

**HUMAN ERROR DAN INTENTIONAL MISUSE DALAM PENYEBARAN HOAKS POLITIK BERBASIS AI: PERSPEKTIF KRIMINOLOGI DAN HUKUM PIDANA INDONESIA****Anisa Dyah Wijayanti<sup>1</sup>, Yosanda Syahwa Septyani<sup>2</sup>, Oci Senjaya<sup>3</sup>**Email: [anisadyahwijayantii@gmail.com](mailto:anisadyahwijayantii@gmail.com), [yosanda.s.s@gmail.com](mailto:yosanda.s.s@gmail.com), [oci.senjaya@fh.unsika.ac.id](mailto:oci.senjaya@fh.unsika.ac.id)**Fakultas Hukum, Universitas Singaperbangsa Karawang****Abstract**

*The development of artificial intelligence (AI) has made it easier to create and distribute various types of information, but it has also created new problems related to the spread of political hoaxes. AI can be used to produce deepfake videos, audio, images, and texts that appear authentic and may influence public perceptions and create legal problems. This research aims to examine the forms of human error and intentional misuse in the spread of AI-based political hoaxes and to analyze criminal liability under Indonesian criminal law. This research uses a normative juridical method with a criminological approach and applies a descriptive-analytical analysis. The results show that human error generally occurs due to lack of knowledge, negligence, low digital literacy, and the habit of sharing information without proper verification. In contrast, intentional misuse involves the deliberate and planned use of AI to manipulate public opinion, harm certain individuals, or gain political advantages. From a criminological perspective, this phenomenon can be explained through routine activity theory and rational choice theory, which emphasize motivated offenders, suitable targets, weak guardianship, and the consideration of benefits and risks. Under Indonesian criminal law, criminal liability remains focused on the human user of AI by considering the elements of fault, intention, or negligence. Although the Electronic Information and Transactions Law and the Indonesian Criminal Code provide legal grounds for dealing with the spread of false information, the development of AI still creates challenges in proving the offender's intent, identifying perpetrators, and determining the distribution of responsibility. Therefore, stronger regulations, improved digital forensic capabilities, effective law enforcement, and increased digital literacy are needed.*

**Article History**

Received : Oktober 2026

Reviewed: Oktober 2026

Published: Oktober 2026

**Copyright : Author****Publish by : CAUSA**

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

<sup>1</sup> 2410631010015, Fakultas Hukum Universitas Singaperbangsa Karawang

<sup>2</sup> 2410631010079, Fakultas Hukum Universitas Singaperbangsa Karawang

<sup>3</sup> 0014019002, Fakultas Hukum Universitas Singaperbangsa Karawang

**Keywords:** *Human Error, Intentional Misuse, Political Hoaxes, Artificial Intelligence, Criminal Liability.*

### Abstrak

Perkembangan kecerdasan artifisial (AI) memberikan kemudahan dalam pembuatan dan penyebaran berbagai jenis informasi, tetapi di sisi lain juga menimbulkan persoalan baru dalam penyebaran hoaks politik. Penggunaan AI untuk membuat video deepfake, audio, gambar, maupun teks yang seolah-olah nyata dapat memengaruhi persepsi masyarakat dan menimbulkan persoalan hukum. Penelitian ini bertujuan untuk menganalisis bentuk human error dan intentional misuse dalam penyebaran hoaks politik berbasis AI serta melihat konstruksi pertanggungjawaban pidananya berdasarkan hukum pidana Indonesia. Penelitian ini menggunakan metode yuridis-normatif dengan pendekatan kriminologis dan bersifat deskriptif-analitis. Hasil penelitian menunjukkan bahwa human error umumnya terjadi karena ketidaktahuan, kelalaian, rendahnya literasi digital, serta kebiasaan menyebarkan informasi tanpa melakukan verifikasi. Sementara itu, intentional misuse dilakukan secara sadar dan terencana untuk memanipulasi opini publik, merugikan pihak tertentu, atau memperoleh keuntungan politik. Dari perspektif kriminologi, fenomena tersebut dapat dijelaskan melalui routine activity theory dan rational choice theory, karena adanya pelaku yang termotivasi, target yang sesuai, lemahnya pengawasan, serta pertimbangan antara keuntungan dan risiko. Dalam hukum pidana Indonesia, pertanggungjawaban tetap berpusat pada manusia sebagai pihak yang menggunakan AI, dengan memperhatikan unsur kesalahan, kesengajaan, atau kealpaan. Meskipun UU ITE dan KUHP telah memberikan dasar hukum untuk menindak penyebaran informasi palsu, perkembangan AI masih menimbulkan tantangan dalam pembuktian, penelusuran pelaku, dan pembagian tanggung jawab. Oleh karena itu, diperlukan penguatan regulasi, kemampuan forensik digital, penegakan hukum, serta literasi digital masyarakat.

**Kata kunci:** Human Error, Intentional Misuse, Hoaks Politik, Artificial Intelligence, Pertanggungjawaban Pidana.

## PENDAHULUAN

Perkembangan kecerdasan artifisial (AI) generatif telah mengubah cara informasi diproduksi dan didistribusikan dalam ruang digital.<sup>4</sup> Teknologi ini memungkinkan pengguna membuat teks, gambar, audio, dan video sintetis dengan cepat, murah, dan semakin sulit dibedakan dari konten autentik.<sup>5</sup> Dalam konteks politik, AI generatif tidak hanya dapat dimanfaatkan untuk kampanye dan pendidikan politik, tetapi juga berpotensi disalahgunakan untuk menyebarkan disinformasi yang persuasif dan sulit diverifikasi.<sup>6</sup>

Indonesia menghadapi tantangan serius terkait hoaks politik berbasis AI, terutama selama Pemilu 2024. Berbagai konten manipulatif beredar luas, termasuk video *deepfake* pidato Presiden Joko Widodo dalam bahasa Mandarin, video *deepfake* Prabowo Subianto berpidato dalam bahasa Arab, rekaman audio *deepfake* percakapan fiktif Surya Paloh dan Anies Baswedan, serta gambar sintetis yang digunakan untuk membangun narasi politik tertentu.<sup>7</sup> Konten-konten tersebut ditonton dan dibagikan jutaan kali di platform seperti TikTok, X (Twitter), dan WhatsApp, berpotensi memengaruhi persepsi publik terhadap kandidat dan proses demokrasi.<sup>8</sup>

Fenomena ini memunculkan dua pola perilaku manusia yang perlu dibedakan. Pertama, human error, yaitu kesalahan akibat ketidaktahuan, kelalaian, atau rendahnya literasi digital dan AI, seperti membagikan konten tanpa verifikasi atau membuat konten AI tanpa memahami risiko hukumnya.<sup>9</sup> Kedua, intentional misuse, yaitu penggunaan AI secara sadar dan terencana untuk memfitnah lawan politik, menciptakan skandal palsu, atau memengaruhi elektabilitas.<sup>10</sup> Perbedaan ini penting karena berkaitan dengan motif, tingkat kesalahan, dan pertanggungjawaban pidana.

