Kasus Putusan No 28/Pid.Sus-TPK/2022/PN Mam dan No 29/Pid.Sus-TPK/2022/PN Mam)", *Skripsi Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Sulawesi Barat, Mejene*, hlm. 18

pertanggungjawaban pidana. Pelaku yang tidak cakap bertanggung jawab tidak dapat dijatuhi pidana atas perbuatan yang dilakukannya.

Kemampuan bertanggung jawab juga berkaitan dengan umur tertentu bagi pelaku tindak pidana.<sup>47</sup> Hanya individu yang telah mencapai batas usia tertentu sebagaimana ditentukan oleh Undang-undang yang dipandang mempunyai kecakapan untuk bertanggung jawab dan berkewajiban mempertanggungjawabkan tindakannya. Ketentuan ini didasarkan pada pertimbangan bahwa faktor usia berpengaruh terhadap kondisi psikologis seseorang yang dapat memengaruhi cara ia bertindak atau mengambil keputusan dalam berbuat suatu perbuatan.

Pada hakikatnya, anak pada usia tertentu belum memiliki kemampuan penuh untuk memahami secara jelas perbuatan yang dilakukannya. Dengan kata lain, pada tahap usia tersebut anak belum mampu untuk mencari perbedaan antara perilaku yang benar dan yang salah, sehingga hal ini cukup berpengaruh terhadap faktor ketidakmampuannya dalam memahami makna dari tindakannya sendiri.

Apabila anak pada umur tertentu yang belum dapat membedakan perbuatan yang benar dan salah melakukan tindak pidana dan dikarenakan tindakannya diterapkan proses pembedaan

---

<sup>47</sup> Afridus Darto, Arif Syahrul Alam. et al., 2023, Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pembunuhan Pengidap Gangguan Kejiwaan Dalam Perspektif Hukum Pidana, *Jurnal Ilmu Hukum Wijaya Putra*, Vol. 1 No. 2, hlm. 262

maka mental anak tersebut dapat terganggu di kehidupan saat ia tumbuh dewasa.

KUHP tidak mengatur terkait kemampuan dalam bertanggung jawab tetapi dalam KUHP sendiri diatur mengenai kebalikan dari kemampuan bertanggung jawab.<sup>48</sup> Pasal 44 KUHP mengatur mengenai kebalikan dari kemampuan bertanggung jawab.

Dalam pasal 44 ini seseorang yang berbuat tindak pidana tidak bisa dikenai pertanggungjawaban atas tindakan yang telah dirinya perbuat jika tidak memenuhi unsur kemampuan bertanggung jawab.

Unsur kemampuan seseorang bertanggung jawab didalam diri pembuat mempunyai kesalahan, kesalahan tersebut ada dua yaitu pembuat mengalami gangguan atau keterbelakangan mental yang mengakibatkan ketidakmampuannya dalam memisahkan antara perbuatan yang benar dan perbuatan yang salah saat ia dalam masa perkembangan dan apabila ia menderita suatu penyakit yang menyebabkan fungsi akalnya tidak bekerja secara normal atau mengalami penurunan kemampuan berpikir<sup>49</sup>

Dalam proses penjatuhan pidana, hakim berkewajiban menelusuri dan membuktikan apakah pelaku memiliki kemampuan untuk mempertanggungjawabkan perbuatannya. Hal ini penting karena pelaku terbukti tidak mempunyai kecakapan bertanggung

---

<sup>48</sup> Jhon Tyson.P., Ismansyah. et al., 2025, *Inkonsistensi Penerapan Sanksi Pidana Pada Undang-Undang Perkebunan*, CV. Green Publisher Indonesia, Jawa Barat, hlm. 38

<sup>49</sup> Firdaus Renuat, Padrisan Jamba. et al., 2023, *Pengantar Hukum Pidana*, CV. Gita Lentera, Sumatera Barat, hlm. 73



jawab, disebabkan oleh faktor usia yang belum memenuhi ketentuan maupun karena adanya gangguan kondisi psikologis, maka pelaku tersebut tidak dapat dimintai pertanggungjawaban atas perbuatannya.<sup>50</sup>

d. Tidak ada alasan pemaaf

Dalam proses pengenaan pidana kepada seseorang yang terbukti berbuat tindak pidana, diperlukan pembuktian bahwa pelaku tidak mempunyai kemampuan dalam bertanggung jawab serta berbuat dengan unsur kesengajaan atau kelalaian. Selain itu, harus dipastikan pula bahwa pada diri pembuat tidak terdapat alasan pemaaf, yaitu alasan yang dapat menghapuskan kesalahan dari terdakwa.<sup>51</sup> Jika pengertian alasan pemaaf dipahami seperti demikian, maka alasan tersebut hanya berfungsi untuk menghapus kesalahan yang ada pada diri terdakwa sehingga ia tidak dapat dijatuhi pidana. Hal ini dipedomankan pada asas bahwa tidak ada pidana tanpa adanya kesalahan. Namun, perlu dipahami bahwa penyebab seseorang tidak dapat dipidana tidak semata-mata karena adanya alasan pemaaf, melainkan juga dapat disebabkan oleh adanya alasan pembenar.

Dalam doktrin hukum pidana, alasan pembenar dan alasan pemaaf dibedakan karena keduanya memiliki peran yang tidak

---

<sup>50</sup> Agus Rusianto, 2016, *Tindak Pidana dan Pertanggung Jawaban Pidana*, Prenadamedia Group, Jakarta, hlm.80

<sup>51</sup> Arianus Harefa, 2023, *Dasar-Dasar Hukum Pidana Di Indonesia-Pasca Berlakunya KUHP Nasional*, CV jejak anggota IKAPI, Jawa Barat, hlm. 233

sama. Perbedaan tersebut terletak pada hakikatnya, di mana alasan pembeda berfungsi untuk memberikan “pembedaan” terhadap suatu perbuatan yang secara hukum dianggap melanggar, sedangkan alasan pemaaf berfokus pada pemberian “pemaafan” kepada pelaku meskipun ia telah melakukan tindakan yang bertentangan dengan hukum pidana..<sup>52</sup>

Alasan pembeda dan alasan pemaaf muncul karena dalam kondisi tertentu pelaku tindak pidana tidak memiliki pilihan lain selain melakukan perbuatan yang dilarang, meskipun sebenarnya ia tidak menghendakinya. Akibat dari tindakannya tersebut, pelaku tetap harus berhadapan dengan proses hukum. Situasi semacam ini tidak dapat dihindari oleh pelaku, karena tindakan yang dilakukannya didorong oleh faktor eksternal yang mempengaruhi kehendaknya.

Faktor-faktor eksternal maupun batiniah yang memengaruhi pelaku tindak pidana dapat menyebabkan dirinya tidak memiliki pilihan lain untuk bertindak, sehingga kesalahannya dianggap hapus. Dengan kata lain, dalam kondisi tersebut pelaku memperoleh alasan penghapusan pidana, dan pertanggungjawaban pidananya ditunda hingga dapat dipastikan ada atau tidaknya unsur alasan pemaaf dalam diri pelaku tindak pidana tersebut.

---

<sup>52</sup> Hanafi Amrani, Mahrus Ali, *Op Cit.*, hlm.45

Dalam hukum pidana yang termasuk dalam alasan pemaaf yakni tidak cakap bertanggungjawab, terdapat daya paksa, pembelaan terpaksa melampaui batas.<sup>53</sup> Dalam hukum pidana, alasan pembeda mencakup keadaan darurat, pembelaan terpaksa, pelaksanaan peraturan perundang-undangan, serta pelaksanaan perintah jabatan yang sah. Kondisi darurat termasuk ke dalam alasan pembeda karena seseorang dalam situasi tersebut dihadapkan pada dilema dan terpaksa memilih satu tindakan yang dianggap paling tepat. Dalam konteks ini, hakim perlu menelaah dan menentukan apakah seseorang tidak dapat dipidana karena adanya alasan pembeda atau justru karena alasan pemaaf.

#### **4. Subjek Pertanggungjawaban Pidana dalam Konteks Tindak Pidana Siber**

Pada dasarnya subjek pertanggungjawaban pidana adalah manusia yang melakukan perbuatan pidana. Namun, perkembangan hukum memperluas subjek hukum pidana sehingga mencakup korporasi, terutama dalam tindak pidana ekonomi atau kejahatan yang dilakukan dalam kerangka badan hukum.

Dalam era digital prinsip-prinsip klasik pertanggungjawaban pidana menghadapi tantangan baru, khususnya dalam kasus kejahatan siber. Perkembangan teknologi ini memunculkan diskursus mengenai

---

<sup>53</sup> Sumiati Adelina.H., Ica Karina. et al., 2024, Pengantar Hukum Pidana (Teori dan Implementasi Pada Era Revolusi Industri 4.0 Menuju Era Society 5.0), PT. Sonpedia Publishing Indonesia, Jambi, hlm. 76

kemungkinan AI atau sistem otonom menjadi subjek pertanggungjawaban pidana.

Hal ini sangat mungkin dilakukan karena mengingat kejahatan di dunia siber semakin marak terjadi. Kejahatan seperti pemalsuan identitas digital melalui teknologi *Deepfake* menimbulkan kesulitan dalam hal identifikasi pelaku, pembuktian kesalahan, serta atribusi pertanggungjawaban.

Saat ini Hukum positif di Indonesia belum mengakui AI sebagai subjek hukum pidana, maka pertanggungjawaban pidananya akan dibebankan pada pengguna, pengembang, atau pihak yang mengoperasikan teknologi tersebut. Meskipun pembebanan pertanggungjawaban pidana dibebankan sesuai asas umum pertanggungjawaban pidana akan tetapi dalam penerapan dalam konteks pidana berbasis AI memerlukan penyesuaian regulasi dan interpretasi hukum yang lebih adaptif.

## **B. Tinjauan Umum Teknologi *Artificial Intelligence***

### **1. Pengertian Umum *Artificial Intelligence***

*Artificial Intelligence* kerap juga disebut AI atau kecerdasan buatan merupakan salah satu inovasi teknologi yang berkembang pesat pada era digital yang memiliki kemampuan pemecahan masalah layaknya manusia. Menurut Rich and Knight, AI merupakan sebuah studi tentang bagaimana melakukan hal-hal yang pada saat ini dapat dilakukan lebih baik oleh manusia yang dilakukan oleh computer.

Teknologi AI identik dengan mesin cerdas yaitu komputer yang dirancang menyerupai manusia dari segi kepintaran dan kemampuan menyelesaikan sebuah pekerjaan. Bahkan secara fisik dirancang menyerupai manusia agar mampu menyelesaikan berbagai pekerjaan manusia. Mesin ini disebut robot atau dalam bahasa Rusia disebut dengan *robota*.<sup>54</sup>

Menurut Winston dan Prendergast, terdapat beberapa tujuan utama dari pengembangan AI. Pertama, tujuan utama dari AI itu sendiri untuk menciptakan mesin yang memiliki kemampuan berpikir cerdas layaknya manusia. Kedua, untuk memahami hakikat kecerdasan buatan dari sisi ilmiah, yaitu menggali bagaimana proses berpikir dan pengambilan keputusan dapat direplikasi oleh mesin. Ketiga, dari aspek kewirausahaan, pengembangan AI ditujukan agar mesin dapat memberikan manfaat praktis dan efisiensi yang tinggi dalam berbagai bidang kehidupan manusia.

Secara umum, AI dikategorikan menjadi AI lemah, apabila dirancang untuk tugas-tugas spesifik seperti pengenalan suara atau gambar, dan AI kuat apabila memiliki kemampuan untuk melakukan berbagai tugas dan beradaptasi seperti manusia.

AI merupakan bentuk kecerdasan yang ditampilkan oleh sistem buatan, yang umumnya berupa komputer. Teknologi ini dirancang dan diprogram ke dalam komputer dengan tujuan agar mesin tersebut mampu

---

<sup>54</sup> John C. Lennox, 2020, *Pandangan Kristen Tentang Kecerdasan Buatan (Artificial Intelligence) dan Masa Depan Umat Manusia*, Terjemahan Stevy Tilaar, Jawa Timur: Literatur, hlm. 14.



melaksanakan tugas serta menunjukkan tingkat kecerdasan yang menyerupai kemampuan manusia.

Kecerdasan Buatan seperti manusia ini tidak digeneralisasi hanya dengan satu aspek saja, melainkan dengan mengkombinasikan berbagai kemampuan berbeda meliputi kemampuan belajar, mencari alasan, memiliki persepsi, kemampuan memecahkan masalah, dan kemampuan mengenali dengan menggunakan bahasa untuk berkomunikasi.<sup>55</sup>

Beberapa jenis bentuk yang memakai kecerdasan buatan yakni:

- a) Pemrosesan bahasa alami bertujuan agar pengguna AI dapat berinteraksi dan berkomunikasi dengan komputer memakai bahasa sehari-hari.
- b) Pengenalan ucapan memungkinkan manusia untuk berinteraksi dengan komputer melalui suara yang dihasilkan dan diproses oleh sistem AI.
- c) *Computer vision* berfungsi untuk menafsirkan serta mengenali gambar maupun objek nyata dengan bantuan teknologi komputer.
- d) *Intelligent Computer-Aided Instruction* merupakan sistem komputer yang berperan sebagai pelatih yang mampu memberikan bimbingan dan pengajaran.

---

<sup>55</sup> Halifa Haqqi dan Hasna Wijayati, 2019, *Revolusi Industri 4.0 di Tengah Society 5.0*, Penerbit Quadrant, Yogyakarta, hlm. 92

- e) Komputer juga dapat dimanfaatkan sebagai media penyimpanan pengetahuan dari para ahli, sehingga mampu meniru keahlian tersebut dalam memecahkan berbagai permasalahan secara cerdas.

## 2. Regulasi Mengenai *Artificial Intelligence*

Di Indonesia ketentuan hukum yang secara eksplisit mengatur penggunaan AI masih terbatas. Pengaturan mengenai dampak hukum AI dapat ditemukan secara parsial dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta beberapa peraturan turunan yang mengatur keamanan siber dan perlindungan informasi digital. Namun, belum ada ketentuan spesifik yang menegaskan batasan etis maupun pertanggung jawaban hukum dalam penggunaan AI, terutama dalam konteks kejahatan digital seperti *deepfake*.

Di negara lain peraturan mengenai AI mulai dibahas dan dirancang, contohnya yaitu di Uni Eropa dan Amerika. Uni Eropa dan Amerika Serikat menjadi dua yurisdiksi yang menonjol dalam pengembangan kerangka hukum mengenai AI, meskipun keduanya mengadopsi pendekatan yang berbeda secara filosofis maupun normatif.

Uni Eropa menempatkan aspek perlindungan individu, etika, dan kepastian hukum sebagai prioritas utama melalui regulasi yang ketat dan preventif. Sementara itu, Amerika Serikat berfokus pada inovasi, efisiensi ekonomi, dan kebebasan industri, dengan pendekatan aturan yang lebih

adaptif dan berbasis pada bidang yang menerapkan. Meskipun berbeda, kedua yurisdiksi tersebut memiliki tujuan yang sama, yaitu memastikan pengembangan AI yang aman, transparan, dan bertanggung jawab.

### 3. Sejarah *Artificial Intelligence*

Sejak zaman kuno, manusia telah mempunyai imajinasi mengenai mesin yang dapat berpikir dan berperilaku seperti manusia. Dari mitologi Yunani konsep sejarah mengenai AI telah muncul dalam benak manusia jauh sebelum teknologi memungkinkan untuk mewujudkannya. AI merupakan jawaban dari suatu kompleksitas kebutuhan manusia. Herbert Marcuse pernah mengemukakan bahwa “Penemuan merupakan ibu dari segala kebutuhan”. Dengan begitulah AI hadir sebagai bagian dari sejarah perkembangan manusia.

Sejarah kecerdasan buatan (AI) menunjukkan perkembangan pesat baik dari sisi teknologi maupun konsep, yang berfokus pada kemampuan mesin dan komputer untuk meniru kecerdasan manusia. Istilah *Artificial Intelligence* pertama kali diperkenalkan oleh John McCarthy, seorang profesor dari Massachusetts Institute of Technology, dalam konferensi *Dartmouth Summer Research Project on Artificial Intelligence* pada tahun 1956. Konferensi yang diadakan di Dartmouth College tersebut menjadi tonggak awal lahirnya bidang studi AI secara resmi.

Meskipun konsep tentang AI telah lama ada dalam pikiran manusia dan perkembangan pesat mengenai AI terjadi pada tahun 1956, dasar dari kecerdasan buatan ini mulai terbentuk pada abad ke-20 seiring dengan

kemajuan ilmu komputer dan matematika. Seorang ilmuwan matematika asal Inggris, Alan Turing membuat gagasan tentang mesin universal yang dapat menjalankan berbagai perintah secara logis pada tahun 1940-an.

Kemudian dalam makalahnya yang terkenal di tahun 1950, yang berjudul *Computing Machinery and Intelligence*, seorang Turing memengemukakan bahwa suatu mesin dapat dikatakan cerdas jika mesin berkelakuan seperti manusia. Turing menggunakan sebuah tes yang disebut Tes Turing untuk menilai apakah mesin dapat memperlihatkan sikap cerdas seperti manusia. Banyak peneliti mulai terinspirasi oleh gagasan yang Turing lakukan untuk mengembangkan mesin yang dapat berpikir, belajar, dan membuat keputusan secara mandiri.<sup>56</sup>

Pendapat yang dikemukakan Turing tersebut juga diperkuat oleh hasil temuan Newel dan Simon pada tahun 1955 melalui pengembangan *The Logic Theorist* merupakan sebuah program yang mempresentasikan masalah seperti sebuah pohon yang memiliki cabang. Masalah tersebut diselesaikan melalui pemilihan cabang yang tepat. Teori ini menghasilkan sebuah teknologi yang menurut para ahli adalah program AI pertama. Teknologi ini juga menjadi salah satu pencapaian awal yang menggambarkan kemampuan mesin untuk berpikir secara logis.<sup>57</sup>

Sekitar tahun 1956, John McCarthy melalui konferensi *The Dartmouth Summer Research Project on Artificial Intelligence*

---

<sup>56</sup> Sudirwo, Abdul Hadi. et al., 2025, *Artificial Intelligence (Teori, Konsep, dan Implementasi di Berbagai Bidang)*, Jambi, hlm. 2

<sup>57</sup> Feri Sulianta, 2025, *Dasar dan Konsep Modern AI*, Penerbit Feri Sulianta, hlm. 4

mengemukakan pendapatnya mengenai AI. John dalam konferensi tersebut juga mendemonstrasikan mesin buaatannya dengan keunggulan yang dapat menirukan kelakuan manusia.<sup>58</sup> Kemudian dalam konferensi *The Dartmouth* ini juga dihadiri oleh para peneliti perintis AI yang membahas berbagai kemungkinan menciptakan mesin yang memiliki kecerdasan manusia. Tokoh tersebut antara lain seperti John McCarthy, Marvin Minsky,

Pada tahun 1956 dan 1970-an, tokoh peneliti seperti Frank Rosenblatt dan Herbert Simon mengfokuskan penelitian pengembangan pada algoritma AI, termasuk algoritma pencarian dan jaringan saraf pertama. Program awal yang diciptakan merupakan sistem berbasis aturan yang dirancang untuk memecahkan berbagai permasalahan, seperti *Logic Theorist* yang berfungsi membuktikan teorema-teorema matematika serta *General Problem Solver* atau GPS yang digunakan untuk menyelesaikan masalah secara umum.