Dari perspektif kriminologi, penyebaran hoaks politik berbasis AI dapat dipahami melalui *routine activity theory* dan *rational choice theory*. Teori pertama menjelaskan bahwa kejahatan terjadi ketika pelaku termotivasi, target sesuai, dan pengawasan lemah.<sup>11</sup> Teori kedua memandang pelaku melakukan kalkulasi rasional antara keuntungan

---

<sup>4</sup> Kementerian Komunikasi dan Digital Republik Indonesia, *Kajian Pemanfaatan Kecerdasan Artifisial dalam Komunikasi Pemerintah* (Jakarta: Direktorat Jenderal Komunikasi Publik dan Media, tanpa tahun).

<sup>5</sup> Ibid.

<sup>6</sup> Burhanuddin Muhtadi dan Maria Monica Wihardja, "Deepfakes and Selective Belief: How Partisanship Affects Voters' Exposure and Susceptibility to Deepfake Content," *ISEAS Perspective* 2024, no. 58 (2024): 2.

<sup>7</sup> Tempo, "CekFakta #271: Membaca Penyebab Kecenderungan Percaya Hoaks dan Deepfake saat Pemilu," 2 Agustus 2024, <https://www.tempo.co/newsletter/cekfakta-271-membaca-penyebab-kecenderungan-percaya-hoaks-dan-deepfake-saat-pemilu-32439>; MAFINDO, "Siaran Pers: Hoaks Politik Meningkatkan Tajam Jelang Pemilu 2024," 2 Februari 2024, <https://mafindo.or.id/2024/02/02/siaran-pers-mafindo-hoaks-politik-meningkat-tajam-jelang-pemilu-2024-ganggu-demokrasi-indonesia/>.

<sup>8</sup> Muhtadi dan Wihardja, "Deepfakes and Selective Belief," 3.

<sup>9</sup> Kementerian Komunikasi dan Digital Republik Indonesia, *Kajian Pemanfaatan Kecerdasan Artifisial dalam Komunikasi Pemerintah*.

<sup>10</sup> Sinta Dewi Rosadi, "The Use of AI and Social Media for 'Black Campaign' in Indonesia," Yale Law School, 2024, 8.

<sup>11</sup> Lawrence E. Cohen dan Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588–608.

(elektabilitas, popularitas, ekonomi) dan risiko (hukum, sosial).<sup>12</sup> AI generatif memperkuat kedua teori ini dengan menurunkan biaya kejahatan, memperluas jangkauan, dan mempersulit deteksi.

Secara normatif, Indonesia telah memiliki instrumen hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) yang dapat digunakan untuk menindak penyebaran informasi palsu.<sup>13</sup> Namun, ketentuan tersebut belum secara spesifik mengatur penggunaan AI generatif untuk hoaks politik, menimbulkan kesenjangan dalam pembuktian unsur kesengajaan dan pertanggungjawaban pidana.<sup>14</sup> KPU dan Bawaslu juga mengakui bahwa Indonesia belum memiliki regulasi khusus mengenai AI dan *deepfake* dalam konteks pemilihan.<sup>15</sup>

Berdasarkan uraian tersebut, penelitian mengenai "Human Error dan Intentional Misuse dalam Penyebaran Hoaks Politik Berbasis AI: Perspektif Kriminologi dan Hukum Pidana Indonesia" menjadi penting untuk mengkaji bentuk-bentuk kesalahan, pola perilaku, dan konstruksi pertanggungjawaban pidana yang relevan dengan perkembangan teknologi ini.

## METODE PENELITIAN

Penelitian ini merupakan penelitian hukum **yuridis-normatif** dengan pendekatan kriminologis dan bersifat **deskriptif-analitis**. Penelitian menelaah norma hukum, asas hukum, serta konstruksi pertanggungjawaban pidana dalam peraturan perundang-undangan Indonesia tanpa menggunakan data primer dari lapangan. Bahan penelitian berupa data sekunder yang diperoleh melalui studi kepustakaan (*library research*).<sup>16</sup>

Sifat deskriptif digunakan untuk menggambarkan fenomena penyebaran hoaks politik berbasis kecerdasan artifisial (*artificial intelligence*/AI), khususnya bentuk *human error* dan *intentional misuse*. Sifat analitis digunakan untuk menganalisis pertanggungjawaban pidana atas kedua bentuk perbuatan tersebut serta mengidentifikasi kesenjangan pengaturan dalam hukum positif Indonesia.<sup>17</sup>

---

<sup>12</sup> Derek B. Cornish dan Ronald V. Clarke, eds., *The Reasoning Criminal: Rational Choice Perspectives on Offending* (New York: Springer-Verlag, 1986), 1–16.

<sup>13</sup> Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1; Indonesia, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.

<sup>14</sup> Komisi Pemilihan Umum Republik Indonesia, "Tantangan Integritas Pemilu di Tengah Kemajuan Artificial Intelligence," 17 Mei 2026, <https://www.kpu.go.id/berita/baca/13661/tantangan-integritas-pemilu-di-tengah-kemajuan-artificial-intelligence>.

<sup>15</sup> Ibid.

<sup>16</sup> Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2014), hlm. 134.

<sup>17</sup> Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif* (Malang: Bayumedia Publishing, 2006), hlm. 57–58.

## Pendekatan Penelitian

Penelitian menggunakan tiga pendekatan. **Pendekatan perundang-undangan** (*statute approach*) dilakukan dengan menelaah peraturan yang relevan, khususnya UUD NRI Tahun 1945, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, serta Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum sebagaimana diubah dengan Undang-Undang Nomor 7 Tahun 2023.