Perkembangan tersebut mendorong untuk pengembangan berbagai pendekatan awal dalam teknologi kecerdasan buatan, seperti pemrograman simbolik dan sistem berbasis aturan. Pendekatan ini digunakan oleh sistem pakar dalam membantu pengambilan keputusan diberbagai bidang, seperti dalam bidang teknik dan bidang kedokteran. Namun, karena ekspektasi yang terlalu tinggi terhadap pengembangan AI tidak segera terpenuhi yang disebabkan oleh keterbatasan komputasi dan kesulitan menangani

---

<sup>58</sup> Amelia Damayanti & Susi Wulandari, 2024, Artificial Intelligence In The Discourse of Hadith Science, *International Conference on Muslim Society and Thought*, Vol.4, hlm. 330

kompleksitas yang terjadi di dunia nyata. Ini menyebabkan periode yang dikenal sebagai *Winter AI* pada akhir 1970-an dan awal 1980-an, pendanaan dan minat terhadap AI turun drastis.<sup>59</sup>

Pada tahun 1980-an hingga 1990-an, AI mengalami pengembangan kembali yang ditandai dengan munculnya teknik pembelajaran mesin atau *machine learning* yang lebih efisien, termasuk dalam pengembangan jaringan saraf tiruan dan algoritma genetika. Pada periode ini, para peneliti mulai mengfokuskan algoritma yang memungkinkan mesin belajar dari data lebih efektif daripada memprogram mesin dengan aturan jelas.

Dengan memanfaatkan teknik penalaran berbasis pengetahuan seperti representasi pengetahuan, jaringan semantik, serta logika, komputer dapat dimodelkan agar mampu meniru cara manusia berpikir dan melakukan proses penalaran layaknya manusia. Peneliti juga melakukan Pengembangan metode "*backpropagation*" dimana pengembangan ini merupakan kemajuan besar; ini memungkinkan jaringan saraf tiruan untuk mempelajari pola data dengan lebih baik. Selain itu, berbagai aplikasi kecerdasan buatan mulai menggunakan teknik seperti algoritma pohon keputusan dan *Support Vector Machines* (SVM).<sup>60</sup>

Dengan peningkatan pengembangan daya komputasi, ketersediaan data yang cukup besar, dan kemajuan dalam algoritma pembelajaran sistem mesin, AI berkembang pesat di abad ke-21. AI mulai digunakan di ranah

---

<sup>59</sup> Sudirwo, Abdul Hadi. et al., Loc. Cit., hlm. 2

<sup>60</sup> Ibid, hlm. 3



seperti kesehatan, keuangan, transportasi, dan hiburan dan tidak hanya terbatas pada laboratorium penelitian saja. Saat ini algoritma kecerdasan buatan juga digunakan dalam mendiagnosis penyakit, mengoptimalkan jalannya rute transportasi, mengelola keuangan, dan menghasilkan konten dalam bentuk teks, gambar, bahkan video.

Dalam bidang seperti pengenalan wajah, pemrosesan bahasa alami atau *Natural Language Processing* atau biasa disebut NLP, dan kendaraan otonom, teknologi seperti *deep learning* menghasilkan terobosan yang cukup besar berkat arsitektur jaringan saraf yang cukup kompleks. Perkembangan Artificial Intelligence terus meningkat. Sejarah perkembangan AI semakin memperlihatkan potensi perkembangan AI yang akan semakin maju seperti sistem aplikasi dalam kehidupan masyarakat.

Namun, dibalik perkembangan yang pesat ini terdapat tantangan etis dan sosial seperti privasi, bias algoritma, dan efek AI terhadap lapangan kerja. Penelitian menunjukkan bahwa di masa depan, AI akan semakin menjadi bagian penting dari kehidupan manusia. Maka hal ini akan membuka jalan baru untuk inovasi teknologi dan otomatisasi di banyak bidang.<sup>61</sup>

#### **4. Cabang Artificial Intelligence**

Perkembangan teknologi yang semakin pesat mendorong meluasnya ruang lingkup penerapan kecerdasan buatan (AI). Saat ini, AI tidak hanya

---

<sup>61</sup> Ibid, hlm. 3

berperan penting dalam bidang ilmu informatika, tetapi juga telah berkembang dan diterapkan di berbagai disiplin ilmu lainnya.

AI tidak dapat dipandang sebagai satu sistem tunggal, melainkan sebagai suatu sistem yang kompleks yang tersusun atas berbagai elemen utama yang saling berhubungan dalam menciptakan bentuk kecerdasan buatan yang mampu meniru bahkan melampaui kemampuan manusia. Komponen-komponen tersebut melibatkan berbagai disiplin ilmu, terutama bidang ilmu komputer dan matematis, yang mengandalkan teknik pemrosesan data secara lebih mendalam dan terstruktur.

Empat elemen utama yang menjadi fondasi AI modern antara lain:<sup>62</sup>

a) *Machine Learning*

*Machine Learning* atau pembelajaran mesin yaitu sebuah bidang AI yang fokus pada perencanaan algoritma dan model yang menunjukkan sistem komputer untuk belajar dari data yang bekerja tanpa pemrograman yang eksplisit. Proses pembelajaran tersebut menghasilkan kemampuan untuk mengenali pola, kemampuan membuat keputusan dengan mempertimbangkan data masa lalu, serta memprediksi kemungkinan yang muncul dari data baru.

Salah satu contohnya dapat dilihat pada penggunaan Gmail yang memiliki fitur filter otomatis untuk mempermudah pencarian pesan dengan cepat. Selain itu, pada perangkat ponsel pintar juga terdapat fitur

---

<sup>62</sup> Singgih Subiyantoro, 2024, Buku Ajar *Artificial Intelligence*, Penerbit Underline (Anggota IKAPI No. 267/JTE/2023), Jawa Tengah, hlm. 32

seperti kalender dan alarm yang berfungsi mengingatkan pengguna pada waktu tertentu terkait kegiatan atau hal penting yang perlu dilakukan.<sup>63</sup>

Terdapat tiga pendekatan utama dalam ML:<sup>64</sup>

- 1) *Supervised Learning*, data yang telah ditentukan label digunakan untuk melatih sistem. Contohnya yaitu klasifikasi email spam
- 2) *Unsupervised Learning*, data tanpa label dan belajar untuk mengidentifikasi pola tersembunyi digunakan untuk melatih sistem. Contohnya yaitu segmentasi pasar
- 3) *Reinforcement Learning*, umpan balik berbasis *reward* dan *punishment* digunakan untuk melatih sistem. Contohnya yaitu robot navigasi atau agen game.

b) *Deep Learning*

*Deep Learning* atau yang sering disebut DL merupakan salah satu cabang dari AI dan bagian dari *machine learning* yang bekerjanya melalui arsitektur jaringan saraf tiruan atau melalui lapisan tersembunyi.<sup>65</sup> Struktur dan fungsi otak manusia menjadi inspirasi dalam teknik yang ada pada sistem ini. Teknik sistem ini mengajarkan untuk melakukan tindakan yang mirip dengan apa yang dilakukan manusia dan pemrosesan data yang sangat tinggi dan konkrit.

*Deep Learning* terbukti efisien dalam mengidentifikasi pola dari data yang bersifat abstrak, seperti gambar, suara, maupun teks.

---

<sup>63</sup> Al- Khorwizmi dan Arif Ridho.L., 2023, *Artificial Intelligence*, UMSU Press, hlm. 13

<sup>64</sup> Singgih Subiyantoro, *Loc. Cit.*, hlm. 32

<sup>65</sup> Ibid, hlm.33

Keunggulan utamanya terletak pada kemampuannya mengekstraksi fitur secara otomatis tanpa memerlukan campur tangan manusia. Adapun contoh penerapan *deep learning* antara lain pada sistem pengenalan wajah, asisten virtual seperti siri, deteksi objek dalam kendaraan otonom, serta penerjemah otomatis berbasis suara atau teks.<sup>66</sup>

c) *Natural Language Processing*

Pengolahan Bahasa Alami atau sering disingkat NLP merupakan salah satu cabang AI yang berfokus dalam interaksi suatu komunikasi antara pengguna *computer* dengan suatu *computer* menggunakan bahasa asli manusia atau bahasa dalam kehidupan sehari-hari manusia. Hal ini dapat tercapai apabila komputer mampu mengekstraksi berbagai informasi dari beragam input berupa bahasa alami dan kemudian menghasilkan output yang juga disajikan dalam bentuk bahasa alami.<sup>67</sup>

Melalui cara yang bermakna dan bermanfaat memberikan mesin untuk paham, menerjemahkan, dan menanggapi dalam bahasa alami manusia. Contoh dari NLP termasuk chatbots yang berkomunikasi dengan manusia atau alat penerjemah otomatis yang dapat menerjemahkan teks dari satu bahasa ke bahasa lain, ada juga dalam sistem deteksi sentiment di media social.

Beberapa komponen penting dalam NLP meliputi:<sup>68</sup>

---

<sup>66</sup> Ibid, hlm.33

<sup>67</sup> Al- Khorwizmi dan Arif Ridho.L., Op Cit., hlm. 10

<sup>68</sup> Singgih Subiyantoro, Loc. Cit., hlm. 33

- 1) *Tokenization*, berperan untuk memisahkan teks ke unit-unit kecil seperti kata atau frasa.
- 2) *Part-of-Speech Tagging*, berperan untuk mengidentifikasi jenis kata seperti kata benda, kata kerja, dsb.
- 3) *Named Entity Recognition* atau *NER*, berperan untuk mengidentifikasi identitas pribadi.
- 4) *Sentiment Analysis*, berperan untuk menentukan perasaan sebuah teks

d) *Computer Vision*

Computer Vision merupakan sebuah cabang dari kecerdasan buatan yang berfokus pada pemahaman hubungan antara objek dan presisi dalam pemrosesan gambar. Teknologi ini memanfaatkan sistem penglihatan berbasis gambar untuk melakukan inspeksi otomatis, mengendalikan proses, serta memandu robot dalam berbagai penerapan baik di lingkungan rumah tangga maupun di sektor industri.<sup>69</sup>

Computer Vision memiliki keterkaitan erat dengan upaya membangun pemahaman dari gambar menuju objek fisik komputer untuk menangkap, memproses, serta menganalisis visual dari lingkungan nyata. Ketika teknologi ini dikombinasikan dengan kecerdasan buatan secara umum, akan dihasilkan sistem cerdas visual atau *Visual Intelligent System*. Penerapan Computer Vision sangat luas, antara lain pada sistem keamanan dan pengawasan seperti *Smart CCTV*,

---

<sup>69</sup> Ibid, hlm. 34

diagnosis medis berbasis citra seperti *CT Scan* dan *MRI*, kendaraan otonom yang memanfaatkan penglihatan komputer untuk mengenali rambu lalu lintas, pejalan kaki, serta kendaraan lain di jalan, hingga aplikasi *Augmented Reality* yang menggabungkan dunia nyata dengan elemen digital. *Computer Vision* memiliki fungsi utama yakni *Image Classification, Object Detection, Segmentation, Facial Recognition*.<sup>70</sup>

## **5. Penerapan *Artificial Intelligence* dalam Berbagai Bidang**

Perkembangan yang cukup pesat terhadap teknologi *Artificial Intelligence*, menghasilkan efek yang luas diberbagai aspek kegiatan manusia. AI kini menjadi suatu unsur penting dalam proses otomatisasi, penganalisisan data, dan pengambilan keputusan di beragam sector publik maupun di sektor privat. Penerapan AI dalam kehidupan sehari-hari juga bertujuan untuk meningkatkan efisiensi, akurasi, serta efektivitas kerja yang dilakukan oleh manusia dalam memanfaatkan kemampuan mesin dalam belajar dan beradaptasi dari data yang tersedia.

Dalam bidang ekonomi dan bisnis, AI berfungsi sebagai instrumen strategis dalam meningkatkan produktivitas dan efisiensi operasional. Penerapan *machine learning* dan *data analytics* memungkinkan perusahaan melakukan analisis perilaku konsumen secara mendalam, memprediksi tren pasar, serta mengoptimalkan strategi pemasaran melalui sistem rekomendasi produk secara otomatis.

---

<sup>70</sup> Ibid, hlm. 34



Di sektor perbankan dan keuangan, AI berfungsi sebagai pendeteksi penipuan, analisis risiko kredit, hingga layanan pelanggan otomatis berbasis *chatbot*. Dengan demikian, AI tidak hanya memberikan efisiensi waktu dalam proses pengambilan keputusan, tetapi juga meminimalisasi kesalahan yang dilakukan manusia di sektor ekonomi.

Di bidang kesehatan, AI memberikan kontribusi signifikan terhadap peningkatan kualitas pelayanan medis. Melalui sistem *medical imaging* dan *predictive analytics*, AI mampu membantu tenaga medis dalam mendiagnosis penyakit secara lebih cepat dan akurat, dan membantu jalannya manajemen rumah sakit. Aplikasi ini juga mampu mendeteksi kelainan pada organ tubuh dengan tingkat akurasi tinggi. Penggunaan *telemedicine* dan *chatbot* berbasis AI turut mempermudah masyarakat terhadap layanan kesehatan jarak jauh. Implementasi AI dalam penelitian farmasi juga mempercepat proses penemuan obat baru melalui analisis data genomik dan simulasi molekuler.

Pada bidang pendidikan, AI berfungsi dalam menciptakan sistem pembelajaran yang bersifat adaptif melalui *adaptive learning systems* yang dapat menyesuaikan materi berdasarkan kemampuan peserta didik. Aplikasi ini juga diterapkan dalam sistem penilaian otomatis, manajemen pembelajaran daring, serta penerjemahan bahasa untuk memperluas akses pendidikan lintas budaya. Dengan demikian, AI berpotensi mempersempit kesenjangan kualitas pendidikan dan meningkatkan efektivitas proses pembelajaran.

Dalam bidang pemerintahan dan keamanan juga mulai mengintegrasikan AI dalam mendukung tata kelola pemerintahan digital, analisis data publik, serta sistem pengawasan keamanan.

Dalam sektor keamanan, AI digunakan dalam sistem pengawasan berbasis *facial recognition* dan analisis perilaku guna mencegah tindak kejahatan. Namun hal itu, penggunaan AI di ranah ini menimbulkan persoalan etis dan hukum, terutama mengenai perlindungan hak pribadi dan hak pribadi sebagai warga berbangsa.

Selain itu, AI juga digunakan dalam bidang transportasi melalui pengembangan kendaraan otonom yang mampu mengemudi tanpa campur tangan manusia dan berpotensi mengurangi angka kecelakaan akibat kelalaian manusia serta meningkatkan efisiensi mobilitas.

Sementara itu, dalam bidang pertanian, AI digunakan untuk mengoptimalkan proses budidaya melalui sistem sensor pintar yang dapat memantau kondisi tanah, cuaca, serta kebutuhan irigasi tanaman secara real time. Dalam bidang hukum, AI mulai diterapkan dalam analisis dokumen hukum, prediksi putusan pengadilan, dan sistem pendukung keputusan hukum.

Di Indonesia, terdapat komitmen terhadap pengembangan dan penerapan AI diwujudkan melalui Strategi Nasional Kecerdasan Artifisial atau biasa disebut Stranas KA 2020–2045 yang ditetapkan oleh Kementerian Komunikasi dan Informatika. Strategi ini menetapkan lima bidang prioritas nasional, yakni kesehatan, pendidikan dan penelitian,

reformasi birokrasi, ketahanan pangan, serta mobilitas dan kota cerdas. Dengan adanya kebijakan ini, AI diharapkan tidak hanya menjadi instrumen teknologi semata, tetapi juga menjadi pilar strategis dalam mendukung pembangunan nasional yang berkelanjutan, inklusif, dan berkeadilan sosial.

## C. Tinjauan Umum Tindak Pidana Pemalsuan

### 1. Pengertian Umum Tindak Pidana Pemalsuan

Menurut Adami Chazawi, tindak pidana pemalsuan merupakan bentuk kejahatan yang mengandung unsur ketidakbenaran mengenai suatu objek, tampak benar dari luar, padahal pada kenyataannya berbeda dengan keadaan sesungguhnya.<sup>71</sup>

Tindak Pidana Pemalsuan merupakan tindak pidana yang kerap terjadi dalam kehidupan manusia dan yang cukup mengganggu masyarakat karena tidak berguna bagi pribadi orang lain dan mengganggu ketertiban umum. Tujuan serta maksud dari perbuatan pemalsuan yaitu untuk mendapatkan keuntungan diri sendiri atau orang lain.

Tindakan pemalsuan dapat dikategorikan sebagai perbuatan dusta atau kebohongan, karena di dalamnya terkandung unsur ketidakjujuran, yaitu tidak menyampaikan kebenaran sebagaimana mestinya. Dalam Al-Qur'an, Allah SWT secara tegas melarang umat-Nya untuk berbuat dusta.

Secara epistemologis, dusta atau *al-kidzb* dipahami sebagai lawan dari *al-shidq* (kejujuran). Terdapat ayat dalam Al-Qur'an yang menegaskan

---

<sup>71</sup> Yogi Fahrissal, 2020, *Penegakan Hukum Pidana Dalam Sengketa Penguasaan Tanah*, CV. Adamu Abimata, Jawa Barat, hlm. 108

larangan Allah SWT terhadap perbuatan dusta. Dalam ayat-ayat tersebut, istilah dusta sering dikaitkan dengan perilaku orang-orang kafir yang tidak membenarkan wahyu Allah SWT dan bahkan menuduh ayat-ayat Al-Qur'an sebagai kebohongan.

Salah satu ayat yang menerangkan perbuatan dusta terdapat dalam Surat A-Baqarah ayat 42, yang berbunyi:<sup>72</sup>

وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ وَتَكُنُوا لِلْحَقِّ وَالْأَنفُسِ يَعْلَمُونَ ﴿٤٢﴾

Artinya: “dan janganlah kamu campuradukkan kebenaran dengan kebatilan dan (janganlah) kamu sembunyikan kebenaran, sedangkan kamu mengetahuinya” (QS. Al-Baqarah: 42)

Tindak pemalsuan dikategorikan sebagai bentuk kejahatan “penipuan”, meskipun tidak semua tindakan penipuan termasuk dalam kategori pemalsuan. Suatu tindakan dianggap sebagai pemalsuan apabila seseorang menggambarkan suatu keadaan seolah-olah benar atau asli, padahal kenyataannya tidak demikian.

Akibat dari gambaran tersebut, pihak lain dapat tertipu dan mempercayai bahwa hal yang digambarkan itu benar adanya. Pemalsuan terhadap tulisan maupun data terjadi ketika isi atau informasi yang sebenarnya tidak asli dibuat tampak seperti aslinya.<sup>73</sup>

---

<sup>72</sup> Al-Qur'an Surat Al-Baqarah Ayat: 42

<sup>73</sup> Milenia Lombogia, Dezen D.R. et al., 2021, Sanksi Terhadap Pelaku Tindak Pidana Penggunaan Surat Palsu Menurut Kitab Undang-Undang Hukum Pidana (KUHP), *Lex Crimen*, Vol. X, No. 9, hlm. 30

Menurut para ahli hukum, penentuan kriteria suatu perbuatan sebagai pemalsuan dapat dilihat dari cara tindak pidana tersebut dilakukan. Tindak pidana pemalsuan dalam KUHP berlandaskan pada beberapa asas, yaitu:

- 1) Tindakan pemalsuan tersebut harus dilakukan dengan tujuan jahat, serta adanya pengakuan terhadap hak atas jaminan keaslian atau kebenaran suatu tulisan maupun data, tindakan pemalsuan tersebut harus dilakukan dengan tujuan jahat;
- 2) Pelaku pemalsuan harus mempunyai niat menimbulkan keyakinan sesuatu yang dipalsukan tersebut terlihat asli.