**Pendekatan konseptual** (*conceptual approach*) digunakan untuk mengkaji doktrin mengenai kesalahan (*mens rea*), kesengajaan (*dolus*), kealpaan (*culpa*), dan pertanggungjawaban pidana. Pendekatan ini juga digunakan untuk membedakan *human error* sebagai kesalahan tidak disengaja dari *intentional misuse* sebagai penyalahgunaan teknologi AI secara sengaja.<sup>18</sup>

**Pendekatan kriminologis** digunakan untuk menganalisis pola perilaku, motivasi, dan faktor yang memfasilitasi penyebaran hoaks politik berbasis AI. Analisis menggunakan *routine activity theory* untuk menjelaskan peluang terjadinya kejahatan digital serta *rational choice theory* untuk menjelaskan pertimbangan rasional pelaku dalam menggunakan AI untuk memproduksi dan menyebarkan disinformasi.<sup>19</sup>

## Sumber Bahan Hukum

Bahan hukum primer meliputi peraturan perundang-undangan yang bersifat mengikat, yaitu UUD NRI Tahun 1945, KUHP baru, UU ITE beserta perubahannya, UU Pemilu beserta perubahannya, serta peraturan pelaksana yang relevan. Bahan hukum sekunder mencakup buku, jurnal, artikel ilmiah, hasil penelitian, tesis, makalah, *working paper*, serta laporan lembaga resmi atau organisasi masyarakat sipil yang membahas hukum pidana, hukum siber, AI, *deepfake*, disinformasi, dan integritas pemilu. Bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber daring resmi seperti JDIH BPK RI, JDIH Kementerian Sekretariat Negara, JDIH KPU, dan Kementerian Komunikasi dan Digital.<sup>20</sup>

## Teknik Pengumpulan dan Analisis

Pengumpulan bahan hukum dilakukan melalui penelusuran regulasi, literatur, dan sumber daring resmi. Bahan yang diperoleh kemudian diseleksi berdasarkan relevansi,

---

<sup>18</sup> Peter Mahmud Marzuki, *Penelitian Hukum*, hlm. 141–142.

<sup>19</sup> Lawrence E. Cohen dan Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979), hlm. 588–608; Derek B. Cornish dan Ronald V. Clarke, eds., *The Reasoning Criminal: Rational Choice Perspectives on Offending* (New York: Springer-Verlag, 1986), hlm. 1–16.

<sup>20</sup> Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2011), hlm. 20–21.

keakuratan, otoritas sumber, dan status keberlakuannya, lalu diinventarisasi secara sistematis.<sup>21</sup>

Analisis dilakukan secara kualitatif melalui identifikasi norma hukum, sistematisasi bahan hukum, analisis normatif, analisis kriminologis, dan penarikan kesimpulan secara deduktif. Analisis normatif menilai unsur tindak pidana dan bentuk pertanggungjawaban pidana, khususnya kealpaan pada *human error* serta kesengajaan pada *intentional misuse*. Analisis kriminologis menjelaskan faktor pendorong dan pola perilaku pelaku menggunakan teori *routine activity* dan *rational choice*.<sup>22</sup>

Penelitian ini tidak bertujuan menguji hipotesis, melainkan memberikan pemahaman komprehensif mengenai konstruksi pertanggungjawaban pidana atas penyebaran hoaks politik berbasis AI serta rekomendasi pengembangan hukum dan kebijakan di Indonesia.<sup>23</sup>

## HASIL DAN PEMBAHASAN

### 2.1 Bentuk-bentuk *Human Error* dan *Intentional Misuse* dalam Penyebaran Hoaks Politik Berbasis AI di Indonesia

#### 2.1.1 Konsep *Human Error* dan *Intentional Misuse* dalam Konteks AI

*Human error* dalam konteks AI merujuk pada kesalahan yang dilakukan pengguna karena ketidaktahuan, kelalaian, atau kurangnya pemahaman terhadap risiko hukum dan sosial dari penggunaan teknologi tersebut.<sup>24</sup> Kesalahan ini dapat terjadi pada tahap pembuatan konten, verifikasi, maupun distribusi informasi. Sementara itu, *intentional misuse* merupakan penggunaan AI secara sadar dan terencana untuk tujuan yang merugikan, seperti memanipulasi opini publik, memfitnah lawan politik, atau menciptakan narasi palsu untuk keuntungan elektoral.<sup>25</sup>

Perbedaan mendasar antara keduanya terletak pada unsur kesengajaan (*mens rea*). Pada *human error*, pelaku tidak memiliki niat jahat, sedangkan pada *intentional misuse*, kesengajaan merupakan unsur utama yang mendorong perbuatan tersebut.<sup>26</sup> Pemahaman terhadap perbedaan ini penting karena

<sup>21</sup> Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif*, hlm. 24.

<sup>22</sup> Peter Mahmud Marzuki, *Penelitian Hukum*, hlm. 156.

<sup>23</sup> Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, hlm. 57–58.

<sup>24</sup> Kementerian Komunikasi dan Digital Republik Indonesia, *Kajian Pemanfaatan Kecerdasan Artifisial dalam Komunikasi Pemerintah* (Jakarta: Direktorat Jenderal Komunikasi Publik dan Media, tanpa tahun).

<sup>25</sup> Burhanuddin Muhtadi dan Maria Monica Wihardja, "Deepfakes and Selective Belief: How Partisanship Affects Voters' Exposure and Susceptibility to Deepfake Content," *ISEAS Perspective* 2024, no. 58 (2024): 2–3.

<sup>26</sup> Indonesia, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.

berkaitan dengan konstruksi pertanggungjawaban pidana dan kebijakan penegakan hukum yang akan diterapkan.