Perbuatan pemalsuan yaitu tindakan seseorang dengan cara mengubah, meniru, atau membuat sesuatu yang palsu dengan maksud untuk menyesatkan pihak lain atau memperoleh keuntungan yang tidak sah. Tindakan pemalsuan dapat dikategorikan sebagai bentuk pelanggaran terhadap dua norma pokok, yaitu:

- a) Norma mengenai kebenaran dan kepercayaan, di mana perbuatan tersebut termasuk dalam golongan tindak penipuan.
- b) Norma yang berkaitan dengan ketertiban umum di masyarakat, di mana perbuatan tersebut tergolong sebagai kejahatan yang mengancam negara atau ketertiban sosial masyarakat.

## **2. Peraturan Perundang-Undangan dan Jenis-jenis Tindak Pidana Pemalsuan**

Dalam Kitab Undang-Undang Hukum Pidana (KUHP), istilah pemalsuan diatur dalam beberapa ketentuan, antara lain Pasal 263 sampai

dengan Pasal 278 KUHP, yang menjelaskan mencakup pemalsuan surat, mata uang, merek, segel, serta tanda pengenal resmi.

Dalam Buku II KUHP, perbuatan Kejahatan diklasifikasikan menjadi empat golongan, yakni :

- 1) Golongan pertama merupakan kejahatan sumpah palsu yang diatur dalam ketentuan bab IX KUHP
- 2) Golongan kedua merupakan kejahatan pemalsuan uang yang diatur dalam ketentuan bab X KUHP
- 3) Golongan ketiga merupakan kejahatan pemalsuan materai dan merk yang diatur dalam ketentuan bab XI KUHP
- 4) Golongan keempat merupakan kejahatan pemalsuan surat yang diatur dalam bab XII KUHP

Pengklasifikasikan dilihat atas obyek dari pemalsuan. Terdapat enam obyek kejahatan yaitu keterangan di atas sumpah, mata uang, uang kertas, materai, merek dan surat.<sup>74</sup>

Pemalsuan data yang dilakukan melalui media sosial maka akan diterapkan Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik yang telah dibaharui dengan Undang Undang Nomor 16 Tahun 2019 Tentang Informasi dan Transaksi Elektronik dalam Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

---

<sup>74</sup> Fritsky Lantang, Edwin Neil Tinangon. et al., 2024, Penggunaan Tanda Tangan Elektronik Dalam Perjanjian, *Lex Pravatum*, Vol. 14, No. 02, hlm. 8



Secara tidak langsung dapat dikemukakan bahwa individu dilarang memalsukan informasi di media elektronik khususnya internet. Tindak pidana pemalsuan data melalui media internet merupakan kejahatan *cybercrime* yang tindakannya dapat dilakukan oleh perseorangan maupun terorganisir. *Cybercrime*.

Salah satu bentuk kejahatan dalam ranah *cybercrime* adalah pemalsuan identitas, di mana identitas berfungsi sebagai tanda pengenal seseorang. Tindakan pemalsuan data melalui media ini meliputi berbagai dokumen pribadi, seperti akta kelahiran, kartu keluarga, surat nikah, ijazah, KTP, SIM, dan dokumen lainnya. Terdapat pula dokumen niaga yang kerap menjadi objek pemalsuan, antara lain cek, obligasi, saham, wesel, serta kuitansi.<sup>75</sup>

Berdasarkan Pasal 1 ayat (4) Undang-Undang Nomor 19 Tahun 2016, dijelaskan bahwa dokumen elektronik mencakup setiap bentuk informasi elektronik yang dibuat, dikirim, diterima, atau disimpan melalui komputer maupun sistem elektronik, yang dapat berupa tulisan, suara, gambar, huruf, maupun simbol tanpa adanya batasan format.

### **3. Unsur-Unsur Dalam Tindak Pidana Pemalsuan**

Tindak pidana pemalsuan adalah salah satu bentuk kejahatan kepercayaan publik. Esensi dari tindak pidana ini terletak pada tindakan

---

<sup>75</sup> Putri Jeri Astuti, Suwarno Abadi. et al., 2024, Penerapan Sanksi Pidana Terhadap Pelaku Pemalsuan Dokumen Yang Dilakukan Melalui Media Sosial, *Jurnal Ilmu Hukum Wijaya Putra*, Vol. 2, No. 1, hlm. 39

yang mengakibatkan berkurangnya rasa kepercayaan masyarakat terhadap kebenaran dan keaslian suatu dokumen atau identitas.

Dalam konteks hukum pidana, tindak pidana pemalsuan memiliki dua unsur utama, yaitu unsur objektif dan unsur subjektif, yang keduanya harus terpenuhi agar suatu tindakan dapat dikualifikasikan sebagai tindak pidana pemalsuan. Unsur objektif dari tindak pidana pemalsuan terdiri dari tiga hal utama, yaitu:

- 1) Tindakan, yaitu tindakan memalsukan suatu surat atau identitas dengan sengaja. Tindakan tersebut dapat berupa pembuatan dokumen palsu secara keseluruhan maupun merubah sebagian isi dari dokumen yang sebenarnya. Pemalsuan dalam konteks digital, tindakannya dapat berupa manipulasi data elektronik, pengubahan citra digital, atau pembuatan identitas fiktif menggunakan teknologi seperti AI.
- 2) Objek yang dipalsukan, yaitu suatu surat, tanda pengenal, dokumen resmi, atau data identitas yang memiliki nilai pembuktian hukum. Pasal 263 KUHP menyatakan bahwa surat yang dipalsukan harus terdapat kemampuan untuk menimbulkan akibat hukum yang dapat dipakai sebagai alat bukti, sarana administrasi, atau media transaksi. Sehingga, pemalsuan dokumen tidak hanya menyangkut bentuk fisik surat, tetapi juga substansi dan tujuan penggunaannya.
- 3) Akibat yang Ditimbulkan, yaitu pemalsuan yang berpotensi menimbulkan kerugian atau bahaya terhadap kepentingan atau proses hukum, baik terhadap suatu individu maupun masyarakat. Kerugian

tidak semata bersifat materiil, melainkan juga dapat berupa kerugian immateriil misalnya rusaknya reputasi, hilangnya kepercayaan, atau bahkan dapat menimbulkan terganggunya sistem dalam administrasi negara. Dalam pemalsuan identitas digital, akibat hukum dapat berupa penyebaran berita palsu yang dapat menyesatkan informasi publik dan pelanggaran privasi individu.

Unsur subjektif dari tindak pidana pemalsuan berhubungan dengan sikap batin pembuat terhadap tindakannya. Unsur ini mencakup kesengajaan atau *dolus* dan niat atau *opzet* dalam menggunakan atau membuat dokumen palsu yang memiliki tujuan agar terlihat asli dan benar sehingga dapat menimbulkan akibat hukum.

Menurut Moeljanto, kesengajaan dalam tindak pidana pemalsuan berarti pelaku sadar akan perbuatannya itu melanggar hukum dan menghendaki akibat perbuatan itu terjadi. Dengan demikian, unsur subjektif tidak dapat terpenuhi apabila perbuatan yang dilakukan karena kekhilafan atau ketidaktahuan semata. Sehingga unsur-unsur dalam tindak pidana pemalsuan dirumuskan sebagai berikut:

- a) Adanya perbuatan membuat palsu atau memalsukan
- b) Obyek pemalsuan berupa surat atau identitas yang memiliki kekuatan hukum
- c) Adanya akibat hukum yang merugikan kepentingan publik atau individu
- d) Adanya kesengajaan dari pelaku

- e) Adanya maksud atau tujuan untuk menggunakan hasil pemalsuan tersebut seolah-olah benar.

Keseluruhan unsur diatas harus terpenuhi seluruhnya agar seseorang dapat dimintai pertanggungjawaban pidana atas perbuatannya melakukan tindak pidana pemalsuan. Dalam perkembangan modern, termasuk pada kasus pemalsuan identitas digital menggunakan teknologi AI, penafsiran terhadap unsur-unsur ini perlu diperluas mencakup bentuk digital dan elektronik dari dokumen atau identitas, sesuai dengan asas *expansive interpretation* dalam hukum pidana teknologi informasi.

#### **4. Perkembangan Tindak Pidana Pemalsuan Dalam Era Digital**

Perkembangan teknologi informasi dan komunikasi menimbulkan efek terhadap bentuk dan modus operandi tindak pidana, termasuk tindak pidana pemalsuan. Dahulu, pemalsuan identik dengan tindakan mengubah atau membuat surat, dokumen, dan tanda tangan asli ke palsu secara fisik yang menimbulkan akibat hukum. Namun di era digital, pemalsuan telah berevolusi menjadi bentuk kejahatan yang lebih kompleks, mencakup manipulasi data elektronik, dokumen digital, hingga identitas pribadi berbasis teknologi. Perubahan ini menuntut adaptasi hukum pidana agar dapat menjangkau tindak pidana yang timbul di ruang siber, termasuk dalam konteks pemalsuan digital.

Pemalsuan digital merupakan tindakan mengubah, memalsukan, atau menciptakan informasi elektronik sedemikian rupa sehingga tampak seolah-olah benar dan autentik. Dalam konteks hukum Indonesia, perbuatan ini

diatur dalam Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau kerap disebut UU ITE sebagaimana telah diubah dengan UU No. 19 Tahun 2016, tentang manipulasi dokumen tanpa izin dan merugikan orang lain. dengan tujuan agar dianggap data tersebut benar dan autentik dapat dipidana.<sup>76</sup> Ketentuan ini menunjukkan bahwa hukum telah berusaha mengantisipasi bentuk pemalsuan modern yang tidak lagi terbatas pada dokumen fisik, melainkan juga meliputi data digital yang memiliki kekuatan pembuktian hukum dalam transaksi elektronik.

Dalam perkembangan lebih modern, muncul bentuk pemalsuan digital yang memanfaatkan teknologi AI, salah satunya adalah fenomena *deepfake*. *Deepfake* menggunakan algoritma pembelajaran mendalam atau kerap disebut *deep learning* untuk memanipulasi citra, suara, dan video seseorang sehingga tampak realistis dan sulit dibedakan dari yang asli.

Teknologi ini menimbulkan ancaman serius terhadap privasi individu, keamanan informasi, dan kepercayaan publik terhadap kebenaran visual.<sup>77</sup> Dalam konteks hukum pidana, konten *deepfake* dapat dikategorikan sebagai bentuk pemalsuan identitas digital karena memenuhi unsur membuat sesuatu yang palsu agar dianggap benar dan menimbulkan akibat hukum, seperti kerugian reputasi atau penipuan digital.

---

<sup>76</sup> Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan UU No. 19 Tahun 2016.

<sup>77</sup> Chesney, Robert & Citron, Danielle Keats, 2019, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, *California Law Review*, Vol. 107, No. 6

Selain itu, kemajuan teknologi telah memunculkan bentuk pemalsuan berbasis data biometrik seperti sidik jari, wajah, dan suara digital. Kejahatan ini dikenal dengan istilah identity theft atau pencurian identitas digital. Pencurian identitas digital merupakan bentuk lanjutan dari tindak pidana pemalsuan karena pelaku dengan sengaja menggunakan data pribadi orang lain untuk memperoleh keuntungan atau menghindari tanggung jawab hukum.<sup>78</sup> Fenomena ini menegaskan bahwa pemalsuan tidak hanya terkait dengan pengubahan dokumen, tetapi juga melibatkan manipulasi identitas sebagai bentuk serangan terhadap hak personal dan integritas data.

Perkembangan tindak pidana pemalsuan di era digital juga mendorong munculnya berbagai regulasi baru di Indonesia. Selain UU ITE, terdapat Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi atau biasa disebut UU PDP yang memperluas perlindungan hukum terhadap data pribadi dan identitas digital. Pasal 67 UU PDP mengemukakan bahwa setiap orang yang secara melawan hukum memperoleh atau menggunakan data pribadi orang lain untuk tujuan yang merugikan dapat dikenakan sanksi pidana.<sup>79</sup> Ketentuan ini memperkuat aspek perlindungan hukum dalam ranah digital, termasuk terhadap pemalsuan identitas berbasis AI.

## **D. Tinjauan Umum Identitas Digital**

### **1. Konsep dan Pengertian Identitas Digital**

---

<sup>78</sup> Setiawan, R., 2023, Pemalsuan Identitas Digital dalam Perspektif Hukum Siber, *Jurnal Hukum dan Teknologi*, Vol. 5, No. 2.

<sup>79</sup> Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi



Identitas digital merupakan bentuk elektronik dari identitas seseorang di ruang siber yang mencakup kumpulan data dan informasi yang dapat digunakan untuk mengenali, memverifikasi, serta mengautentikasi individu dalam aktivitas digital.

Dalam Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022 menyatakan identitas digital merupakan sebuah informasi elektronik digunakan untuk memperlihatkan dokumen dalam aplikasi digital melalui gawai yang menampilkan data pribadi sebagai identitas yang bersangkutan.<sup>80</sup>

Secara umum, identitas digital mencakup nama pengguna, kata sandi, alamat email, tanda tangan elektronik, data biometrik, dan berbagai informasi pribadi lainnya yang tersimpan dalam sistem elektronik.

Menurut Daniel J. Solove, identitas digital merupakan kumpulan jejak digital yang secara keseluruhan membentuk representasi individu dalam dunia maya. Identitas ini menjadi kunci utama dalam berbagai kegiatan elektronik seperti transaksi elektronik, interaksi daring, dan sistem pemerintahan berbasis digital yang semakin berkembang di era transformasi teknologi.

Identitas digital termasuk dalam kategori informasi elektronik yang memiliki akibat hukum, karena dapat digunakan untuk mengidentifikasi seseorang dan memiliki konsekuensi hukum apabila disalahgunakan. Oleh karena itu, identitas digital di mata hukum adalah sebuah data pribadi yang

---

<sup>80</sup> Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022

harus dilindungi oleh negara dan dijaga penggunaannya oleh setiap individu.

Perbedaan utama antara identitas fisik dan identitas digital terletak pada bentuk eksistensi dan mekanisme pengendaliannya. Identitas fisik biasanya diwujudkan dalam dokumen resmi seperti KTP, paspor, atau SIM, yang dikelola oleh lembaga pemerintah. Sedangkan identitas digital bersifat virtual, terbentuk melalui sistem elektronik yang digunakan oleh lembaga publik maupun swasta, serta dapat terdistribusi di berbagai platform digital secara global.

Identitas digital bersifat dinamis, karena dapat berubah sewaktu-waktu, dan memiliki risiko tinggi terhadap penyalahgunaan karena tersimpan dalam sistem jaringan yang rentan terhadap serangan siber. Maka dari itu, perlindungan hukum terhadap identitas digital tidak hanya menyangkut aspek privasi individu, namun juga menyangkut kepercayaan publik terhadap sistem digital dan integritas data dalam ruang siber.

Selain berfungsi sebagai sarana autentikasi dan verifikasi identitas dalam dunia digital, identitas digital juga memiliki nilai ekonomi dan hukum yang tinggi. Dalam konteks transaksi elektronik, identitas digital digunakan untuk memastikan keabsahan subjek hukum yang melakukan perbuatan hukum secara daring, seperti dalam kontrak elektronik atau layanan perbankan digital.

Identitas digital dapat menimbulkan implikasi hukum baru, karena segala bentuk penyalahgunaan terhadap identitas tersebut dapat

dikategorikan sebagai tindak pidana apabila menimbulkan akibat hukum, seperti kerugian, penipuan, atau pencemaran nama baik. Identitas digital tidak entitas teknis, melainkan subjek yang memiliki dimensi hukum pidana, perdata, dan administrasi.

Sehingga, identitas digital pada hakikatnya merupakan konstruksi hukum dan teknologi yang menggambarkan eksistensi seseorang di dunia maya. Perlindungan terhadap identitas digital memiliki urgensi yang tinggi dalam rangka menjamin hak privasi, keamanan transaksi elektronik, dan kepercayaan publik terhadap sistem digital.

Oleh sebab itu, pemahaman mengenai identitas digital tidak hanya perlu dilihat dari aspek teknologinya, tetapi juga dari sudut pandang hukum pidana yang bertujuan untuk mencegah dan menindak penyalahgunaan identitas yang dapat mengancam hak dan kepentingan hukum masyarakat di era digital.

## **2. Dasar Hukum Identitas Digital di Indonesia**

Identitas digital merupakan representasi elektronik dari identitas seseorang yang diakui secara hukum di Indonesia. Pengakuan ini dibuktikan karena terdapat peraturan perundang-undangan yang membentuk kerangka hukum nasional terkait aktivitas digital. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau biasa disebut UU ITE beserta perubahannya melalui Undang-undang Nomor 19 Tahun 2016 menjadi dasar utama pengakuan identitas digital.

Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi atau biasa disebut UU PDP memperkuat perlindungan hukum terhadap identitas digital sebagai bagian dari hak atas privasi. Pasal 1 angka 2 UU PDP mendefinisikan data pribadi sebagai setiap data yang dapat mengidentifikasi individu, termasuk elemen-elemen digital seperti nama, foto, alamat IP, dan sidik jari elektronik. Undang-undang ini juga memberikan sanksi terhadap penyalahgunaan data pribadi yang berkaitan dengan perlindungan identitas digital dari pemalsuan atau penyebaran tanpa izin.

Lebih lanjut, Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik atau disingkat menjadi SPBE menegaskan pentingnya identitas digital dalam integrasi layanan publik berbasis teknologi. Identitas digital juga berakar pada Undang-undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan, yang memperkenalkan *e-KTP* sebagai bentuk identitas elektronik nasional dan menjadi basis sistem identitas digital.

Keberadaan identitas digital di Indonesia memiliki legitimasi hukum yang kuat. Keseluruhan regulasi tersebut menunjukkan bahwa Indonesia telah membangun kerangka hukum komprehensif dalam mengatur dan melindungi identitas digital warga negara, baik dari aspek administrasi, transaksi elektronik, maupun perlindungan data pribadi.

## **E. Tinjauan Umum Pemalsuan Identitas Digital atau *Deepfake***

### **1. Pengertian dan Mekanisme *Deepfake***

Istilah *deepfake* berasal dari gabungan dua kata, yakni “*deep learning*” dan “*fake*”. Secara umum, *deepfake* merujuk pada konten audio visual palsu seperti foto, video, maupun suara, yang dihasilkan menggunakan metode *deep learning*. Teknologi *deep learning* merupakan bagian dari *Artificial Intelligence* berfokus pada pemrosesan algoritma agar mampu belajar sendiri dan mengambil keputusan cerdas, sehingga dapat digunakan untuk melakukan pemalsuan identitas dalam bentuk digital.

*Deepfake* bertujuan untuk menciptakan sintesis citra manusia, dengan sebuah gambar digabungkan dengan metode tertentu sehingga hasilnya terlihat nyata padahal kenyataannya tidak *pernah* terjadi. Tujuan awal dari teknologi *deepfake* ini hanya untuk hiburan, namun seiring berjalannya waktu penggunaan *deepfake* mulai bergeser ke penggunaan yang negatif yang akibatnya mengikis kepercayaan masyarakat. Contohnya yaitu digunakan dalam pemalsuan identitas digital.

*Deepfake* dapat muncul dalam berbagai bentuk teknologi yang menjadi tantangan serius dalam mengetahui keaslian pada konten multimedia. *Deep learning*, yang pada awalnya dikembangkan untuk kepentingan industri seperti pengenalan wajah dan suara, kini juga dimanfaatkan dalam pembuatan konten palsu berbasis teknologi *deepfake*.