### 2.1.2 Tipologi Hoaks Politik Berbasis AI di Indonesia

Berdasarkan temuan selama Pemilu 2024, hoaks politik berbasis AI di Indonesia dapat diklasifikasikan menjadi beberapa tipologi:

Tabel 1. Tipologi Hoaks Politik Berbasis AI di Indonesia

| Jenis Konten                 | Contoh Kasus                                                                                                   | Platform Distribusi           |
|------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------|
| Video <i>deepfake</i> pidato | Video Presiden Joko Widodo berpidato dalam bahasa Mandarin; video Prabowo Subianto berpidato dalam bahasa Arab | TikTok, X (Twitter), YouTube  |
| Audio <i>deepfake</i>        | Rekaman suara Surya Paloh menegur Anies Baswedan; rekaman percakapan fiktif Jokowi dan Ahmad Lutfi             | WhatsApp, TikTok, Instagram   |
| Gambar sintetis              | Foto tokoh politik dalam situasi fiktif; gambar balon udara Ganjar-Mahfud yang diedit dengan CGI               | Facebook, Instagram, X        |
| Teks generatif AI            | Narasi kebijakan fiktif, kutipan palsu, berita bohong yang dibuat menggunakan chatbot AI                       | Media sosial, grup percakapan |

Sumber: Diolah dari berbagai sumber, termasuk laporan Tempo CekFakta dan ISEAS.<sup>27</sup>

Kasus-kasus tersebut menunjukkan bahwa teknologi AI generatif telah digunakan secara luas untuk memproduksi konten politik yang menyesatkan. Video *deepfake* Prabowo berpidato dalam bahasa Arab, misalnya, ditonton jutaan kali di TikTok dan diduga bertujuan meningkatkan popularitasnya di kalangan pemilih Muslim.<sup>28</sup> Sementara itu, video *deepfake* Jokowi dalam bahasa Mandarin dan audio

<sup>27</sup> Tempo, "CekFakta #271: Membaca Penyebab Kecenderungan Percaya Hoaks dan Deepfake saat Pemilu," 2 Agustus 2024, <https://www.tempo.co/newsletter/cekfakta-271-membaca-penyebab-kecenderungan-percaya-hoaks-dan-deepfake-saat-pemilu-32439>; Muhtadi dan Wihardja, "Deepfakes and Selective Belief," 2–3.

<sup>28</sup> Muhtadi dan Wihardja, "Deepfakes and Selective Belief," 3.

*deepfake* Surya Paloh-Anies Baswedan diduga bertujuan merusak citra tokoh politik tertentu.<sup>29</sup>

### 2.1.3 Bentuk-bentuk *Human Error* dalam Penyebaran Hoaks Politik Berbasis AI

Beberapa bentuk *human error* yang teridentifikasi dalam penyebaran hoaks politik berbasis AI di Indonesia meliputi:

1. Pembuatan konten AI tanpa kesadaran melanggar hukum. Sebagian pengguna membuat konten AI berupa narasi, gambar, atau video tokoh politik hanya untuk tujuan hiburan atau "coba-coba" tanpa memahami bahwa tindakan tersebut dapat dipidana.<sup>30</sup> Ketidaktahuan terhadap ketentuan hukum, khususnya UU ITE dan KUHP, menjadi faktor utama.
2. Penyebaran tanpa verifikasi (*share before check*). Banyak pengguna media sosial membagikan konten politik berbasis AI tanpa melakukan verifikasi terlebih dahulu.<sup>31</sup> Rendahnya literasi digital dan literasi AI menyebabkan konten palsu mudah tersebar, terutama ketika konten tersebut sesuai dengan bias politik atau preferensi elektoral pengguna.
3. Penggunaan AI untuk "mempercantik" narasi politik. Beberapa pihak menggunakan AI untuk membuat konten visual atau teks yang lebih menarik tanpa memastikan kebenaran substansi informasi.<sup>32</sup> Tindakan ini sering kali dilakukan tanpa niat jahat, tetapi tetap berkontribusi terhadap penyebaran disinformasi.
4. Kurangnya pemahaman bahwa tindakan tersebut dapat dipidana. Aspek *ignorance of law* masih menjadi masalah serius. Banyak pengguna tidak menyadari bahwa menyebarkan hoaks politik, meskipun tanpa niat jahat, dapat dikenai sanksi berdasarkan UU ITE atau ketentuan pidana lainnya.<sup>33</sup>

### 2.1.4 Bentuk-bentuk *Intentional Misuse* dalam Penyebaran Hoaks Politik Berbasis AI

Berbeda dengan *human error*, *intentional misuse* melibatkan kesengajaan dan perencanaan yang matang. Beberapa bentuk yang teridentifikasi meliputi:

1. Perancangan narasi palsu untuk memfitnah tokoh politik. Konten *deepfake* audio Surya Paloh yang seolah-olah menegur Anies Baswedan merupakan contoh nyata

---

<sup>29</sup> Tempo, "CekFakta #271"; MAFINDO, "Siaran Pers: Hoaks Politik Meningkatkan Tajam Jelang Pemilu 2024," 2 Februari 2024, <https://mafindo.or.id/2024/02/02/siaran-pers-mafindo-hoaks-politik-meningkat-tajam-jelang-pemilu-2024-ganggu-demokrasi-indonesia/>.

<sup>30</sup> Kementerian Komunikasi dan Digital Republik Indonesia, *Kajian Pemanfaatan Kecerdasan Artifisial dalam Komunikasi Pemerintah*.

<sup>31</sup> Tempo, "CekFakta #299: Ketika Disinformasi AI Mengintai," 14 Februari 2025, <https://www.tempo.co/newsletter/cekfakta-299-ketika-disinformasi-ai-mengintai-kilas-balik-cek-fakta-2024-1206902>.

<sup>32</sup> Ibid.

<sup>33</sup> Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

penggunaan AI untuk menciptakan narasi yang merugikan kandidat tertentu.<sup>34</sup> Konten ini dirancang untuk menggambarkan Anies sebagai "boneka" politik Surya Paloh.

2. Penciptaan skandal palsu untuk memengaruhi elektabilitas. Video *deepfake* yang menampilkan tokoh politik dalam situasi yang tidak pernah terjadi, seperti pidato dalam bahasa asing atau percakapan fiktif, dibuat untuk menciptakan skandal yang dapat memengaruhi persepsi publik.<sup>35</sup>
3. Penggunaan jaringan bot dan akun palsu. Penyebaran hoaks politik berbasis AI sering kali diperkuat dengan penggunaan bot dan akun palsu untuk menciptakan ilusi bahwa konten tersebut viral dan dipercaya banyak orang.<sup>36</sup> Teknik ini dikenal sebagai *astroturfing* dan dapat memanipulasi algoritma media sosial.
4. Eksploitasi momen krusial dalam kontestasi politik. Penyebaran hoaks sering kali dilakukan pada masa kampanye, debat kandidat, masa tenang, atau bahkan hari pemungutan suara untuk memaksimalkan dampak terhadap opini publik.<sup>37</sup>

#### 2.1.5 Analisis Kriminologis: Faktor Penyebab dan Pola Perilaku

Dari perspektif kriminologi, fenomena hoaks politik berbasis AI dapat dianalisis menggunakan *routine activity theory* dan *rational choice theory*.

Berdasarkan *routine activity theory*, kejahatan terjadi ketika tiga elemen bertemu: pelaku yang termotivasi (*motivated offender*), target yang sesuai (*suitable target*), dan tidak adanya penjaga yang mampu (*absence of capable guardian*).<sup>38</sup> Dalam konteks hoaks politik berbasis AI:

- *Motivated offender*: aktor politik, tim siber, atau individu yang memiliki kepentingan elektoral atau ekonomi.
- *Suitable target*: publik pemilih yang memiliki literasi digital rendah, tokoh politik yang menjadi sasaran fitnah, atau proses demokrasi itu sendiri.
- *Absence of capable guardian*: lemahnya literasi AI masyarakat, keterbatasan mekanisme moderasi konten oleh platform, dan belum optimalnya penegakan hukum terhadap kejahatan siber politik.<sup>39</sup>

---

<sup>34</sup> Muhtadi dan Wihardja, "Deepfakes and Selective Belief," 2.

<sup>35</sup> ANFREL, *Elections and Technology Reader*, Juli–Agustus 2024

<sup>36</sup> Sinta Dewi Rosadi, "The Use of AI and Social Media for 'Black Campaign' in Indonesia," Yale Law School, 2024.

<sup>37</sup> Bawaslu, "Bawaslu Tekankan Urgensi Pengaturan AI dalam Pemilu," 4 September 2026, <https://jatim.antaranews.com/berita/994453/bawaslu-tekanan-urgensipengaturan-ai-dalam-pemilu>.

<sup>38</sup> Lawrence E. Cohen dan Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588–608.

<sup>39</sup> Muhtadi dan Wihardja, "Deepfakes and Selective Belief," 5–6.

Sementara itu, *rational choice theory* menjelaskan bahwa pelaku melakukan pertimbangan rasional antara keuntungan dan risiko sebelum melakukan kejahatan.<sup>40</sup> Dalam konteks hoaks politik berbasis AI:

- Keuntungan: peningkatan elektabilitas, penurunan citra lawan, keuntungan ekonomi dari engagement media sosial, atau popularitas.
- Risiko: kemungkinan terdeteksi, dipidana berdasarkan UU ITE atau KUHP, atau mendapat sanksi sosial.
- Kalkulasi: karena biaya pembuatan konten AI relatif rendah, dampaknya luas, dan penegakan hukum masih lemah, banyak pelaku menilai bahwa keuntungan lebih besar daripada risiko.

Teknologi AI generatif berfungsi sebagai *facilitator* dan *multiplier* dalam kejahatan ini. AI memungkinkan produksi konten manipulatif dalam jumlah besar dengan biaya rendah, mempercepat distribusi, dan mempersulit verifikasi. Hal ini menciptakan lingkungan yang kondusif bagi kejahatan informasi politik, terutama ketika tidak diimbangi dengan peningkatan literasi digital dan penegakan hukum yang efektif.

## 2.2 Konstruksi Pertanggungjawaban Pidana Dalam Penyebaran Hoaks Politik Berbasis AI menurut Hukum Pidana Indonesia

### 2.2.1 Teori Pertanggungjawaban Pidana

Tanggung jawab pidana dalam sistem hukum pidana Eropa Kontinental yang dianut oleh Indonesia berlandaskan pada prinsip kesalahan (*schuldbeginsel*) yang terlihat dalam pepatah *geen straf zonder schuld* (tidak ada hukuman tanpa kesalahan) dan *actus non facit reum nisi mens sit rea* (perbuatan tidak dapat membuat seseorang bersalah kecuali disertai dengan niat jahat). Asas kelayakan pemidanaan berakar pada adanya kejahatan atau kekhilafan, yang mana bentuk kelakuan tersebut dapat dikategorikan sebagai niat jahat (*opzet*) maupun kecerobohan (*culpa*).<sup>41</sup>

Kondisi tersebut memperlihatkan bahwasanya landasan penetapan sanksi hukum atas tindakan individu bersumber pada pembuktian terpenuhinya seluruh elemen delik pidana. Apabila komponen delik tersebut dapat dibuktikan secara sah, maka kekhilafan atau kesengajaan pelaku otomatis terkonfirmasi sehingga yang bersangkutan langsung dijatuhi hukum, yang menandakan bahwa pembebanan tanggung jawab pidana menyatu erat dengan elemen-elemen delik itu sendiri.<sup>42</sup>

---

<sup>40</sup> Derek B. Cornish dan Ronald V. Clarke, eds., *The Reasoning Criminal: Rational Choice Perspectives on Offending* (New York: Springer-Verlag, 1986), 1–16.

<sup>41</sup> Musa Darwin Pane, *Pengganti Kerugian Negara dalam Tindak Pidana Korupsi: Alternatif pengganti Pidana Penjara dan Pidana Mati dalam Perspektif Pemberantasan Korupsi*, Logos Publishing, Bandung, 2017, Hlm. 54.

<sup>42</sup> M. Rasyid Ariman dan Fahmi Raghieb, *Hukum Pidana*, Setara Press, Malang, 2015, hlm 205.

Pertanggungjawaban pidana pada dasarnya merupakan suatu bentuk pertanggungjawaban hukum yang dibebankan kepada seseorang atas perbuatan pidana yang telah dilakukannya, sepanjang orang tersebut memenuhi syarat untuk dapat dipersalahkan secara pidana. Dengan demikian, adanya suatu perbuatan yang memenuhi unsur tindak pidana belum secara otomatis berarti bahwa pelakunya harus dijatuhi pidana. Hukum pidana juga perlu melihat keadaan dan kondisi pelaku untuk menentukan apakah perbuatan tersebut benar-benar dapat dibebankan kepadanya sebagai suatu kesalahan. Pertanggungjawaban pidana pada akhirnya berkaitan dengan hubungan antara perbuatan yang dilakukan, kesalahan pelaku, serta kemampuan pelaku untuk mempertanggungjawabkan perbuatannya menurut hukum.