Bentuk-bentuk penerapan *deepfake* antara lain sebagai berikut: <sup>81</sup>

#### 1) Video *Deepfake*

---

<sup>81</sup> Anfa'un Nisa'.F.R., Syariffudin., et al., 2025, Perlindungan Hukum Terhadap Korban Penyalahgunaan Teknik *Deepfake*, *Perspektif Administrasi Publik dan Hukum*, Vol. 2, No. 1, hlm. 250

Pada jenis ini, pelaku dapat menghasilkan rekaman visual yang hampir tidak dapat dibedakan dari aslinya. Wajah serta gerakan seseorang dapat digantikan secara presisi, menciptakan ilusi yang tampak nyata dan meyakinkan.

## 2) Audio *Deepfake*

Dalam format suara, manipulasi dilakukan dengan meniru atau meretas suara seseorang, sehingga dapat menciptakan rekaman percakapan atau pernyataan palsu dengan tingkat keaslian yang sangat tinggi.

## 3) Foto *Deepfake*

Jenis ini dilakukan dengan menggabungkan elemen-elemen visual dari berbagai sumber untuk menghasilkan gambar yang tampak autentik. Pemalsuan ini dapat meliputi wajah, ekspresi, maupun konteks visual, sehingga foto yang dihasilkan terlihat nyata padahal telah mengalami manipulasi digital.

Seiring berjalannya waktu dan berkembangnya teknologi, penggunaan teknologi *deepfake* ini mulai bergeser ke lingkup yang negatif. Terdapat pemalsuan identitas di ruang *siber* yang dilakukan menggunakan teknologi *deepfake*. Penyalahgunaan teknologi *deepfake* ini telah menimbulkan masalah etika yang serius di dunia modern karena memungkinkan untuk manipulasi gambar dan suara yang sangat rumit dan terlihat nyata.

*Deepfake* nampaknya menjadi fenomena yang memerlukan pemahaman dan perhatian mendalam serta pertimbangan etis jika dilihat



melalui perspektif Islam. Terutama dalam *Al-Qura'n*, kitab suci agama Islam yang menawarkan moral dan etika. Umat Islam dalam menjalani kehidupannya harus sesuai dengan cita-cita dan pedoman agama, seperti kejujuran, integritas, dan menjauhi segala bentuk penipuan dan dusta, dengan mengikuti tuntunan yang diberikan oleh *Al-Qur'an*.

Kemampuan *deepfake* untuk menghasilkan pesan visual atau audio palsu yang tampak nyata *namun* sebenarnya merupakan hasil dari manipulasi yang sangat canggih akan berdampak pada pemahaman dan kepercayaan masyarakat terhadap informasi dan kenyataan.<sup>82</sup> Meskipun berpengaruh dalam kemajuan di bidang digital, teknologi ini cukup membahayakan integritas informasi dan kepercayaan publik.

Integritas dan kejujuran merupakan sebuah nilai fundamental yang menjadi pedoman dalam menjalani kehidupan bermasyarakat, hal itu sesuai dengan ajaran yang ada di dalam kitab suci *Al-Qur'an*. Oleh karena itu, teknologi seperti *deepfake* tidak hanya membahayakan keakuratan informasi saja namun juga dapat menyoroiti pentingnya prinsip moral dan etika dalam menegakkan keadilan dan kebenaran dalam kehidupan masyarakat.

*Al-Qur'an* menegaskan atau mengajarkan pentingnya untuk mengikuti jalan yang benar, menghindari *kebohongan* dan perbuatan dusta, serta menjaga kejujuran, seperti yang tercantum dalam salah satu ayat-ayat

---

<sup>82</sup> Faras Paria, 2024, "Fenomena Deepfake di Era Teknologi Informasi Perspektif *Al-Qur'an* (Studi Kasus Analisis Q.S *Al-Baqarah* Ayat 42)", *Skripsi Fakultas Ushuluddin dan Pemikiran Islam UIN Raden Fatah, Palembang*, hlm. 7

yang menekankan mengenai kebenaran, seperti dalam Q.S. Al- Maidah ayat 8:<sup>83</sup>

يَا أَيُّهَا الَّذِينَ آمَنُوا كُونُوا قَوَّامِينَ لِلَّهِ شُهَدَاءَ بِالْقِسْطِ وَلَا يَجْرِمَنَّكُمْ شَنَا نُ قَوْمٍ عَلَىٰ أَلَّا تَعْدِلُوا ۖ اْعْدِلُوا ۚ هُوَ أَقْرَبُ لِلنَّقْوَىٰ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ خَبِيرٌ بِمَا تَعْمَلُونَ

Artinya: "Wahai orang-orang yang beriman, jadilah kamu penegak (kebenaran) karena Allah (dan) saksi-saksi (yang bertindak) dengan adil. Janganlah kebencianmu terhadap suatu kaum mendorong kamu untuk berlaku tidak adil. Berlakulah adil karena (adil) itu lebih dekat pada takwa. Bertakwalah kepada Allah. Sesungguhnya Allah Maha teliti terhadap apa yang kamu kerjakan." (QS. Al Maidah: 8)

## 2. Regulasi Hukum Terkait Teknologi *Deepfake*

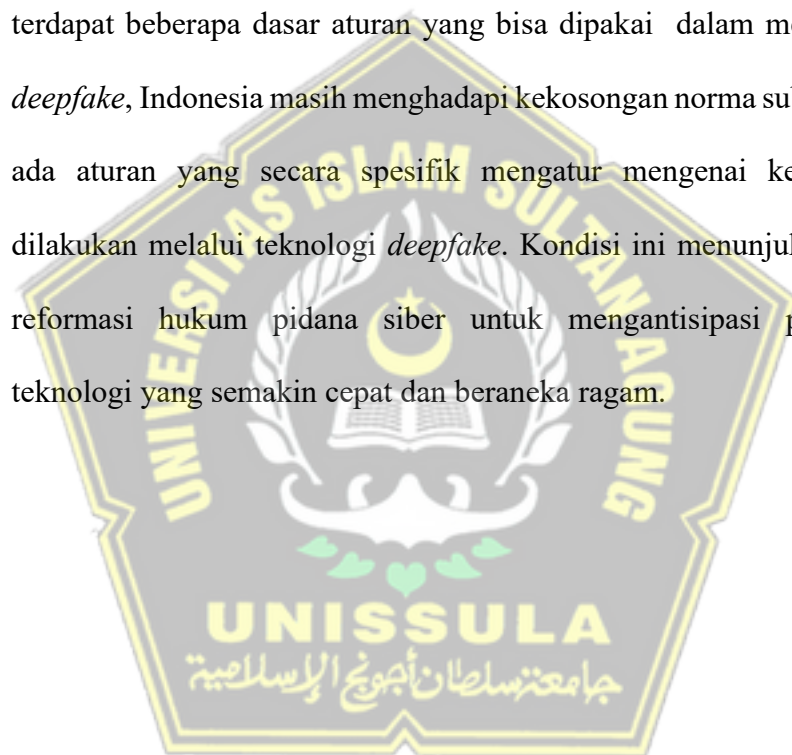
Dalam ranah hukum, Indonesia hingga kini tidak ada peraturan yang spesifik dan tegas membahas mengenai fenomena deepfake atau pemalsuan identitas digital. Kendati demikian, beberapa ketentuan hukum yang sudah berlaku dapat dijadikan landasan yuridis untuk menjerat pelaku kejahatan yang memanfaatkan teknologi tersebut, terutama melalui pendekatan terhadap unsur pemalsuan, penyebaran informasi palsu, serta pelanggaran terhadap privasi individu. Pengaturan yang relevan dalam sejumlah peraturan perundang-undangan, baik yang mencakup hukum pidana umum, hukum siber, maupun perlindungan data pribadi.

Beberapa pasal dalam Undang-Undang Informasi dan Transaksi Elektronik atau biasa disebut dengan UU ITE dapat dijadikan acuan hukum

---

<sup>83</sup> Al-Qur'an Surat Al-Maidah ayat 8

dalam menindak penyalahgunaan teknologi *deepfake*. Contohnya, Pasal 27 ayat (3) UU ITE mengatur mengenai pencemaran nama baik, sedangkan Pasal 28 ayat (1) mengatur tentang penyebaran berita bohong yang dapat merugikan masyarakat. Selain itu, Pasal 310 ayat (2) KUHP W.v.S juga memberikan dasar hukum mengenai ancaman pidana terhadap pelaku pencemaran nama baik yang dilakukan melalui media digital. Walaupun terdapat beberapa dasar aturan yang bisa dipakai dalam menjerat pelaku *deepfake*, Indonesia masih menghadapi kekosongan norma substantif. Tidak ada aturan yang secara spesifik mengatur mengenai kejahatan yang dilakukan melalui teknologi *deepfake*. Kondisi ini menunjukkan perlunya reformasi hukum pidana siber untuk mengantisipasi perkembangan teknologi yang semakin cepat dan beraneka ragam.



### BAB III

#### HASIL PENELITIAN DAN PEMBAHASAN

##### A. Bentuk Tindak Pidana Pemalsuan Identitas Digital *Deepfake* di Ruang Digital Menggunakan Teknologi *Artificial Intelligence* Menurut Hukum Positif di Indonesia

Perkembangan yang cukup pesat dalam teknologi informasi dan komunikasi mendorong transformasi dalam kehidupan sehari-hari manusia, seperti dalam cara manusia berinteraksi, bertransaksi, dan mengekspresikan diri di ruang digital. Wujud nyata dari perkembangan teknologi yang sangat cepat yakni Perkembangan teknologi pada bidang kecerdasan buatan atau *Artificial Intelligence* yang menghadirkan banyak dampak yang signifikan dalam aspek kehidupan.

*Artificial Intelligence* atau kerap disebut juga dengan AI merupakan suatu sistem komputer yang mampu meniru kecerdasan manusia melalui proses pembelajaran atau *machine learning*, pengenalan pola atau *pattern recognition*, serta analisis data dalam skala besar. Salah satu cabang dari teknologi AI yang kini sangat sering dimanfaatkan oleh manusia di berbagai bidang dan menjadi perhatian serius dalam bidang hukum adalah *deepfake*.

*Deepfake* adalah suatu teknologi yang menggunakan teknologi AI guna untuk menciptakan suatu video atau gambar palsu yang merepresentasi wajah, suara, atau gerakan seseorang secara digital, sehingga tampak autentik walaupun sebenarnya palsu dengan tujuan untuk melakukan penipuan identitas. Cara kerja *deepfake* pada teknologi AI ini menggunakan logaritma *machine*

*learning* serta jaringan saraf tiruan yang dapat mempelajari dengan dalam data secara visual maupun audio dari seseorang.<sup>84</sup>

Pada awalnya teknologi *deepfake* ini digunakan dalam bidang kreatif maupun hiburan saja. Akan tetapi karena perkembangan teknologi yang sangat pesat dan sulit dalam mengontrol arus perkembangannya, penggunaan teknologi *deepfake* ini berubah kearah yang negatif. Selain itu perubahan pemanfaatan yang negatif ini disebabkan oleh hasil dari kecerdasan buatan dengan teknologi *deepfake* ini, seperti tidak dapat dibedakan antara mana yang asli dan yang buatan AI sehingga dari hal-hal tersebut membuka ruang atau potensi besar di berbagai hal dalam penggunaannya baik itu digunakan untuk hal yang positif maupun kearah yang negatif.

Dalam perkembangannya teknologi *deepfake* ini terbagi dalam lima kategori utama. Kategori utama tersebut terdiri dari:<sup>85</sup>

#### **1. *Attribute manipulation***

Kategori ini berfokus pada manipulasi bagian tertentu dari wajah dengan memanfaatkan teknik pengubahan fitur atau atribut spesifik, seperti menambahkan atau menghapus kacamata, memperhalus tekstur kulit, serta mengubah elemen fisik lainnya seperti usia, jenis kelamin, warna rambut, warna mata, maupun ekspresi wajah.

---

<sup>84</sup> Sri Maharani M.T.V.M & Rambu Earyca Maharani, 2025, Ganti Kerugian Akibat Penyalahgunaan *Artificial Intelligence (Deepfake)* pada Citra Orang Terkenal di Facebook Berdasarkan Pasal 1365 BW, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol. 6, No. 4, hlm. 7

<sup>85</sup> Naitali, A., Ridouani, M., Salahdine, F. et al., 2023, Deepfake attacks: Generation, detection, datasets, challenges, and research direction. *Computers*, Vol. 12, No. 10, hlm. 26.

Kategori ini Sering juga disebut dengan istilah perbaikan wajah atau *face retouching*. Contoh peberapannya terdapat pada aplikasi seperti *FaceApp* yang memungkinkan pengguna mengubah ekspresi wajah atau usia mereka dalam foto.

Pada kategori ini manipulasi diarahkan sebagian besar dalam format video karena tingkat keterlibatannya yang lebih tinggi dibandingkan dengan konten berbasis gambar. Akibatnya, orang lebih mungkin menjadi korban video *deepfake*. Manipulasi kategori ini dirancang untuk membuat terlihat nyata seolah-olah seseorang melakukan atau mengatakan sesuatu yang sebenarnya tidak mereka lakukan atau katakan.

## 2. *Entire face synthesis*

Kategori ini menggunakan teknik modifikasi wajah yang digunakan untuk menghasilkan wajah yang tidak ada dalam kehidupan nyata. Teknik seperti ini memanfaatkan GAN atau *Generative Adversarial Network* dan dapat menghasilkan gambar wajah berkualitas tinggi.

Contoh penerapannya biasa digunakan dalam pembuatan *video game* dan pembuatan video pemodelan 3D. Namun, kategori ini telah banyak digunakan oleh pelaku kejahatan untuk tujuan yang jahat.

## 3. *Lyp-syncing*

Kategori ini memungkinkan wajah target terlihat realistis dan tersinkronisasi dengan input berupa teks atau audio, sehingga pergerakan bibir tampak alami dan ekspresi wajah sesuai dengan suara sumber. Selain



teknik *lip-sync*, terdapat pula teknologi kloning suara yang memiliki keterkaitan erat dengan metode tersebut.

Kloning suara mereplikasi suara seseorang, sementara *lip-sync* mencocokkan gerakan bibir dalam video dengan audio yang diubah atau baru. Manipulasi ini dapat membuat seseorang seolah-olah mengatakan sesuatu yang tidak pernah mereka katakan.

Kategori seperti ini seringkali disalahgunakan contoh dari penyalahgunaannya adalah dalam pembuatan video yang membuat tokoh publik terlihat mengucapkan sesuatu yang tidak pernah mereka katakan, atau pada dialog film ke bahasa lain dengan gerakan bibir yang sempurna.

#### 4. *Face re-enactment*

Kategori ini pengubahan suatu ekspresi wajah dalam video menggunakan wajah sumber untuk menginspirasi perubahan wajah target. Teknik ini mengambil ekspresi dan gerakan wajah seseorang dan mentransfernya ke wajah orang lain ke suatu video.

Hasilnya orang target akan menampilkan ekspresi yang sama dengan orang sumber, meskipun mereka tidak benar-benar melakukannya. Perubahan tersebut termasuk ekspresi, tatapan, mulut, pose, atau tubuh target. *Deepfake re-enactment* memberikan kemungkinan kepada penyerang untuk memanipulasi konten digital melalui peniruan identitas korban. Dengan modal video dan gambar yang tersedia, pelaku dapat memanfaatkan GAN atau *Generative Adversarial Network* untuk

meregenerasi individu secara digital dengan kemampuan untuk mengendalikan ucapan, ekspresi, dan tingkah lakunya.

Kategori *deepfake* ini menciptakan peluang bagi pelaku untuk merusak bukti hukum, dan juga berbahaya bagi korban karena dengan video tersebut dapat mencemarkan nama baik korban. Hal ini sangat berpotensi untuk menghancurkan reputasi mereka.

#### 5. *Identity swap*

Kategori ini merupakan bentuk manipulasi yang mengganti wajah seseorang dalam video dengan wajah orang lain. Ini adalah kategori *deepfake* yang paling populer, di mana wajah satu orang ditukar atau ditimpa pada wajah orang lain dalam sebuah video atau gambar.

Teknologi ini mempertahankan struktur dan gerakan wajah asli, tetapi identitasnya diganti. Contoh penyalahgunaan kategori ini yaitu dalam pembuatan konten sindiran, seperti meme atau lelucon yang dapat menyinggung perasaan orang lain.

Lima kategori *deepfake* tersebut merupakan jenis *deepfake* yang paling umum digunakan oleh masyarakat. Semua lima kategori tersebut dapat melanggar ketentuan dalam pasal 35 UU ITE, hal itu dikarenakan dalam lima kategori tersebut unsur pemalsuan dokumen elektroniknya semua terpenuhi. Dari lima kategori tersebut terdapat beberapa kategori yang dapat melanggar Pasal 27A, 27B, dan 28 UU ITE, yakni kategori *entire face synthesis*, *lip-sync*, *identity swap*, *face re-enactment*. Dapat dikatakan melanggar hal ini dikarenakan terdapat unsur penyerangan kehormatan, dan penyebaran hoaks sudah terpenuhi.

Lima kategori pemalsuan identitas digital diatas juga dapat melanggar Pasal 263 dan 378 KUHP apabila unsur pemalsuan dan penipuan terpenuhi. Serta dapat melanggar peraturan dalam UU PDP dalam Pasal 65 sampai 68, karena unsur penyalahgunaan data pribadi juga terpenuhi. Dalam teknologi *deepfake* dilihat oleh sebagian kalangan sebagai kesempatan melakukan tindak pidana. Menimbulkan berbagai tindak pidana digital contohnya pemalsuan identitas, penyebaran informasi palsu, terorisme, penipuan, pencemaran nama baik, dan lain sebagainya.<sup>86</sup>

Berbagai bentuk tindak pidana digital tersebut menghasilkan masing-masing konsekuensi hukum dan sosial, antara lain yaitu:<sup>87</sup>

a. **Pemalsuan Identitas Digital atau *Digital Identity Fraud***

Hal ini terjadi ketika wajah, suara, atau atribut lain dipakai tanpa izin untuk menipu pihak ketiga, misalnya membuka rekening, melakukan transfer, atau mengautentikasi transaksi daring, sehingga tindakan tersebut memenuhi unsur penipuan dan pemalsuan data elektronik, tindakan tersebut termasuk dalam ketentuan tentang manipulasi informasi elektronik dan/atau pemrosesan data pribadi yang melawan hukum.

b. **Pencemaran nama baik dan fitnah digital**

Hal ini timbul ketika teknologi *deepfake* merepresentasikan seseorang melakukan atau mengucapkan hal yang merendahkan martabatnya. Penyebaran

---

<sup>86</sup> Banke, R., & Gandrova, S., 2023, Penerapan positif Indonesia terhadap kasus kejahatan dunia maya *deepfake*, *Madani: Jurnal Ilmiah Multidisiplin*, Vol. 3, No. 4, hlm. 651–660.

<sup>87</sup> Diyanggi Priya, R.P., & Alexandro Wiranto T., 2025, Tantangan Penegakan Hukum dan Upaya Mitigasi atas Hadirnya Deepfake Porn sebagai Jenis Tindak Pidana Digital pada Era *Artificial Intelligence*, *Jurnal Pemuliaan Keadilan*, Vol. 2, No. 3, hlm. 187

rekaman yang direkayasa seperti itu dapat dipidana berdasarkan norma anti pencemaran nama baik serta peraturan media elektronik karena menimbulkan kerugian moral dan sosial bagi korban serta mengganggu ketertiban umum.