Berdasarkan gagasan Roeslan, pembebanan sanksi hukum dimaknai sebagai kelanjutan dari penilaian cela secara objektif atas suatu kejahatan, yang mana secara subjektif pelaku telah memenuhi kriteria hukum untuk dijatuhi hukuman atas tindakan yang dilakukannya.<sup>43</sup>

### 2.2.2 *Cyber Crime* / Kejahatan Digital

Kejahatan siber (*cybercrime*) dimaknai sebagai suatu tindak pidana yang menjadikan infrastruktur jaringan komputer sebagai sarana utama, target sasaran, ataupun komponen pendukung dalam pelanggaran hukum, dengan ciri khas berupa tingkat skalabilitas yang masif, sifatnya yang menembus batas negara, serta kerahasiaan identitas pelaku yang kerap menghambat proses penegakan hukum konvensional berbasis yurisdiksi teritorial (Wall, 2007).

Lanskap kejahatan siber (*cyber crime*) mengusung karakteristik khas yang berseberangan dengan delik tradisional, sebab eksekutor dapat melancarkan aksinya tanpa perlu hadir secara fisik di lokasi yang sama dengan pihak korban. Pelaku memanfaatkan penyamaran identitas, akun tanpa nama, jaringan privat, serta aneka rekayasa teknologi guna mengaburkan jejak keberadaannya. Implikasinya, penanganan serta pengungkapan tindak pidana siber menuntut keahlian teknis khusus serta skema penyidikan adaptif yang berbeda dari penanganan pidana umum. Terlebih lagi, penetrasi serangan siber sanggup dilancarkan dalam hitungan detik hingga menerpa korban berskala masif, yang mana tak jarang pelakunya berdomisili di luar batas yurisdiksi hukum nasional.

### 2.2.3 Pertanggungjawaban Pidana Dalam Penyebaran Hoaks Politik Berbasis AI

Gagasan mengenai beban ppidanaan dalam ranah hukum pidana pada hakekatnya merupakan instrumen aturan guna menilai kelayakan penjatuhan sanksi serta celaan terhadap individu atas eksekusi delik (*actus reus*) yang disertai kelakuan jahat atau kecerobohan (*mens rea*). Ajaran fundamental hukum pidana nasional bersandar pada prinsip legalitas dan prinsip tiada pidana tanpa kesalahan (*geen straf zonder schuld*), yang memosisikan niat, kesadaran, serta kehendak individu sebagai poros utama penjatuhan

---

<sup>43</sup> Roeslan Saleh., *Perbuatan Pidana dan Pertanggungjawaban Pidana; Dua Pengertian Dasar dalam Hukum Pidana*, Cetakan ke-3, Aksara Baru, Jakarta, 1983, hlm. 23

pertanggungjawaban hukum.<sup>44</sup> Dalam ranah disinformasi berbasis Kecerdasan Buatan (AI), paradigma ini menghadapi hambatan fundamental lantaran narasi palsu tidak lagi diproduksi secara murni oleh dorongan fisik manusia, melainkan dieksekusi lewat mekanisme algoritma yang beroperasi secara independen maupun parsial. Walau begitu, tatanan hukum nasional masih berorientasi pada manusia (*anthropocentric*), yang menyebabkan pembebanan sanksi pidana tetap ditujukan kepada individu selaku pemangku hak dan kewajiban hukum, sedangkan AI sekadar ditempatkan sebagai piranti atau perantara. Alhasil, tiap pengkajian sanksi hukum atas fabrikasi hoaks berbasis AI diwajibkan untuk mengurai peran serta manusia di balik pengoperasian piranti lunak tersebut. Kondisi ini membuktikan bahwasanya kendala paling krusial bukan berakar pada kekosongan regulasi pembedaan, melainkan pada gagapnya teori hukum konvensional dalam merespons interaksi modern antara niat manusia dan mekanisme kerja mesin.

Prinsip kesalahan (*mens rea*) menjadi poros utama dalam menetapkan penjatuhan sanksi hukum atas fabrikasi hoaks berteknologi AI, lantaran sistem kecerdasan buatan tidak dibekali kesadaran etik, kebebasan berkehendak, ataupun niat buruk. Dalam tatanan hukum pidana tradisional, bentuk kesengajaan (*dolus*) maupun kecerobohan (*culpa*) wajib melekat secara individu pada diri pembuat delik, sementara peranti AI sama sekali tidak memenuhi kualifikasi dasar tersebut.<sup>45</sup>

Atas dasar itulah, *mens rea* secara normatif dialihkan kepada pengguna atau pihak yang dengan sengaja mengeksekusi perintah (*prompt*), mengonfigurasi parameter, atau memanfaatkan *output* sistem AI untuk tindakan yang bertentangan dengan hukum. Dalam aplikasinya, penyebaran *deepfake* maupun rekayasa konten manipulatif berbasis AI yang dimaksudkan untuk memperdaya khalayak dapat dikategorikan sebagai delik berbasis kesengajaan, selama dapat dibuktikan bahwasanya pelaku menyadari sifat kebohongan serta potensi kerugian yang ditimbulkan oleh konten tersebut. Kendati demikian, kerumitan timbul tatkala pelaku berargumen tidak mengerti mekanisme kerja AI secara utuh atau mengklaim bahwa materi tersebut tergenerasi secara otomatis tanpa iktikad buruk. Kondisi ini mengindikasikan bahwasanya asas kesalahan berada dalam tekanan teoritis akibat samar-samarnya garis pemisah antara niat manusia dan kalkulasi sistemik.

Sifat pertanggungjawaban perorangan (*individual liability*) serta *personal liability* dalam ranah hukum pidana nasional menegaskan bahwasanya setiap individu menanggung akibat hukum atas tindakan yang dieksekusinya secara mandiri, mencakup konsekuensi yang secara masuk akal dapat diantisipasi dari perilaku tersebut.<sup>46</sup>

---

<sup>44</sup> Rr. Dijan Widiyowati, "A Comparative Study Of Principle Of Guilt In The Provision Of Indonesian And English Criminal Law," KRTA BHAYANGKARA 18, no. 3 (2024): 559–68, <https://doi.org/10.31599/krtha.v18i3.3302>.

<sup>45</sup> Didi Jubaidi and Khoirunnisa Khoirunnisa, "CORPORATE CRIMINAL LIABILITY: AN ANALYSIS OF CORPORATE CRIME PERPETRATORS UNDER POSITIVE LAW IN INDONESIA," SSRN Electronic Journal, ahead of print, 2025, <https://doi.org/10.2139/ssrn.5068437>.