**c. Pembuatan konten kesusilaan tanpa izin atau *non-consensual pornography***

Bentuk penyalahgunaan AI ekstrem di mana wajah korban disisipkan ke dalam materi pornografis. tindakan ini tidak hanya melanggar kepastian hukum terkait pornografi, melainkan juga hak privasi dan integritas tubuh digital korban serta akibat dari penyalahgunaan tersebut seringkali menimbulkan dampak psikologis dan stigma jangka panjang yang memerlukan perlindungan hukum dan psikologi khusus. Tindakan penyalahgunaan ini dapat berakibat sanksi pidana bagi pelaku dan pendampingan psikologi untuk pemulihan korban.

**d. Manipulasi informasi publik atau *digital mis-information***

Tindakan ini mengacu pada produksi dan penyebaran identitas palsu yang menggambarkan tokoh publik yang sedang membuat pernyataan palsu atau bertindak tidak semestinya. Selain mengganggu ketertiban umum di ruang digital fenomena ini juga memiliki implikasi politik dan keamanan karena dapat menimbulkan disinformasi dalam skala yang luas, mengganggu proses demokrasi, dan memicu keresahan sosial. Oleh karena itu upaya penanggulangan tindakan ini memerlukan kombinasi hukum pidana untuk tindakan kriminal seperti penghasutan atau penipuan, regulasi platform, dan mekanisme *fact-checking*.

Teknologi AI saat ini memang mempunyai sisi positif dan negatif. Namun akhir-akhir ini penggunaan diranah negatif lebih banyak dilakukan. Hal itu dibuktikan dengan adanya berbagai kasus pemalsuan identitas digital yang terjadi dimasyarakat. Hal tersebut dapat dilihat dari pengguna platform digital di Indonesia mengalami peningkatan, mencapai 221.563.479 orang dari total penduduk sebanyak 278.696.200 pada tahun 2023.<sup>88</sup>

Kondisi ini memperluas potensi dalam penyebaran tindak pidana *deepfake* di Indonesia. Pertumbuhan total pengguna platform *online* tersebut didukung teknologi yang memungkinkan pelaksanaan berbagai pekerjaan yang sebelumnya terkendala agar lebih cepat terselesaikan, misalnya dalam mengefisiensi waktu, menghadapi tuntutan global dan menghadapi tantangan saat dan setelah pandemi COVID-19, mengatasi kompleksitas kondisi geografis, serta berbagai hambatan lainnya.<sup>89</sup>

Hal-hal tersebut mengakibatkan, pertumbuhan teknologi di Indonesia mengarah pada revolusi digital. Hampir setiap pemakai sosial media setiap hari terhubung dengan internet. Total pengguna internet yang cukup masif ini pada kenyataannya sangat berpengaruh pada peningkatan tindak kejahatan *deepfake* di Indonesia.<sup>90</sup>

---

<sup>88</sup> Diyanggi Priya, R.P., & Alexandro Wiranto T., 2025, Tantangan Penegakan Hukum dan Upaya Mitigasi atas Hadirnya Deepfake Porn sebagai Jenis Tindak Pidana Digital pada Era *Artificial Intelligence*, *Jurnal Pemuliaan Keadilan*, Vol. 2, No. 3, hlm. 187

<sup>89</sup> Sawitri, D., & Wacika, M., 2023. Peran teknologi dalam transformasi ketenagakerjaan: Analisis dampak dan tantangan di era digital. *Jurnal Kertha Wicara*, Vol. 12, No. 2 hlm. 88–101.

<sup>90</sup> Diyanggi Priya, R.P., & Alexandro Wiranto T., 2025, Tantangan Penegakan Hukum dan Upaya Mitigasi atas Hadirnya Deepfake Porn sebagai Jenis Tindak Pidana Digital pada Era *Artificial Intelligence*, *Jurnal Pemuliaan Keadilan*, Vol. 2, No. 3, hlm. 187

Contoh kasus nyata tentang tindak pidana *deepfake* ini dialami oleh mantan Presiden Indonesia yaitu Joko Widodo. Muncul sebuah video pada Oktober 2023, yang memperlihatkan Presiden Joko Widodo berbicara dalam acara kenegaraan memakai bahasa mandarin fasih. Kemudian video tersebut menyebar semakin luas dan mengganggu ketertiban umum di ruang digital, bahkan banyak yang mempercayai video tersebut merupakan video asli.

Hal tersebut juga mengakibatkan jatuhnya citra presiden Jokowi di masyarakat. Sehingga, untuk mencegah kerusuhan publik di ruang digital yang semakin luas, maka Kementerian Komunikasi dan Digital atau Kemkomdigi kemudian mengeluarkan pernyataan resmi yang menyatakan video tersebut tiruan yang dihasilkan oleh teknologi *deepfake*.

Selain kasus tersebut terdapat kasus lain yang menggemparkan publik, yaitu kasus tentang pemalsuan identitas digital yang menimpa para selebriti, yaitu kasus yang dialami oleh Melaney Ricardo.

Dalam kasus video *deepfake* yang beredar pada 24 Januari 2024, Melaney Ricardo tampak sedang mengiklankan sebuah produk kecantikan. Akibat dari video tersebut, sejumlah yang menontonnya mempercayai keaslian promosi itu dan kemudian membeli produk yang dimaksud. Menanggapi hal ini, Melaney Ricardo memberikan klarifikasi serta mengungkapkan kerugian yang dialaminya akibat penyebaran video *deepfake* tersebut.

Selain kasus yang dialami Melaney Ricardo itu juga terdapat video *deepfake* mengenai Raffi Ahmad dan Najwa Shihab yang mengiklankan situs judi online serta situs pinjaman online. Melihat video *deepfake* ini telah



menimbulkan berbagai macam respon publik, para artis dan masyarakat memberikan dukungan bahwa video Raffi Ahmad dan Najwa Shihab tersebut merupakan hasil dari buatan AI.

Hasil wawancara CNN dengan Wakil Menteri Komunikasi dan Informatika mengungkapkan bahwa pada tahun 2023 terdapat sebanyak 95.820 kasus konten deepfake yang tersebar di seluruh dunia berdasarkan data Home Security. Angka tersebut menunjukkan peningkatan hingga 550 persen dibandingkan tahun 2019 secara global. Kondisi ini menimbulkan kekhawatiran karena teknologi tersebut berpotensi disalahgunakan untuk tindakan penipuan, pornografi, serta berbagai kejahatan lain yang dapat memicu penyebaran disinformasi. Situasi ini juga diperparah dengan posisi Indonesia yang menempati peringkat kedelapan sebagai negara dengan pengguna teknologi AI terbanyak di dunia.<sup>91</sup>

Penyalahgunaan teknologi AI ini yang sering kali menimbulkan penyimpangan hukum, terutama ketika digunakan untuk menipu, mencemarkan nama baik, atau menciptakan representasi palsu dari seseorang tanpa persetujuan. Bahkan riset ilmiah oleh tim dari *University College London* pada tahun 2020 berpendapat bahwa teknologi *deepfake* akan menjadi salah satu ancaman keamanan siber paling serius dan berbahaya yang bersumber dari teknologi AI.<sup>92</sup>

---

<sup>91</sup> Bramcov Stivens Situmeang, et al., 2024, Pengaruh *Artificial Intelligence* Terhadap Tingkat Kasus *Deepfake* Pada Selebritas di Twitter, *Jurnal Device*, Vol.14, No. 1, hlm, 83.

<sup>92</sup> Sekaring Ayu K., & Dina Wanda S.P., 2025, Perlindungan Hak Privasi Dalam Penyalahgunaan Teknologi Deepfake di Indonesia, *Jurnal RechtsVinding: Media Pembinaan Hukum Nasional*, Vol. 14, No. 2, hlm. 202

Para ahli dalam laporan tersebut bahkan memprediksi dalam kurun waktu 15 tahun mendatang, tindakan manipulasi konten dan identitas digital melalui teknologi *deepfake* berpotensi menjadi bentuk tindak kejahatan berbasis teknologi AI yang paling membahayakan dan mengkhawatirkan mengingat cara kerjanya yang mampu dalam menghasilkan video palsu yang sangat sulit dibedakan dari bentuk aslinya.

Untuk mencegah dan mengatasi lebih banyak terjadinya tindak pidana pemalsuan identitas digital ini maka diperlukannya regulasi yang spesifik mengenai AI. Meskipun dalam hukum positif Indonesia, tindak pidana *deepfake* ini dapat dikualifikasikan ke dalam beberapa ketentuan hukum yang telah ada. Misalnya berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau biasa disebut dengan UU ITE sebagaimana telah diubah dengan Undang-Undang No. 19 Tahun 2016.

Kitab Undang-Undang Hukum Pidana atau KUHP, juga dapat digunakan dalam menjerat tindak pidana *deepfake*. Tindakan *deepfake* dapat dianalogikan sebagai bentuk pemalsuan surat atau dokumen elektronik, sebagaimana diatur dalam Pasal 263 ayat (1) KUHP. Untuk KUHP baru atau Undang-Undang No. 1 Tahun 2023 tentang KUHP Nasional telah memperluas definisi “surat” menjadi mencakup dokumen elektronik, sehingga bentuk-bentuk manipulasi digital seperti *deepfake* dapat dikategorikan sebagai pemalsuan dokumen elektronik dengan dasar hukum yang lebih eksplisit.

Tindak Pidana ini juga dapat dijerat menggunakan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi atau UU PDP. Tindak

kejahatan *deepfake* ini dapat dilihat dari sudut pandang perlindungan data pribadi. Hal ini dikarenakan *deepfake* merupakan pelanggaran terhadap hak privasi digital. Berdasarkan Pasal 65 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, setiap orang dilarang memperoleh atau mengumpulkan data pribadi orang lain secara melawan hukum dan dengan tujuan yang dapat merugikan subjek data.

Data biometrik wajah, suara, dan ekspresi yang digunakan dalam proses pembuatan *deepfake* termasuk kategori data pribadi yang sensitif, sebagaimana ditegaskan dalam Pasal 4 ayat (2) UU PDP. Oleh karena itu, penggunaan data tersebut tanpa persetujuan yang sah untuk tujuan manipulatif dapat dianggap sebagai tindak pidana yang mengganggu privasi dan penyalahgunaan data pribadi.

Terdapat peraturan yang bisa dikenakan dalam menjerat pelaku tindak kejahatan pemalsuan identitas digital, namun dalam pelaksanaannya hukum positif Indonesia masih menghadapi berbagai tantangan dalam penegakan hukum terhadap kejahatan *deepfake* ini, antara lain yaitu:

- 1) Ketiadaan pengaturan khusus yang secara eksplisit mengatur tindak pidana *deepfake* atau penyalahgunaan AI.
- 2) Kendala pembuktian digital, karena hasil manipulasi *deepfake* sangat realistis dan sulit dibedakan dari konten asli tanpa keahlian forensik digital.
- 3) Aspek yurisdiksi lintas negara, karena pelaku sering beroperasi dari luar negeri menggunakan platform global.

- 4) Aspek pertanggungjawaban, yakni menentukan siapa yang bertanggung jawab, pembuat, pengguna, atau penyebar konten *deepfake*.

Dari beberapa tantangan tersebut, maka diperlukan reformasi regulasi hukum dalam ruang siber yang adaptif dan responsif dalam perkembangan teknologi AI. Pemerintah perlu mempertimbangkan dan menyeragakan pembentukan peraturan khusus mengenai kejahatan pemalsuan identitas digital berbasis AI. Peraturan tersebut mencakup dan memperjelas batasan tanggung jawab pidana, prosedur pembuktian digital, dan perlindungan terhadap korban tindak pidana *deepfake*. Penguatan kapasitas dan keahlian aparat penegak hukum dalam bidang forensik digital dan *cyber law* juga menjadi suatu hal yang penting agar penegakan hukum dapat berjalan efektif dan adil.

Sistem hukum harus dapat memberikan kepastian hukum sekaligus perlindungan terhadap hak individu. Pendekatan interdisipliner antara hukum, etika, dan teknologi untuk memastikan bahwa pemanfaatan AI tidak hanya efisien secara teknis, tetapi juga adil, bertanggung jawab, dan selaras prinsip-prinsip kemanusiaan.

Regulasi mengenai AI mulai dibahas dan dirancang di negara lain, contohnya yaitu di Uni Eropa dan Amerika. Uni Eropa dan Amerika Serikat menjadi dua yurisdiksi yang menonjol dalam pengembangan kerangka hukum mengenai AI, meskipun keduanya mengadopsi pendekatan yang berbeda secara filosofis maupun normatif. Uni Eropa menempatkan aspek perlindungan individu, etika, dan kepastian hukum sebagai prioritas utama melalui regulasi yang ketat dan preventif. Sementara itu, Amerika Serikat berfokus pada inovasi,

efisiensi ekonomi, dan kebebasan industri, dengan pendekatan aturan yang lebih adaptif dan berbasis pada bidang yang menerapkan. Meskipun berbeda, kedua yurisdiksi tersebut memiliki tujuan yang sama, yaitu memastikan pengembangan AI yang aman, transparan, dan bertanggung jawab.

Dalam konteks global, model yang diadopsi Uni Eropa dianggap memberikan pandangan bagi negara-negara lain yang ingin mengatur AI secara menyeluruh dan berpedoman pada hak asasi manusia. Sedangkan model Amerika Serikat dinilai lebih fleksibel dan inovatif, akan tetapi terdapat risiko yang menciptakan ketimpangan dalam perlindungan hukum antar bidang.

Indonesia sedang merumuskan arah regulasi hukum terkait AI, sehingga kedua pendekatan tersebut dapat dijadikan pedoman komparatif, pendekatan normatif-protektif ala Uni Eropa dan pendekatan pragmatis-inovatif ala Amerika Serikat. Kolaborasi keduanya dapat menghasilkan kerangka hukum AI yang seimbang antara perlindungan kepentingan publik dan dukungan terhadap pengembangan teknologi.

#### **B. Bentuk Pertanggungjawaban Pidana Terhadap Pelaku yang Menggunakan Teknologi Artificial Intelligence Untuk Melakukan Pemalsuan Identitas Digital *Deepfake* Menurut Hukum Positif di Indonesia?**

Di era modern saat ini, AI telah menjadi bagian yang erat dengan kehidupan manusia. Saat ini, kemampuan AI sudah jauh melampaui kemampuan alat-alat lain. AI sering kali mampu melampaui manusia dalam menjawab pertanyaan atau menyelesaikan masalah. Perkembangan ini

menunjukkan bahwa seiring berjalannya waktu, AI mungkin memiliki kemampuan otonom untuk membuat keputusan atau bertindak sendiri tanpa campur tangan manusia. Akibatnya, muncul kekhawatiran baru terkait potensi pelanggaran hukum yang bisa terjadi akibat tindakan AI secara otonom tersebut.

Perkembangan teknologi AI yang cukup cepat, tidak hanya membawa kemajuan dalam berbagai bidang kehidupan manusia, akan tetapi juga menimbulkan persoalan etis dan yuridis yang kompleks. AI, sebagai suatu sistem yang mampu melakukan proses berpikir, belajar, dan mengambil keputusan secara otonom dan seperti manusia, telah mengaburkan batas antara tindakan yang dilakukan manusia dan tindakan yang diproses oleh mesin.

Kondisi tersebut menimbulkan dilema moral dan hukum, khususnya ketika suatu teknologi tersebut digunakan untuk tujuan yang menyimpang dan melanggar dari norma sosial maupun hukum positif yang berlaku, seperti penyebaran disinformasi, pelanggaran privasi, atau pemalsuan identitas digital atau *deepfake*.

Secara etis, keberadaan AI menimbulkan pertanyaan mendasar mengenai tanggung jawab moral dalam penggunaan teknologi. Salah satu permasalahan utama adalah potensi *dehumanisasi* dalam pengambilan keputusan yang dilakukan oleh mesin. Ketika AI digunakan dalam konteks yang menyangkut kepentingan manusia, misalnya dalam bidang peradilan, rekrutmen kerja, atau layanan publik maka keputusan algoritmik dapat menimbulkan bias dan diskriminasi apabila sistem tersebut tidak dirancang dengan prinsip keadilan dan transparansi.



AI dalam melakukan pengolahan, pengumpulan, serta menyebarkan data pribadi tanpa persetujuan juga menimbulkan persoalan etika terkait pelanggaran hak privasi individu. Dalam hal ini, prinsip-prinsip etika seperti *beneficence* atau kemanfaatan, *non-maleficence* atau tidak merugikan, *justice* atau keadilan, dan *autonomy* atau kemandirian menjadi landasan yang sangat penting dalam merumuskan sistem AI yang berkeadilan dan bertanggungjawab.

Ketika AI melakukan pelanggaran hukum maka hal yang akan dipermasalahkan adalah mengenai siapa yang akan bertanggungjawab secara hukum atas tindakan yang telah dilakukannya. Permasalahan pertanggungjawaban pidana menjadi perhatian penting bagi setiap negara saat merancang regulasi mengenai AI. Hal itu disebabkan karena AI memiliki kemampuan untuk beroperasi secara mandiri dengan tingkat otonomi tertentu. Kemampuan inilah yang memungkinkan AI melakukan tindak pidana yang merugikan manusia.

Dalam menetapkan pertanggungjawaban pidana AI, perlu dilakukan identifikasi terhadap status hukum AI sesuai dengan kerangka regulasi yang berlaku sesuai aturan di Indonesia saat ini. Dalam mengidentifikasi mengenai pertanggungjawaban maka hal pertama yang akan dicari adalah siapa subjek hukum yang melakukan tindak pidana tersebut.

Subjek hukum yaitu penyokong utama hak dan kewajiban dari hukum.<sup>93</sup>

Hal ini berarti siapa yang dapat melakukan tindak pidana dan akan dijatuhi

---

<sup>93</sup> Kurniawan Tri Wibowo., 2025, *Aspek Hukum Dalam Dunia Digital*, PT Sada Kurnia Pustaka, Banten, hlm. 126

pidana jika perbuatan yang dilakukan terbukti bersalah di pengadilan. Menurut CST Kansil, subjek hukum merupakan pihak yang memiliki kemampuan untuk memiliki hak serta kecakapan dalam melakukan tindakan hukum, atau dengan kata lain, pihak yang diakui secara hukum memiliki hak dan kewenangan untuk bertindak.

Dalam peraturan hukum di Indonesia, perbuatan yang dilakukan oleh subjek hukum hanya dapat dikerjakan oleh manusia dan korporasi. Sehingga, manusia dan korporasi oleh hukum diakui sebagai pemilik hak dan kewajiban. Subyek hukum pidana ialah unsur yang penting, hal ini dikarenakan subyek hukum akan menjadi faktor utama dalam mengidentifikasi pertanggungjawaban pidana yang kemudian akan menentukan mengenai penjatuhan pidana.

AI memiliki kemampuan untuk menganalisis dan menalar data besar secara rasional untuk tujuan mengambil keputusan secara mandiri guna mencapai tujuan tertentu. Selain itu, kecerdasan yang dimiliki AI memungkinkannya untuk memberikan jawaban atas pertanyaan, melaksanakan perintah, serta melakukan berbagai tindakan yang menyerupai perilaku manusia. Walaupun AI mampu membangun pola pikir yang menyerupai kemampuan kognitif manusia, hal tersebut tidak dapat dijadikan dasar untuk menganggap bahwa AI adalah manusia.

AI tidak dapat dikategorikan sebagai sesuatu yang mirip dengan manusia *naturlijk persoon* sebagaimana dimaksud dalam hukum pidana. AI juga bukan merupakan badan hukum, sehingga secara yuridis AI tidak termasuk dalam subjek hukum pidana.