<sup>46</sup> Adhryansyah et al., "Elaboration of the Concept of Serious Human Rights Violations in Indonesia: Jus Cogens in the Framework of Corporations Criminal Responsibility," Yuridika 40, no. 2 (2025): 227–52, <https://doi.org/10.20473/ydk.v40i2.60820>.

Dalam konteks disinformasi berbasis AI, asas ini diimplementasikan dengan menempatkan sistem kecerdasan buatan sekadar sebagai peranti, setara dengan komputer atau instrumen lunak lainnya, sehingga tiap luaran yang dihasilkan secara yuridis tetap bermuara pada individu pengoperasinya. Pihak yang mengoperasikan AI guna mencetak atau mendistribusikan narasi bohong tak dapat menjadikan independensi sistem sebagai tameng pelindung, sebab secara yuridis ia bertindak sebagai pemegang kendali utama atas tindakan penyebaran tersebut. Bahkan pada ranah kecerobohan, beban sanksi tetap dapat dibebankan bilamana pemakai alpa menjalankan pemastian keabsahan (*due diligence*) atas muatan AI sebelum melemparnya ke ranah terbuka. Oleh sebab itu, doktrin *personal liability* bertindak sebagai penghubung normatif untuk menambal kekosongan pertanggungjawaban di tengah pesatnya inovasi teknologi. Meskipun demikian, daya guna asas ini kian diragukan tatkala sistem AI bekerja dengan derajat kemandirian tinggi hingga melahirkan luaran yang sama sekali tak terantisipasi oleh pemakainya.

Kerumitan hukum kian memuncak saat pembebanan sanksi terpecah ke dalam berbagai elemen subjek di ekosistem AI, yakni pemakai, perancang sistem, hingga penyedia jejaring digital. Terpecahnya tanggung jawab ini dipicu oleh beragamnya tingkat keterlibatan serta kendali tiap-tiap entitas terhadap mekanisme kerja AI dan luaran yang tercipta. Perancang sistem memikul beban pada fase perancangan, pelatihan instruksi algoritma, serta pemetaan risiko, sedangkan pemakai bertanggung jawab pada tataran operasional dan pemanfaatan muatan, di mana jejaring digital bertindak selaku fasilitator perantara. Dalam kasus fabrikasi hoaks berbasis AI, ketidakjelasan batas penentuan dalang utama (*actor liability*) acap kali memicu kerancuan yuridis dalam praktik penegakan hukum. Petugas penegak hukum kerap menemui jalan buntu untuk mengidentifikasi apakah kekhilafan bersumber dari malfungsi desain, manipulasi pemakai, atau ketiadaan penyaringan oleh penyedia jejaring. Perpecahan peran ini riskan memicu saling lempar kesalahan (*blame shifting*) yang justru mengikis ketegasan hukum serta membuka celah impunitas bagi oknum yang seharusnya bertanggung jawab.

#### 2.2.4 Ketentuan Pidana yang Relevan dengan Hoaks Politik Berbasis AI

Dari perspektif hukum pidana, UU ITE dan KUHP memberikan dasar normatif yang kuat untuk menjerat pelaku penyebaran hoaks. Pasal 28 ayat (1) dan ayat (3) UU ITE, khususnya setelah perubahan melalui UU No. 1 Tahun 2024, menegaskan larangan penyebaran informasi bohong yang berdampak nyata, baik berupa kerugian konsumen maupun kerusakan masyarakat.

Ketentuan tersebut diperkuat dengan ancaman pidana dalam Pasal 45A ayat (3) UU ITE berbunyi

*“Setiap Orang yang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusakan di masyarakat sebagaimana dimaksud dalam Pasal 28 ayat (3) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”*

Pasal a quo mencerminkan keseriusan negara dalam menanggulangi kejahatan informasi. Selain itu, Pasal 390 KUHP yang berbunyi:

*“Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan menyiarkan kabar bohong atau pemberitahuan palsu, membuat harga barang dagangan, dana-dana atau surat berharga menjadi turun atau naik, diancam dengan pidana penjara paling lama dua tahun delapan bulan.”*

### 2.2.5 Tantangan Pembuktian Unsur Kesalahan

Hambatan teknis paling krusial dalam pembuktian kasus disinformasi berbasis AI bersumber dari minimnya kapabilitas forensik digital. Unit pemeriksa digital acap kali kewalahan melacak jejak rekayasa AI yang kian presisi serta miskin artefak eksekusi. Instrumen forensik tradisional kerap tak berdaya menyingkap konten hasil sintesis *generative adversarial networks* maupun teknik *voice cloning*. Kendala ini semakin rumit lantaran kelangkaan tenaga ahli yang menguasai keahlian spesifik di ranah forensik AI. Dampaknya, proses pembuktian hukum berlangsung alot dan tertinggal jauh dari eksponensialnya laju penyebaran berita bohong di ruang siber. Dalam perspektif yuridis, situasi ini mengikis prinsip *due process of law*, sebab kelambatan pembuktian berisiko melumpuhkan efektivitas jaminan perlindungan hukum bagi publik. Di samping keterbatasan forensik, penyamaran identitas pelaku juga merupakan tantangan teknis yang sangat rumit. Oknum penyebar hoaks berbasis AI memanfaatkan sarana VPN, perantara *proxy*, enkripsi *end-to-end*, serta jaringan akun anonim atau *bot* guna mengaburkan jejak keberadaannya.<sup>47</sup> Penggunaan sarana-sarana tersebut menjadikan alur pelacakan oknum pelaku sangat rumit dan berlapis, bahkan tak jarang mustahil untuk dituntaskan dalam tempo singkat. Pada berbagai penanganan perkara, penegak hukum acap kali cuma berhasil meringkus eksekutor lapangan atau penyebar tingkat sekunder, sedangkan dalang intelektual di balik pembuatan konten tetap bebas melenggang. Implikasinya, terjadi ketimpangan penjatuhan sanksi hukum serta memicu ruang kebal hukum (*impunity*). Secara doktrinal, penyamaran identitas ini merusak sendi-sendi prinsip *personal liability* dalam hukum pidana, disebabkan kejelasan identitas individu selaku subjek hukum menjadi serba samar.