Tindak pidana yang dilakukan oleh subjek hukum pidana adalah suatu tindakan tertentu yang diancam dengan sanksi pidana oleh undang-undang sesuai dengan asas legalitas. Oleh karena itu, unsur utama dari tindak pidana adalah adanya tindakan yang dilakukan oleh manusia atau badan hukum. Setiap perbuatan yang tidak berasal dari manusia dan badan hukum tidak dapat dikategorikan sebagai tindak pidana yang dapat dikenai hukuman.<sup>94</sup> Sebagai contoh, tindakan seekor harimau yang menggigit seseorang hingga menimbulkan luka berat atau kematian tidak termasuk dalam ranah tindak pidana, karena bukan merupakan perbuatan manusia.

Pertanggungjawaban pidana pada hakikatnya adalah proses pemberian sanksi kepada pelaku karena tindakannya yang melanggar hukum atau menghasilkan kondisi yang dilarang. Dengan begitu, pertanggungjawaban pidana mencerminkan pengalihan hukuman dari perbuatan yang bersifat objektif kepada pelakunya secara subjektif.

Dalam konsep hukum pidana yang dianut Indonesia, seseorang dianggap dapat dipertanggungjawabkan secara pidana apabila hukuman yang melekat pada tindak pidana secara sah dialihkan kepadanya. Pertanggungjawaban pidana ditentukan oleh adanya kesalahan pada diri pelaku, bukan karena terpenuhinya unsur-unsur tindak pidana.

Kesalahan memiliki kedudukan sentral dalam memutuskan dapat tidaknya seseorang dipertanggungjawabkan secara pidana, dan tidak hanya dianggap sebagai unsur batiniah dari tindak pidana semata. Sehingga,

---

<sup>94</sup> Ibid, hlm. 127

penentuan adanya kesalahan pada seseorang merupakan bagian paling penting dari konsep pertanggungjawaban pidana.

Penjatuhan pidana dalam hukum pidana materiil memberikan syarat adanya perbuatan pidana dan pertanggungjawaban pidana.<sup>95</sup> Teori pembedaan harus terpenuhi unsur subyektif dan objektif. Pembedaan dapat dilakukan baik terhadap perbuatan dan terhadap orangnya. Pembedaan pelaku tindak pidana tidak hanya berdasarkan pelaku yang telah melakukan tindakan yang dilarang oleh peraturan, akan tetapi harus juga memenuhi syarat pelaku yang mempunyai kesalahan.<sup>96</sup>

Saat ini terdapat banyak pertanyaan apakah AI harus mempunyai *mens rea* agar dapat dikenai pertanggungjawaban pidana. Pertanyaan tersebut secara logis dapat dijawab dengan tegas, bahwa AI tidak mempunyai perasaan, karena pada hakikatnya AI saat ini masih sebatas mesin yang tidak memiliki akal dan batin atau perasaan.

Kecerdasan buatan yang ada sekarang belum mampu bertindak berdasarkan kehendaknya sendiri, melainkan tetap bergantung pada instruksi dari penggunanya. Meskipun demikian, perkembangan teknologi menunjukkan kemajuan yang signifikan, salah satu contohnya adalah pernyataan seorang insinyur Google bernama Blake Lemoine, yang mengungkapkan bahwa sistem kecerdasan buatan yang ia kembangkan bersama timnya diduga telah menunjukkan tanda-tanda memiliki perasaan.

---

<sup>95</sup> Ibid, hlm. 128

<sup>96</sup> Kurniawan Tri Wibowo dan Riski Ardiansyah, 2024, *Hukum Pidana Nasional*, Papas Sinar Sinanti, Depok, hlm. 147

Ketika AI mempunyai perasaan maka sudah tentu AI mempunyai niat dan tujuan, maka AI akan berubah seperti manusia. Hal tersebut tentunya memberikan peringatan dan perlu diwaspadai sehingga hukum tidak selalu kalah dengan perkembangan teknologi, tertinggal di belakang dan memberikan kebingungan bagi para penegak hukum juga bagi masyarakat.

Berbagai pandangan telah muncul mengenai kedudukan AI sebagai subjek hukum, di antaranya:

Pertama, terdapat pendapat yang menyatakan AI dapat diakui subjek hukum yang memiliki hak, kewajiban, serta kesadaran. Pandangan ini berasumsi bahwa AI merupakan entitas elektronik baik berupa mesin, komputer, robot, maupun program yang memiliki kecerdasan menyerupai manusia, serta mampu bertindak secara sadar tanpa bergantung sepenuhnya pada algoritma yang diciptakan oleh manusia.

Kedua, ada pula pandangan yang menyamakan status hukum AI dengan hewan. Dalam perspektif ini, AI dianggap memiliki tingkat kesadaran dan emosi tertentu, serta kemampuan untuk bergerak secara mandiri atau *autonomous*. Namun demikian, sebagaimana hewan, AI tidak dapat dijadikan subjek hukum. Apabila AI melakukan tindakan yang merugikan pihak lain, tanggung jawab hukum tetap dibebankan kepada pemiliknya sebagai pihak yang berstatus subjek hukum.

Ketiga, sebagian ahli hukum di Amerika Serikat menempatkan AI dalam posisi hukum yang serupa dengan pegawai di sebuah perusahaan. Dengan status ini, AI dapat dianggap sebagai entitas hukum yang dapat dimintai kompensasi

atas kerugian atau bahaya yang ditimbulkannya. Meskipun begitu, tanggung jawab hukum secara penuh tetap berada pada pengguna, pemilik, ataupun perancang teknologi AI sebagai pihak yang mengendalikannya.

Pertanggungjawaban pidana menuntut pemenuhan unsur-unsur delik seperti *actus reus* atau perbuatan, *mens rea* atau adanya kesalahan, *toerekeningsvatbaarheid* atau kemampuan bertanggung jawab dan ketiadaan alasan pemaaf.

Fenomena *deepfake* dengan memanipulasi audio ataupun visual menggunakan teknik *deep learning* mengaburkan batas antara tindakan manusia dan keluaran sistem otomatis sehingga menimbulkan tantangan dalam atribusi kesalahan dan pembuktian. Dalam hukum positif Indonesia, meskipun belum ada norma khusus yang menyebut *deepfake*, terdapat sejumlah ketentuan substantif dan institusional seperti yang diatur dalam KUHP lama maupun KUHP baru yaitu Undang-Undang No. 1 Tahun 2023, UU ITE, UU PDP, Peraturan Administrasi dan Regulasi Penyelenggara Sistem Elektronik yang menjadi dasar penjatuhan pertanggungjawaban pidana terhadap pelaku *deepfake*. Analisis masing-masing dari peraturan-peraturan tersebut akan dijelaskan berikut ini:

Dalam hukum positif Indonesia, peraturan mengenai tindak pidana pemalsuan dan penipuan yang diatur dalam KUHP memiliki relevansi terhadap fenomena tindak pidana *deepfake* sebagai bentuk pemalsuan identitas digital. Dalam Pasal 263 KUHP mengatur mengenai tindak pidana pemalsuan surat, yaitu perbuatan membuat atau menggunakan surat palsu atau dipalsukan dengan



maksud untuk menimbulkan hak, kewajiban, atau pembebasan dari suatu perikatan, atau untuk digunakan sebagai alat bukti yang dapat menimbulkan kerugian bagi pihak lain.

Tindak pidana *deepfake*, hasil manipulasi berupa video, gambar, atau rekaman suara yang menampilkan seseorang melakukan tindakan atau mengucapkan sesuatu yang sebenarnya tidak terjadi dapat disamakan secara analogi dengan pemalsuan dokumen atau identitas karena mengandung unsur merekayasa fakta untuk menipu atau menyesatkan pihak lain.

Di dalam Pasal 378 KUHP yang mengatur tentang penipuan juga dapat diterapkan, karena perbuatan tersebut melibatkan penggunaan tipu muslihat untuk memperoleh keuntungan atau merugikan orang lain. Unsur tersebut merupakan unsur yang sering melekat pada penyebaran tindak pidana *deepfake*, khususnya dalam kasus penipuan daring, pemerasan digital, atau pencemaran nama baik.

Didalam KUHP baru yang tertuang dalam Undang-Undang Nomor 1 Tahun 2023 membawa pembaruan penting dengan memperluas pengertian surat, makna awalnya surat hanya dalam bentuk konvensional atau fisik, sekarang lebih luas mencakup dokumen elektronik. Perluasan ini memiliki implikasi signifikan terhadap penegakan hukum terhadap tindak pidana berbasis teknologi, termasuk dalam tindak pidana *deepfake*, karena memperjelas dasar legal bagi aparat penegak hukum untuk menjerat pelaku yang memalsukan atau memanipulasi data elektronik yang berfungsi sebagai sarana komunikasi, identifikasi, atau pembuktian hukum.

Perbuatan menciptakan atau menyebarkan identitas digital dengan meniru wajah, suara, atau perilaku seseorang untuk menyesatkan publik atau memperoleh keuntungan tertentu dapat dikategorikan sebagai bentuk pemalsuan dokumen elektronik sebagaimana dimaksud dalam Pasal 391 KUHP baru.

Didalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana juga menunjukkan sifat progresif dan antisipatif terhadap perkembangan teknologi, khususnya dalam mengatur perbuatan pidana yang dilakukan melalui perantara alat. Dalam Penjelasan Pasal 20 huruf b, yang dimaksud perantara alat mencakup penggunaan sarana seperti *remote control* yang memungkinkan seseorang melakukan tindak pidana secara tidak langsung.

Konsep *remote control* tersebut dapat diperluas maknanya dan dianalogikan dengan agen elektronik, yaitu sistem digital yang mampu menjalankan fungsi tertentu tanpa keterlibatan langsung manusia. Oleh karena itu, meskipun AI memiliki kemampuan mengambil keputusan secara otonom tanpa campur tangan manusia, akan tetapi individu yang menggunakan AI sebagai sarana untuk melakukan tindakan yang menimbulkan akibat pidana tetap dapat dipertanggungjawabkan sebagai pelaku tindak pidana.

Pihak yang menciptakan atau merancang AI juga tidak sepenuhnya terbebas dari tanggung jawab hukum. Apabila tindakan atau kelalaian dalam perancangan sistem AI menyebabkan AI tersebut melakukan perbuatan yang melanggar hukum, maka pembuatnya dapat dianggap lalai atau *culpa*. Dengan

begitu, meskipun pembuat AI tidak memiliki niat atau kesengajaan untuk melakukan tindak pidana, kelalaiannya yang mengakibatkan timbulnya perbuatan pidana oleh AI dapat menimbulkan konsekuensi hukum.

Ketentuan ini memperkuat korelasi antara regulasi tradisional tentang pemalsuan dan perkembangan kejahatan digital modern, serta menegaskan bahwa hukum pidana Indonesia telah beradaptasi terhadap tantangan baru yang dihadirkan oleh kecerdasan buatan dan manipulasi digital dalam ruang digital.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 atau kerap disebut juga dengan UU ITE merupakan salah satu alat hukum utama yang mengatur perilaku masyarakat dalam ruang digital, termasuk perbuatan manipulasi data melalui teknologi AI seperti yang terjadi dalam tindak pidana *deepfake*.

Dalam konsep hukum pidana Indonesia AI dapat disamakan dengan agen elektronik, hal ini dikarenakan AI memiliki sifat dalam otomatisasi pemrosesan informasi.<sup>97</sup> Menurut Pasal 1 UU ITE, yang dimaksud dengan agen elektronik adalah suatu perangkat yang merupakan bagian dari sistem elektronik, untuk melaksanakan perbuatan tertentu mengenai informasi elektronik secara otonom dan dioperasikan oleh manusia. Sehingga, agen elektronik tidak berdiri sendiri, melainkan menjadi komponen integral dalam sistem elektronik secara keseluruhan.

---

<sup>97</sup> Maria Karunia P.M., Heryanto A. et al., 2025, Analisis Perlindungan Hukum terhadap Penyimpangan *Artificial Intelligence* dalam Tindak Pidana Deepfake Pornografi Berdasarkan Hukum Pidana, JURRISH: Jurnal Riset Rumpun Ilmu Sosial, Politik, dan Humaniora, Vol. 4, No. 1, hlm. 298

Setiap pihak yang menyelenggarakan sistem elektronik, termasuk agen elektronik di dalamnya, memiliki kewajiban hukum untuk menjamin bahwa sistem yang digunakan berfungsi dengan aman, andal, dan dapat dipertanggungjawabkan. Tanggung jawab tersebut meliputi seluruh dampak atau akibat hukum yang mungkin timbul dari penggunaan sistem dimaksud. Sebagaimana ditegaskan dalam Pasal 21 UU ITE, penyelenggara agen elektronik bertanggung jawab sepenuhnya atas semua akibat hukum yang muncul akibat penciptaan atau pemanfaatan sistem tersebut.

Dalam konteks tindak pidana *deepfake* melalui teknologi AI ini, terdapat beberapa ketentuan dalam UU ITE yang memiliki relevansi langsung terhadap tindak kejahatan pemalsuan identitas digital. Dalam Pasal 27 ayat (3) mengatur larangan terhadap setiap perbuatan mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan pencemaran nama baik. Dalam kasus tindak pidana *deepfake*, ketika seseorang membuat atau menyebarkan konten yang menampilkan individu dengan ucapan atau tindakan yang bersifat merendahkan martabat, maka perbuatan tersebut dapat dikategorikan sebagai tindak pidana pencemaran nama baik berbasis media digital.

Dalam Pasal 28 ayat (1) UU ITE mengatur larangan penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian bagi konsumen atau masyarakat. Manipulasi konten digital berupa tindakan pemalsuan identitas digital yang digunakan untuk menyebarkan informasi palsu, misalnya menampilkan tokoh publik menyampaikan pernyataan palsu atau melakukan

tindakan tertentu yang tidak benar, dapat dikenakan pasal ini karena berpotensi menimbulkan keresahan sosial dan kerugian publik.

Terdapat Pasal 35 UU ITE yang menjadi pasal paling relevan dalam mengkategorikan perbuatan *deepfake* sebagai tindak pidana. Pasal ini menyebutkan setiap orang yang sengaja dan tanpa hak memanipulasi, membuat, mengubah, menghapus, merusak, atau menampilkan informasi elektronik atau dokumen elektronik seolah-olah otentik, dapat dikenai pidana.

Unsur manipulasi agar dianggap autentik secara langsung mencerminkan karakteristik utama dari tindak pidana *deepfake*, yakni kemampuan teknologi untuk menciptakan representasi palsu yang tampak benar secara visual dan audiotif. Dalam perspektif hukum pidana, tindakan tersebut memenuhi unsur kesengajaan karena pelaku secara sadar menggunakan teknologi untuk menciptakan ilusi kebenaran dengan tujuan menipu, mencemarkan nama baik, atau memperoleh keuntungan tertentu.

Unsur tanpa hak menegaskan bahwa perbuatan tersebut dilakukan tanpa persetujuan atau kewenangan yang sah dari pihak yang identitasnya digunakan. Sehingga, Pasal 35 UU ITE menjadi dasar hukum yang kuat untuk menjerat pelaku manipulasi digital melalui teknologi AI, baik dalam konteks penipuan, pencemaran nama baik, maupun penyebaran konten palsu yang menyesatkan publik. Ketentuan ini menunjukkan bahwa UU ITE berfungsi sebagai jembatan normatif yang memungkinkan penerapan asas-asas hukum pidana tradisional terhadap bentuk-bentuk kejahatan baru yang timbul akibat kemajuan teknologi informasi dan kecerdasan buatan.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi atau biasa disebut juga dengan UU PDP merupakan tonggak penting dalam sistem hukum Indonesia yang memayungi aspek yuridis terhadap hak privasi individu di era digital saat ini. Dalam UU PDP ini secara komprehensif mengatur mengenai pengumpulan, pemrosesan, penyimpanan, penyebaran, hingga penghapusan data pribadi yang dilakukan baik oleh individu maupun badan hukum.

Aspek penting yang diatur dalam UU PDP adalah mengenai data biometrik, yang mencakup data wajah, suara, sidik jari, retina mata, dan elemen biologis lainnya yang dapat digunakan untuk mengidentifikasi seseorang. Dalam konteks tindak pidana *deepfake*, teknologi ini sering kali menggunakan data biometrik seseorang tanpa izin, seperti menyalin wajah atau suara individu untuk menciptakan representasi digital yang menyerupai aslinya.

Data pribadi yang dimanfaatkan sebagai bahan dasar dalam penyalahgunaan teknologi AI dalam tindak pidana *deepfake* tergolong dalam data pribadi biometrik. Jenis data ini mencakup informasi yang berhubungan dengan aspek fisik, fisiologis, maupun perilaku seseorang yang mengidentifikasi individu secara unik, misalnya citra wajah atau data sidik jari.

Dalam konteks hak-hak subjek data pribadi sebagaimana diatur dalam Bab IV UU PDP, Pasal 12 menegaskan bahwa setiap subjek data pribadi, termasuk korban pelanggaran, memiliki hak mengajukan gugatan serta memperoleh ganti rugi apabila terjadi pelanggaran terhadap pemrosesan data pribadinya, sesuai dengan ketentuan peraturan perundang-undangan yang



berlaku. Sehingga perbuatan penyalahgunaan teknologi AI dalam tindak pidana *deepfake* yang memanfaatkan data biometrik seseorang tanpa izin dapat dikualifikasikan sebagai delik aduan, di mana proses penegakan hukumnya bergantung pada adanya pengaduan dari pihak yang dirugikan.

Tindakan seperti menyalin wajah atau suara individu untuk menciptakan bentuk palsu yang mirip dengan identitas aslinya termasuk dalam kategori pemrosesan data pribadi tanpa dasar hukum yang sah, sebagaimana diatur dalam Pasal 20 dan Pasal 21 UU PDP, bahwa setiap pemrosesan data pribadi harus didasarkan pada persetujuan spesifik pemilik data.

Dalam Pasal 65 hingga Pasal 68 UU PDP ketentuan sanksi pidana terhadap setiap orang yang sengaja dan melawan hukum memperoleh, mengumpulkan, mengungkapkan, atau menggunakan data pribadi tanpa hak. Pelanggaran terhadap ketentuan tersebut dapat dikenakan pidana penjara dan/atau denda, tergantung pada tingkat kesalahan dan dampak yang dihasilkan.

Dalam kaitannya dengan pemalsuan identitas digital melalui teknologi AI, penggunaan data biometrik seseorang tanpa izin untuk tujuan manipulatif atau menyesatkan dapat dikualifikasikan sebagai pelanggaran berat terhadap perlindungan data pribadi. UU PDP juga menegaskan tanggung jawab pengendali dan prosesor data dalam memastikan keamanan dan kerahasiaan data pribadi yang dikelolanya, termasuk penerapan prinsip-prinsip *lawfulness*, *transparency*, dan *accountability* dalam setiap kegiatan pengolahan data.

UU PDP memberikan landasan hukum yang tegas bagi penegakan hukum terhadap penyalahgunaan teknologi AI seperti tindak pidana *deepfake*

yang melibatkan data pribadi individu. Pengaturan ini memperkuat posisi hukum Indonesia dalam menghadapi tantangan kejahatan digital modern yang bersifat kompleks dan lintas batas, sekaligus menegaskan bahwa perlindungan data pribadi bukan hanya sekedar isu teknis, melainkan menjadi bagian integral dari perlindungan hak asasi manusia di ranah digital saat ini.

Terdapat pula Undang-Undang dan Peraturan Pemerintah lain yang mengatur mengenai perlindungan data elektronik. Seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang menjadi turunan dari UU ITE. Peraturan Pemerintah ini dibuat untuk menggantikan Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang dianggap sudah tidak relevan dan sesuai dengan dinamika dan kebutuhan hukum masyarakat saat ini. Serta terdapat pula berbagai Peraturan Menteri Komunikasi dan Informatika atau Permenkominfo seperti Permenkominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat, serta No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Permenkominfo yang mengatur tentang Penyelenggaraan Sistem Elektronik atau PSE, berfungsi sebagai instrumen hukum pelengkap dalam pengaturan aktivitas digital di Indonesia, termasuk yang berkaitan dengan penyalahgunaan teknologi AI dalam tindak pidana *deepfake*.

Regulasi ini menegaskan bahwa setiap pemakai sistem elektronik wajib menjaga integritas, keandalan, dan keamanan data elektronik yang ada di bawah pengelolaannya. Hal ini mencakup kewajiban untuk memastikan bahwa data

tidak mengalami modifikasi, kebocoran, atau manipulasi tanpa izin yang sah, terutama ketika melibatkan data pribadi atau konten yang bersifat sensitif.

PP No. 71 Tahun 2019 dan peraturan turunannya juga mengharuskan setiap penyelenggara sistem menyediakan mekanisme penghapusan atau pemblokiran terhadap konten elektronik yang melanggar hukum atau menimbulkan kerugian bagi pihak lain, termasuk konten yang dihasilkan melalui teknologi *AI*. Ketentuan ini menjadi penting untuk mencegah penyebaran informasi palsu, pelanggaran privasi, atau pencemaran nama baik yang timbul akibat manipulasi digital.

Peraturan tersebut tidak hanya menegaskan tanggung jawab hukum bagi penyelenggara sistem, akan tetapi juga memperkuat upaya negara dalam menciptakan ekosistem digital yang memberikan rasa aman, bertanggung jawab, dan beretika di tengah perkembangan pesat teknologi berbasis kecerdasan buatan saat ini.

Dari berbagai permasalahan mengenai siapa yang akan bertanggung jawab apabila suatu teknologi *AI* melakukan tindak pidana, maka dapat diidentifikasi dalam berbagai bentuk pertanggungjawaban pidana menurut subjeknya yang menafsirkan serta melakukan tindakan. Masing-masing dari subyeknya memerlukan analisis tersendiri:

- 1. Pertanggungjawaban pidana apabila dikenakan kepada Pelaku langsung atau individu pembuat dan penyebar *deepfake***

Perbuatan atau *actus reus*, yang dilakukan oleh pelaku langsung yaitu meliputi pembuatan, publikasi, atau distribusi konten manipulatif. Dalam UU ITE Pasal 35 perbuatan yang termasuk dalam pelanggaran meliputi memanipulasi atau menciptakan atau mengubah informasi elektronik. Sehingga keduanya unsur dan perbuatannya saling berkaitan dan terpenuhi sesuai dalam Pasal 35 UU ITE.

Adapun sanksi pidana bagi pelanggaran Pasal 35 diatur dalam Pasal 51 ayat (1) UU ITE, yaitu dikenai hukuman pidana berupa penjara dengan masa maksimal dua belas tahun dan/atau dikenakan denda paling tinggi sebesar Rp12.000.000.000,00. Sehingga, sanksi tersebut juga berlaku bagi pelaku yang terbukti melakukan manipulasi data elektronik, termasuk dalam konteks *deepfake* atau pemalsuan identitas digital. Sanksi ini menunjukkan bahwa negara menempatkan keaslian dan keautentikan informasi elektronik sebagai hal penting dalam melindungi kesatuan ruang digital dan kepercayaan publik terhadap sistem elektronik.

Kesalahan atau *mens rea*, yang dilakukan oleh pelaku individu unsur kesalahan nya dapat terpenuhi dalam Pasal 35 UU ITE yang mensyaratkan perbuatan “dengan sengaja dan tanpa hak/melawan hukum”. Apabila pembuat atau penyebar mengetahui sifat manipulatif konten dan bermaksud menghasilkan persepsi palsu atau merugikan pihak lain, maka unsur ini terpenuhi sehingga dapat dijerat dengan pasal 35 UU ITE. Kemudian, Jika terbukti adanya unsur penipuan finansial, pencemaran nama baik, atau unsur kesusilaan, pasal lain juga dapat diberlakukan.

Kemampuan bertanggung jawab pelaku individu juga penting untuk diperhatikan, dalam kasus tindak pidana *deepfake* umumnya terpenuhi karena pembuat atau penyebar bertindak dengan kesadaran penuh, tetapi terdapat pengecualian apabila terdapat gangguan jiwa atau unsur paksaan. Maka kemampuan bertanggungjawab itu akan dihilangkan atau dimaafkan sesuai dengan pasal 44 KUHP.

Kualifikasi delik dalam menjerat pelaku individu, apabila dilihat dari analisis maka pelaku langsung atau individu pembuat dan penyebar konten *deepfake* dapat dikenai pidana berupa pemalsuan data elektronik yang sesuai dengan Pasal 35 UU ITE, penipuan sesuai dengan Pasal 378 KUHP, yang sanksi bagi pelaku tindak pidananya diatur dalam Pasal 378 KUHP yakni pidana penjara maksimal empat tahun.

Dalam suatu perbuatan terdapat unsur untuk memperoleh keuntungan disertai dengan tindakan pencemaran nama baik, maka pelaku dapat dijerat menggunakan ketentuan Pasal 27 ayat (3) Undang-Undang ITE. Pelanggaran terhadap pasal tersebut dapat dikenai pidana penjara paling lama empat tahun dan/atau denda paling banyak Rp750 juta. Namun, perlu diketahui bahwa ketentuan Pasal 27 UU ITE telah mengalami perubahan melalui Pasal 27 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua UU ITE, di mana dalam versi terbaru tersebut tidak lagi mengatur mengenai penghinaan dan/atau pencemaran nama baik sebagaimana tercantum pada ketentuan sebelumnya.

Dalam Undang-Undang Nomor 1 Tahun 2024, antara Pasal 27 dan Pasal 28 telah ditambahkan dua pasal baru, yaitu Pasal 27A dan Pasal 27B. Berdasarkan ketentuan Pasal 27A, orang yang sengaja menyerang kehormatan atau nama baik orang lain agar diketahui oleh publik, baik melalui informasi elektronik maupun dokumen elektronik yang disebarluaskan melalui sistem elektronik, dapat dikenai pidana penjara paling lama dua tahun dan/atau denda paling banyak Rp400 juta. Lalu, menurut Pasal 27A UU 1 Tahun 2024 merupakan tindak pidana aduan yang hanya dapat dituntut atas pengaduan korban atau orang yang terkena tindak pidana dan bukan oleh badan hukum.

Berdasarkan penjelasan Pasal 27B ayat (2) Undang-Undang Nomor 1 Tahun 2024, yang dimaksud dengan “ancaman pencemaran” ialah tindakan mengancam untuk menyerang kehormatan atau nama baik, dengan tujuan agar tuduhan tersebut diketahui oleh khalayak umum.

Pelaku yang melanggar ketentuan sebagaimana tercantum dalam Pasal 27B ayat (2) Undang-Undang Nomor 1 Tahun 2024 dapat dikenai pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp1 miliar, sebagaimana diatur dalam Pasal 45 ayat (10) undang-undang yang sama. Meskipun demikian, perlu ditekankan bahwa tindak pidana sebagaimana dimaksud dalam Pasal 27B ayat (2) tersebut hanya dapat diproses berdasarkan pengaduan dari korban.

Dalam perbuatan tersebut juga terdapat unsur penyebaran berita bohong, maka pelaku dapat dijerat dengan ketentuan pidana sebagaimana



diatur dalam Pasal 28 UU ITE. Ketentuan sanksinya diatur dalam Pasal 45A UU Nomor 19 Tahun 2016 tentang perubahan atas UU ITE. Sanksi pidana dalam Pasal 28 UU ITE secara umum berupa pidana penjara maksimal enam tahun dan/atau denda maksimal satu miliar rupiah, tergantung pada jenis pelanggaran yang dilakukan.

## **2. Pengguna yang memanfaatkan teknologi AI dalam tindak pidana *deepfake* untuk tujuan kriminal**

Pengguna yang memakai teknologi AI dalam tindak pidana *deepfake* untuk memperoleh keuntungan atau menipu pihak ketiga, seperti dalam kasus otentikasi transaksi, maka perbuatannya memenuhi unsur penipuan dan pemalsuan, yang dapat dipidana sebagai pelaku utama atau turut serta tergantung peran. Meskipun pelaku perbuatan menggunakan hasil ciptaan pihak lain akan tetap dapat menimbulkan pertanggungjawaban jika unsur *mens rea* nya terpenuhi.

## **3. Pengembang model AI atau penyedia layanan konten *Deepfake***

Dalam proses pembuktian sulit apabila secara langsung memidana sistem atau algoritma, maka dalam menemukan siapa yang dapat mempertanggungjawabkan perbuatan tindak pidana akibat dari sistem yang bermasalah maka orang atau entitas yang termasuk subyek hukum yang mengembangkan atau menyediakan dapat dilimpahkan tanggung jawab pidananya apabila memenuhi satu dari beberapa kondisi, antara lain:

- a. Keterlibatan langsung, artinya pengembang sengaja merancang model untuk tujuan kriminal atau menyediakan model dengan fitur yang jelas

dimaksudkan untuk memfasilitasi pembuatan pemalsuan identitas digital yang ilegal. Perbuatan yang secara langsung dilakukan ini dapat mengakibatkan terpenuhinya unsur kesalahan dalam tindak pidana.

- b. Kelalaian atau *culpa lata*, hal ini berarti jika pengembang lalai menerapkan langkah mitigasi yang wajar misalnya saat sistem mengalami masalah dan pembuat tidak melakukan filter, atau tidak menerapkan batasan penggunaan, dapat dipertimbangkan tanggung jawabnya atas kelalaiannya apabila norma positif yang berlaku menyatakan kewajiban pengembang dalam mengantisipasi permasalahan yang ada pada sistem.<sup>98</sup>

#### 4. Platform dan korporasi teknologi penjiar konten hasil *deepfake*

Platform yang menyiarkan hasil dari pemalsuan identitas digital atau *deepfake* dapat dikenai tanggung jawab pidana atau administratif apabila:

- a. Secara nyata memfasilitasi penyebaran setelah diberi peringatan namun tidak bertindak
- b. Turut serta atau mendapat keuntungan dari penyalahgunaan dan pemalsuan yang dilakukan
- c. Melanggar kewajiban perlindungan data atau pengelolaan konten menurut peraturan yang tertera dalam PSE.

UU PDP dan Permenkominfo akan memberi ruang sanksi administratif yang dapat menjadi pemicu timbulnya tanggung jawab pidana

---

<sup>98</sup> Loc. Cit, Ecep Nurjamal, hlm. 32

apabila dalam perbuatan pemalsuannya ditemukan unsur perbuatan yang melawan hukum.

Peraturan mengenai penyalahgunaan AI memang sudah diatur meskipun tidak spesifik mengatur mengenai AI. Namun terdapat hal-hal lain yang perlu untuk lebih diperhatikan, yakni proses saat pembuktian. Dalam membuktikan tindak pidana yang dilakukan melalui AI, terdapat tantangan dan masalah.

Masalah pembuktian dalam tindak pidana yang melibatkan teknologi AI seperti digunakan dalam tindak pidana *deepfake*, menjadi salah satu tantangan paling kompleks dalam ranah hukum pidana digital di Indonesia. Salah satu kendala utamanya terletak pada kesulitan dalam identifikasi, dimana hasil manipulasi dari tindak pidana *deepfake* sering kali hampir tidak dapat dibedakan dari wujud aslinya oleh penglihatan manusia biasa.

Untuk membuktikan bahwa suatu materi digital merupakan hasil rekayasa, maka diperlukan analisis forensik multimedia yang mendalam, termasuk pemeriksaan metadata, penelusuran jejak transformasi digital, identifikasi bahan dasar yang dihasilkan oleh suatu sistem dalam algoritma *Generative Adversarial Network* atau GAN, serta perbandingan dengan dataset asli yang digunakan dalam proses pembuatannya. Proses ini membutuhkan keahlian teknis tinggi serta alat analisis digital yang canggih agar hasil pembuktian dapat diterima secara sah di pengadilan. Walaupun Undang-Undang Nomor 11 Tahun 2008 tentang UU ITE telah mengakui alat bukti elektronik sebagai bukti yang otentik di pengadilan, unsur keaslian, integritas, dan keandalan bukti digital tetap menjadi faktor krusial. Selain itu, sesuatu yang

dapat menjadi bukti elektronik harus dapat diverifikasi dan dipertanggungjawabkan secara forensik agar memiliki nilai pembuktian yang kuat.

Dalam aspek pembuktian unsur kesalahan atau *mens rea* juga menjadi permasalahan tersendiri. Untuk membuktikan adanya niat atau kesengajaan pelaku, penegak hukum harus mengumpulkan bukti digital seperti data aktivitas pembuatan konten, rekam jejak transaksi atau komunikasi daring, serta bukti adanya keuntungan ekonomi atau motif tertentu di balik penggunaan hasil *deepfake*. Di samping itu, keterangan ahli digital forensik sering kali dibutuhkan untuk menjelaskan proses teknis dan relevansi bukti tersebut di hadapan hakim.

Adapun permasalahan yang tidak kalah penting adalah proses pembuktian adanya pidana diluar lingkup yurisdiksi Indonesia. Dalam banyak kasus, data atau server tempat *deepfake* dibuat dan disebar berada di luar wilayah hukum Indonesia, sehingga proses penegakan hukum memerlukan kerja sama internasional melalui mekanisme *Mutual Legal Assistance Treaty* atau MLAT untuk memperoleh data dan alat bukti dari negara lain.

Proses tersebut menimbulkan tantangan dari segi waktu, prosedur, serta terdapat perbedaan sistem hukum antarnegara. Sehingga efektivitas penegakan hukum terhadap penyalahgunaan teknologi AI dalam tindak pidana *deepfake* sangat bergantung pada kemampuan aparat penegak hukum dalam memahami teknologi, menjaga integritas dalam menegakkan hukum di ruang digital, serta memperkuat kerja sama lintas batas yurisdiksi untuk menjamin keadilan dan kepastian hukum di era digital.

Permasalahan pada saat menentukan pertanggungjawaban dan dalam proses pembuktian cukup membutuhkan identifikasi yang sangat dalam dan menteluruh. Akan tetapi dalam konteks tindak pidana yang melibatkan penggunaan teknologi AI untuk menciptakan atau menyebarkan identitas palsu, pelaku biasanya mengajukan pembelaan.

Adapun bentuk pembelaan dan alasan pembebasan hukum yang dapat diajukan oleh pelaku dalam proses peradilan pidana. Salah satu pembelaan yang umum diajukan adalah adanya persetujuan dari pihak korban. Misalnya, jika pembuatan konten *deepfake* dilakukan berdasarkan izin eksplisit dari individu yang wajah atau suaranya digunakan, maka unsur melawan hukum dapat dianggap tidak terpenuhi. Namun, pembelaan ini hanya sah apabila izin tersebut diberikan secara sadar, tertulis, dan tanpa adanya unsur paksaan atau penipuan, serta konten yang dihasilkan tidak menimbulkan kerugian terhadap kehormatan atau privasi individu yang bersangkutan.

Pelaku dapat mengajukan pembelaan bahwa konten *deepfake* dibuat dalam konteks karya seni, parodi, atau satire. Namun, dalam praktiknya, pembelaan ini harus diuji terhadap unsur niat jahat dan akibat yang ditimbulkan, karena kebebasan berekspresi tidak bersifat absolut. Apabila karya tersebut menimbulkan kerugian, mencemarkan nama baik, atau melanggar privasi orang lain, maka pelaku tetap dapat dimintai pertanggungjawaban pidana.

Pembelaan lain yang mungkin diajukan adalah ketiadaan unsur kesengajaan. Dalam kasus tertentu, pelaku mungkin hanya menggunakan perangkat atau *software* berbasis AI tanpa menyadari bahwa hasil akhirnya akan

disalahgunakan untuk kepentingan yang melawan hukum. Dalam kondisi seperti itu, jika dapat dibuktikan bahwa pelaku sama sekali tidak mengetahui atau tidak menghendaki akibat yang ditimbulkan, maka unsur kesengajaan dapat dianggap tidak terpenuhi. Namun, apabila terbukti bahwa pelaku lalai, misalnya dengan tidak memperhatikan standar keamanan, etika penggunaan, atau akibat potensial dari tindakannya, maka pertanggungjawaban pidana masih dapat diterapkan berdasarkan prinsip kelalaian atau tanggung jawab korporatif.

Penilaian batas antara pembelaan yang sah dan alasan pembebasan pidana dalam kasus tindak pidana *deepfake* sangat bergantung pada niat, konteks, serta akibat hukum yang ditimbulkan oleh tindakan tersebut. Oleh karena itu, hakim dan penegak hukum harus menilai secara cermat setiap unsur fakta, motif, serta kesadaran pelaku agar penerapan hukum tetap sejalan dengan prinsip keadilan substantif dan proporsionalitas dalam hukum pidana modern.

Permasalahan-permasalahan yang terjadi merupakan akibat dari adanya kekosongan hukum yang spesifik terkait penggunaan teknologi AI dalam pembuatan konten yang menimbulkan tindak pidana. Kekosongan hukum tersebut menjadi tantangan serius dalam sistem hukum positif Indonesia. Hingga saat ini, belum terdapat definisi yuridis yang eksplisit mengenai apa itu tindak pidana *deepfake*, sehingga para aparat penegak hukum sering kali harus melakukan penafsiran analogis atau sistematis lintas peraturan, seperti mengacu pada ketentuan dalam KUHP, UU ITE, dan UU PDP.

Ketiadaan peraturan khusus ini menimbulkan ketidakpastian hukum dan potensi ketidak konsistensi dalam putusan pengadilan, karena hakim dapat



menafsirkan unsur tindak pidana yang berkaitan dengan pemalsuan digital secara berbeda-beda tergantung pada konteks kasus dan pendekatan hukum yang digunakan. Selain itu, terdapat ketidakjelasan atribusi tanggung jawab hukum terhadap pihak-pihak yang terlibat dalam ruang lingkup penyalahgunaan AI, khususnya pengembang, penyedia platform, atau distributor teknologi konten *deepfake*.

Pertanyaan mendasar muncul mengenai sejauh mana mereka dapat dimintai pertanggungjawaban apabila teknologi yang mereka ciptakan disalahgunakan oleh pihak ketiga untuk tujuan kriminal. Tanpa adanya pengaturan eksplisit yang menetapkan batas tanggung jawab antara pengguna, pengembang, dan penyelenggara sistem elektronik, proses pembuktian kesalahan menjadi sulit.

Dalam praktiknya, pemidanaan terhadap pengembang AI hanya dimungkinkan apabila dapat dibuktikan adanya niat jahat atau *mens rea* ataupun adanya kelalaian berat dalam menciptakan suatu sistem yang memungkinkan terjadinya suatu pelanggaran hukum. Kondisi tersebut menunjukkan urgensi perlunya pengaturan khusus mengenai teknologi AI dalam hukum nasional.

Beberapa prinsip yang dapat diadopsi antara lain:

1. Kewajiban dalam perlindungan privasi yang aman, hal ini sangat diperlukan karena dengan memberikan perlindungan terhadap privasi, pengembang AI harus memperhatikan aspek etika, keamanan, dan privasi sejak tahap perancangan sistem

2. Kewajiban mitigasi penyalahgunaan, yang menuntut penyedia platform untuk aktif mencegah penggunaan teknologi secara ilegal
3. Aturan pelabelan konten berbasis AI generatif, agar masyarakat dapat membedakan antara konten asli dan hasil manipulasi digital
4. Mekanisme pelaporan dan perbaikan cepat, hal ini perlu dilakukan dalam menanggulangi penyebaran konten *deepfake* yang merugikan individu atau masyarakat.

Prinsip-prinsip berikut akan memperkuat perlindungan hukum terhadap korban sekaligus menegaskan tanggung jawab semua pihak yang terlibat dalam penggunaan dan penyebaran teknologi AI. Sehingga, pengaturan yang komprehensif tidak hanya mengisi kekosongan hukum, melainkan juga menjadi fondasi penting dalam menghaikan sistem hukum yang akuntabel, dan responsif mengenai pertumbuhan teknologi digital modern.

Analisis dari banyaknya kasus mengenai penyalahgunaan AI yang terjadi, yang salah satu penyebabnya yaitu adanya kekosongan hukum mengenai teknologi AI. Sehingga apabila dilihat dari hukum positif Indonesia dan praktik hukum internasional, terdapat beberapa saran hukum yang perlu dipertimbangkan untuk memperkuat regulasi dan penegakan hukum terhadap penyalahgunaan teknologi AI dalam konteks pemalsuan identitas digital atau *deepfake*, antara lain:

Pertama, diperlukan langkah konkret dalam merumuskan definisi hukum dan delik khusus mengenai manipulasi identitas digital berbasis teknologi AI yang diatur didalam peraturan perundang-undangan, baik dengan

menambahkan ketentuan baru dalam UU ITE maupun melalui revisi atau perluasan peraturan didalam KUHP. Dengan Definisi hukum yang jelas akan menghilangkan ketidakpastian penafsiran dan menjadi dasar bagi aparat penegak hukum dalam menjerat pelaku secara efektif, tanpa bergantung pada analogi pasal-pasal yang tidak secara langsung relevan.

Kedua, perlu dilakukan penegasan dalam pertanggungjawaban pidana bagi korporasi, pengembang, dan penyedia teknologi AI, terutama terkait dengan standar kelalaian dan kewajiban mitigasi penyalahgunaan dan permasalahan pada sistem. Dalam kasus yang melibatkan data biometrik atau privasi individu, dapat dipertimbangkan penerapan prinsip tanggung jawab pidana, di mana pelaku atau penyelenggara sistem dapat dimintai pertanggungjawaban tanpa pembuktian unsur kesengajaan, apabila terbukti lalai melindungi keamanan data atau mengantisipasi penyalahgunaan teknologi atau sistem yang dikembangkannya.

Ketiga, penguatan kapasitas seluruh lembaga penegak hukum, dengan menguatkan kemampuan serta ilmu para aparat penegak hukum menjadi langkah strategis yang tak terelakkan. kepolisian, kejaksaan, dan lembaga peradilan perlu dilengkapi dengan kemampuan forensik digital yang mumpuni, baik dalam hal analisis bukti multimedia, verifikasi keaslian konten, maupun deteksi pola manipulasi konten *deepfake*. Pengembangan standar teknis dalam pembuktian juga diperlukan agar bukti digital yang diajukan di pengadilan memiliki nilai integritas, validitas, dan dapat dipertanggungjawabkan secara ilmiah.

Keempat, sistem hukum nasional juga perlu dalam menyediakan mekanisme perbaikan yang cepat, melalui kerangka UU PDP dan regulasi Penyelenggara Sistem Elektronik atau PSE. Mekanisme ini mencakup hak untuk penghapusan data, prosedur takedown konten digital yang merugikan, serta pemberian kompensasi kepada korban atas pelanggaran data atau penyalahgunaan identitas digitalnya.

Mengingat sifat lintas batas yuridiksi dari tindak pidana digital, Indonesia perlu memperkuat kerja sama internasional melalui *Mutual Legal Assistance Treaty* maupun dengan perjanjian bilateral lain untuk mempercepat proses penelusuran pelaku lintas negara, penyitaan bukti elektronik, dan pertukaran data forensik.

Terakhir, diperlukan pendekatan preventif sebagai bagian dari strategi hukum yang berkelanjutan. Pemerintah dapat memberlakukan regulasi desain aman, kewajiban pelabelan konten berbasis AI generatif, serta program literasi digital dan etika teknologi bagi masyarakat. Pendekatan ini tidak hanya berfungsi sebagai langkah pencegahan terhadap potensi kejahatan digital, tetapi juga berkontribusi pada pembangunan ekosistem digital yang aman, transparan, dan bertanggung jawab sejalan dengan prinsip-prinsip hukum siber modern dan perlindungan hak asasi manusia di era teknologi digital saat ini.

## BAB VI

### PENUTUP

#### A. Kesimpulan

1. Bentuk tindak pidana pemalsuan identitas digital melalui teknologi *Artificial Intelligence* menurut hukum positif yang ada di Indonesia mencakup tindakan manipulasi data elektronik, pelanggaran privasi, pencemaran nama baik, serta penyebaran informasi palsu, yang dapat dijerat dengan ketentuan UU ITE, KUHP, dan UU PDP. Meskipun secara normatif sudah ada landasan hukum yang dapat digunakan, secara praktis masih dibutuhkan pengaturan yang lebih spesifik mengenai penggunaan teknologi AI agar hukum pidana nasional mampu menyesuaikan diri dengan dinamika kejahatan digital di era kecerdasan buatan.
2. Pertanggungjawaban pidana atas penggunaan AI untuk membuat konten *deepfake* dapat ditegakkan dengan menggunakan kombinasi ketentuan UU ITE yang tertera Pasal 35, Pasal 27, Pasal 28, KUHP yang tercantum dalam pasal mengenai pemalsuan serta penipuan, UU PDP dalam pasal mengenai penggunaan data pribadi atau biometrik, serta peraturan administratif terkait penyelenggaraan sistem elektronik. Bentuk pertanggungjawaban bergantung pada peran subyek yang bersangkutan yaitu terdiri dari pembuat atau penyebar dikenai pertanggungjawaban langsung, untuk pengguna dapat dipidana sebagai pelaku atau turut serta, kemudian bagi pengembang

atau platform dapat dimintai pertanggungjawaban apabila ada niat, kelalaian berat, atau dasar korporasi ataupun administratif yang jelas.

## **B. Saran**

1. Perlunya pengaturan khusus tentang teknologi *Artificial Intelligence* dalam hukum nasional. Pemerintah perlu segera merumuskan regulasi khusus yang mengatur penggunaan, pengawasan, serta pertanggungjawaban pidana atas penyalahgunaan teknologi *Artificial Intelligence*, termasuk tindak pidana *deepfake*.
2. Saran bagi masyarakat pendekatan preventif dapat dilakukan melalui literasi digital dan etika teknologi. Perlu dilakukan pendekatan preventif melalui pendidikan etika teknologi dan literasi digital kepada masyarakat luas. Masyarakat harus memahami potensi bahaya dari tindak pidana *deepfake*, cara melindungi data pribadi, serta pentingnya verifikasi konten digital sebelum menyebarkannya.



## DAFTAR PUSTAKA

### A. Al-Qur'an dan Hadist

Al-Qur'an Surat Al-Baqarah Ayat: 42

Al-Qur'an Surat Al-Maidah ayat 8

### B. Buku

Agus Rusianto, 2016, *Tindak Pidana dan Pertanggung Jawaban Pidana*, Prenadamedia Group, Jakarta

Al- Khorwizmi dan Arif Ridho.L., 2023, *Artificial Intelligence*, UMSU Press

Arianus Harefa, 2023, *Dasar-Dasar Hukum Pidana Di Indonesia-Pasca Berlakunya KUHP Nasional*, CV jejak anggota IKAPI, Jawa Barat.

Ecep Nurjamal, 2020, *Hukum Pidana dan Penerapan Hukum Acara Pidana*, Edu Publisher, Jawa Barat.

Faisal Riza & Erwin Amsadi, 2023, *Hukum Pidana Indonesia*, UMSU Press, Medan.

Feri Sulianta, 2025, *Dasar dan Konsep Modern AI*, Penerbit Feri Sulianta

Firdaus Renuat, Padrisan Jamba. et al., 2023, *Pengantar Hukum Pidana*, CV. Gita Lentera, Sumatera Barat

Halifa Haqqi dan Hasna Wijayati, 2019, *Revolusi Industri 4.0 di Tengah Society 5.0*, Quadrant, Yogyakarta.

Hanafi Amrani dan Mahrus Ali, 2015, *Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan*, Rajawali Press, Jakarta.

I Gusti Kade Budhi.H., 2022, *Artificial Intelligence: Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana*, PT Raja Grafindo Persada, Depok.

Jhon Tyson.P., Ismansyah, et al., 2025, *Inkonsistensi Penerapan Sanksi Pidana Pada Undang-Undang Perkebunan*, CV. Green Pub;isher Indonesia, Jawa Barat.

John C.Lennox, 2020, *Pandangan Kristen Tentang Kecerdasan Buatan (Artificial Intelligence) dan Masa Depan Umat Manusia*, Terjemahan Stevy Tilaar, Jawa Timur.

Karimah, 2020, *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana (Fraud) Kecurangan Dalam Transaksi Perbankan*, Guepedia, DKI Jakarta.

Kelleher John D., 2019, *Deep Learning*, 2019, The MIT Press Essential Knowledge Series, Massachusetts

Mia Amalia, M. Ikhwan Raya. et al., 2024, *Asas-Asas Hukum Pidana*, PT. Sonpedia Publishing Indonesia, Jambi.

Sinamora Sampur Dongan dan Mega Fitri Hertini, 2015, *Hukum Pidana Dalam Bagan*, FH Untan Press, Pontianak.

Singgih Subiyantoro, 2024, *Buku Ajar Artificial Intelligence*, Penerbit Underline (Anggota IKAPI No. 267/JTE/2023), Jawa Tengah

Sumiati Adelina.H., Ica Karina. et al., 2024, *Pengantar Hukum Pidana (Teori dan Implementasi Pada Era Revolusi Industri 4.0 Menuju Era Society 5.0)*, PT. Sonpedia Publishing Indonesia, Jambi.

Yogi Fahrissal, 2020, *Penegakan Hukum Pidana Dalam Sengketa Penguasaan Tanah*, CV. Adamu Abimata, Jawa Barat. Muhaimin, 2020, *Metode Penelitian Hukum*, Mataram University Press, Mataram.

### **C. Peraturan Perundang-Undangan**

KUHP

Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan UU No. 19 Tahun 2016.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

### **D. Jurnal dan Karya Tulis Ilmiah**

Afridus Darto, Arif Syahrul Alam. et al., 2023, *Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pembunuhan Pengidap Gangguan Kejiwaan Dalam Perspektif Hukum Pidana*, *Jurnal Ilmu Hukum Wijaya Putra*, Vol. 1 No. 2

Amelia Damayanti & Susi Wulandari, 2024, *Artificial Intelligence In The Discourse of Hadith Science*, *International Conference on Muslim Society and Thought*, Vol.4

- Anfa'un Nisa'.F.R., Syariffudin, et al., 2025, Perlindungan Hukum Terhadap Korban Penyalahgunaan Teknik *Deepfake*, *Perspektif Administrasi Publik dan Hukum*, Vol. 2, No. 1
- Annisa Ayu 2024, "Persepsi Mahasiswa Terhadap Pemanfaatan *Artificial Intelligence* (AI) Chat GPT Sebagai Sumber Informasi Tugas Kuliah", *Skripsi Fakultas Dakwah UIN Prof. K.H. Saiffudin Zuhri*,
- Banfatin Patricia Morisa, et al., 2025, Pengaturan Hukum Pidana di Indonesia Terhadap Penyalahgunaan Teknologi *Artificial Intelligence Deepfake* Dalam Melakukan Tindak Pidana Cybercrime, *Jurnal Pemuliaan Keadilan*, Vol. 2, No. 1.
- Chesney, Robert & Citron, Danielle Keats, 2019, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, *California Law Review*, Vol. 107, No. 6
- Devianto Devianto dan Saruni Dwiasnati, 2020, Kerangka Kerja Sistem Kecerdasan Buatan dalam Meningkatkan Kompetensi Sumber Daya Manusia Indonesia, *Jurnal Telekomunikasi dan Komputer* Vol. 10, No. 1
- Evi Febryani, Dian Puspa Iwari. et al., 2024, Pertanggung jawaban Pidana sebagai Dampak Penuntutan Terhadap Korporasi Akibat Pailit, *Collegium Studiosum Journal*, Vol. 7, No. 1
- Faras Paria, 2024, "Fenomena *Deepfake* di Era Teknologi Informasi Perspektif Al-Qur'an (Studi Kasus Analisis Q.S Al-Baqarah Ayat 42)", *Skripsi Fakultas Ushuluddin dan Pemikiran Islam UIN Raden Fatah Palembang*, Palembang.
- Fatma, 2023, "Pertanggungjawaban Hukum Terhadap Perintah Jabatan Tanpa Wewenang Melakukan Tindak Pidana Pembunuhan Perspektif Hukum Pidana Islam" *Skripsi Fakultas Syariah dan Ilmu Hukum Isla Institut Agama Islam Negeri Parepare*, Parepare.
- Fitri Dwi, Ade Nur Hidayah. Et al., 2025, *Deepfake* Dan Krisis Kepercayaan; Analisis Hukum Terhadap Penyebaran Konten Palsu di Media Sosial, *JIIIC: Jurnal Intelek Insan Cendekia*, Vol. 2, No 6
- Fritsky Lantang, Edwin Neil Tinangon. et al., 2024, Penggunaan Tanda Tangan Elektronik Dalam Perjanjian, *Lex Pravium*, Vol. 14, No. 02
- Hardiyanti Q, Shofika Safira Ayuni. et al., 2024, Kedudukan dan Konsep Pertanggungjawaban Artificial Intelligence Dalam Hukum Positif Indonesia, *UNES Law Review*, Vol. 6, No. 4

- Haris Muhammad Tan Abdul Rahman & Tantimin, 2022, Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan *Artificial Intelligence* di Indonesia, *Jurnal Komunikasi Hukum*, Vol. 8 No. 1.
- Hizkia A. M. Kaunang, 2019, Tanggungjawab Hukum Pemerintah Dalam Ketersediaan Fasilitas Masyarakat Pejalan Kaki dan Penyandang Cacat Menurut Undang-Undang Nomor 22 Tahun 2009, *Lex Et Societatis*, Vol. VII, No. 11
- Jefferson M.H. & Juanrico A.S.T, 2022, Kajian Hukum Pidana Dalam Penipuan Jual Beli Akun Permainan Online Melalui Media Sosial, *TATOHI Jurnal Ilmu Hukum*, Vol. 2, No. 3
- Kamarudin, 2023, “Analisis Pertanggungjawaban Tindak Pidana Korupsi Di Wilayah Kabupaten Mamasa (Studi Kasus Putusan No 28/Pid.Sus-TPK/2022/PN Mam dan No 29/Pid.Sus-TPK/2022/PN Mam)”, *Skripsi Fakultas Ilmu Sosial dan Ilmu Politik*, Universitas Sulawesi Barat, Mejene
- Kharis Selly Anastassia Amellia, et al., 2023, Analisis Tren Minat Masyarakat Indonesia terhadap *Artificial Intelligence* dalam Menyongsong Society 5.0: Studi Menggunakan Google Trends, *G-Tech: Jurnal Teknologi Terapan*, Vol.7, No. 4
- Kusuma Kusuma. et.al., 2024 “Ius Constituendum: Pengaturan *Artificial Intelligence* sebagai Upaya Anti Cyber Laundering dalam Mekanisme Central Bank Digital Currency (CBDC),” *Jurnal Pendidikan Tambusai*, Vol. 8, no. 2
- Mayana Ranti Fauza, et.al, 2024, Legal Issues of *Artificial Intelligence* – Generated Works: Challenges on Indonesian Copyright Law, *Law Reform*, Vol, 20, No. 1
- Milenia Lombogia, Dezen D.R. et al., 2021, Sanksi Terhadap Pelaku Tindak Pidana Penggunaan Surat Palsu Menurut Kitab Undang-Undang Hukum Pidana (KUHP), *Lex Crimen*, Vol. X, No. 9
- Naitali, A., Ridouani, M., Salahdine, F. et al., 2023, *Deepfake* attacks: Generation, detection, datasets, challenges, and research direction. *Computers*, Vol. 12, No. 10, hlm. 26.
- Noerman Chiquita Thefirstly & Aji Lukman Ibrahim, 2024, Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Perlindungan Negara, *Jurnal USM Law Review*, Vol. 7 No. 2

- Putri Jeri Astuti, Suwarno Abadi. et al., 2024, Penerapan Sanksi Pidana Terhadap Pelaku Pemalsuan Dokumen Yang Dilakukan Melalui Media Sosial, *Jurnal Ilmu Hukum Wijaya Putra*, Vol. 2, No. 1.
- Setiawan, R., 2023, Pemalsuan Identitas Digital dalam Perspektif Hukum Siber, *Jurnal Hukum dan Teknologi*, Vol. 5, No. 2.
- Situmerang Bramcov Stivens et al., 2024, Pengaruh *Artificial Intelligence* Terhadap Tingkat Kasus Deep Fake Pada Selebritas Di Twitter, *Jurnal Device*, Vol.14, No. 1
- Sri Maharani M.T.V.M & Rambu Earyca Maharani, 2025, Ganti Kerugian Akibat Penyalahgunaan *Artificial Intelligence (Deepfake)* pada Citra Orang Terkenal di Facebook Berdasarkan Pasal 1365 BW, *Rewang Rencang: Jurnal Hukum Lex Generalis*, Vol. 6, No. 4, hlm. 7
- Sudirwo, Abdul Hadi. et al., 2025, *Artificial Intelligence (Teori, Konsep, dan Implementasi di Berbagai Bidang)*, Jambi, hlm. 2
- Supriyadi Endang Irawan & Dianing Banyu Asih, 2020, “Implementasi *Artificial Intelligence* (AI) di Bidang Administrasi Publik Pada Era Revolusi Industri 4.0”, *Jurnal Sosial dan Humaniora Universitas Muhammadiyah Bandung*, Vol. 02 No.02
- Tiara.A.M.J Nila, 2024, Analisis Pendekatan Ekonomi Hukum Terhadap Kriminalisasi *Deepfake*, Literasi Sintaks: *Jurnal Ilmiah Indonesia*, Jilid. 9
- Vacari Cristian and Andrew Chadwick, 2020, “*Deepfakes* and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News,” *Social Media + Society* Vol. 6 No. 1
- Yansen. B Desty Aster et al, 2025 Kriminalisasi Pelanggaran Protokol Digital Tinjauan Hukum Pidana Terhadap Penyebaran *Deepfake* di Media Sosial, *INNOVATIVE: Journal Of Social Science Research*, Vol. 5, No. 4

#### **E. Lain-lain**

- "Apa Itu AI (*Artificial Intelligence*): Pengertian, Kelebihan, Dan Kekurangan", universitas stekom <https://stekom.ac.id/artikel/apa-itu-ai-kecerdasan-buatan-pengertian-kelebihan-kekurangan>
- “Pentingnya Bangsa Ini Mulai Adaptif Dengan Industri 5.0”, <https://www.republika.co.id/berita/qynv2n371/pentingnya-bangsa-ini-mulai-adaptif-dengan-industri-50>