Kerumitan kian memuncak saat disinformasi berbasis AI melibatkan mekanisme lintas batas yurisdiksi. Pelaku dapat bermukim di suatu negara, infrastruktur *server* ditempatkan di negara lain, sementara pihak korban berada di bawah kedaulatan hukum yang berbeda. Kondisi ini memicu benturan yurisdiksi yang krusial, mengingat tatanan hukum pidana nasional sejatinya mengusung asas teritorial. Prosedur bantuan hukum timbal balik (*mutual legal assistance/MLA*) yang memakan waktu lama acap kali kalah cepat dibandingkan pergerakan pelaku dalam memusnahkan rekayasa jejak digital. Di samping itu, disparitas standar hukum antarnegara melahirkan asimetri regulasi, di mana suatu perilaku dikategorikan sebagai pelanggaran hukum di sebuah wilayah namun

---

<sup>47</sup> Aga Natalis and Naufal Hasanuddin Djohan, “Cybersex Trafficking: Legal Challenges and Protection for Women and Children in Indonesia,” *International Cybersecurity Law Review* 6, no. 3 (2025): 421–56, <https://doi.org/10.1365/s43439-025-00149-1>.

dianggap sah di wilayah lainnya. Implikasinya, tindakan penegakan hukum menjadi serba terpecah dan meleset dari sasaran. Dalam kacamata doktrinal, fakta ini menegaskan urgensi harmonisasi hukum siber global agar perlindungan entitas masyarakat digital tak terhenti di garis perbatasan negara. Pada tataran aplikatif, petugas penegak hukum masih menjadikan ketetapan hoaks dalam UU ITE serta KUHP sebagai pijakan hukum utama. Pembaruan UU ITE lewat UU Nomor 1 Tahun 2024 mempertegas orientasi penindakan pada hoaks yang memicu keonpratan publik, yang menandai pergeseran fokus dari sebatas materi kebohongan menuju akibat sosial yang ditimbulkannya. Pendekatan berbasis dampak (*impact-based approach*) ini secara yuridis lebih tepat sasaran. Kendati demikian, dalam kasus disinformasi bersumber dari AI, verifikasi atas dampak sosial acap kali sukar dibuktikan, terlebih bila kekacauan yang lahir berwujud psikologis atau gejala di ruang siber. Fenomena ini membuka celah penafsiran yang sangat dinamis bagi aparat serta hakim. Alhasil, sekalipun terjadi penyempurnaan regulasi secara normatif, pengimplementasiannya di lapangan tetap berhadapan dengan hambatan teoritis maupun teknis.<sup>48</sup>

### 2.2.6 Implikasi Hukum terhadap Cyber

Dampak yuridis dari maraknya kejahatan siber (*cybercrime*) di tanah air memegang peranan krusial dalam membendung berbagai potensi kejahatan yang lahir dari eksponensialnya inovasi teknologi digital. Ranah kejahatan digital, yang mencakup penipuan siber, manipulasi data pribadi, hingga pembobolan sistem, sanggup melumpuhkan finansial serta reputasi entitas perorangan, korporasi, sampai lembaga negara, sehingga regulasi hukum hadir guna menjamin kepastian perlindungan publik lewat payung hukum UU ITE yang memetakan jenis-jenis delik terlarang di lanskap siber. Pelanggaran pidana digital, seperti distribusi konten ilegal atau manipulasi dokumen elektronik, diancam dengan hukuman pidana yang mencakup sanksi kurungan hingga pidana denda yang proporsional sesuai gradasi bobot kejahatannya. Kendati demikian, batu sandungan paling berat dalam eksekusi hukum terletak pada karakteristik delik siber yang menembus batas-batas teritorial, di mana acap kali mendatangkan eksekutor dari mancanegara yang menuntut adanya sinergi antarnegara dalam proses penindakannya. Di samping itu, kelangkaan infrastruktur penunjang hukum serta minimnya kuantitas penyidik yang membidangi keahlian forensik siber masih menjadi penghalang nyata, terlebih para eksekutor kerap mengoperasikan peranti canggih guna menyamarkan jejak keberadaan mereka. Atas dasar tersebut, akselerasi kompetensi aparat penegak hukum, penguatan kolaborasi lintas instansi, serta langkah pencegahan melalui sosialisasi dan peningkatan kesadaran publik atas urgensi perlindungan data menjadi kunci utama guna mewujudkan ekosistem siber yang kondusif sekaligus meminimalisasi eskalasi tindak pidana digital di masa mendatang.

---

<sup>48</sup> A. Djoko Sumaryanto et al., "Penerapan Hukum Terhadap Penyebaran Hoaks Berbasis AI (AIGenerated Misinformation)", *Unes Law Review* 8, no.4 (2026): 1449.

## 2.2.7 Kebijakan legislatif

Perumusan regulasi dalam penanganan *cyber crime* merupakan langkah strategis negara guna menyusun serta memperbarui kerangka hukum yang sanggup melandasi penindakan beragam bentuk kejahatan di ranah digital. Akselerasi inovasi teknologi memicu timbulnya modus kejahatan modern yang acap kali tak tersentuh oleh aturan pidana konvensional. Oleh sebab itu, lembaga legislatif dituntut untuk menjamin bahwasanya regulasi tindak pidana siber dirumuskan secara presisi, memetakan batasan delik terlarang, menegaskan batas beban pertanggungjawaban individu, serta mematok sanksi pidana yang sepadan dengan gradasi kesalahan pembuatnya.

## 2.2.8 Kebijakan penegakan hukum

Implementasi penegakan hukum dalam mengatasi *cyber crime* mewujudkan langkah konkret negara untuk mengeksekusi sanksi yuridis terhadap dalang tindak pidana yang memanfaatkan atau menargetkan infrastruktur siber. Penindakan delik siber mengusung karakteristik khusus yang tak sejajar dengan pidana konvensional, lantaran domisili pelaku, posisi korban, hingga keberadaan barang bukti kerap kali tersebar di berbagai wilayah, bahkan melintasi perbatasan antarnegara. Implikasinya, aparat penegak hukum dituntut menguasai kualifikasi teknis dalam memproses perkara berbasis teknologi, mulai dari penelusuran awal, pelacakan identitas eksekutor, pengamanan infrastruktur sistem, hingga ekstraksi dan analisis jejak digital.

Aspek krusial yang menjadi poros dalam penanganan pidana siber terletak pada proses pembuktian hukum. Pada perkara kejahatan digital, rekam pembuktian dapat berwujud lalu lintas pesan elektronik, catatan log aktivitas sistem, deretan alamat IP, manifes dokumen digital, riwayat transaksi siber, hingga berkas tersimpan di dalam perangkat elektronik. Seluruh barang bukti tersebut wajib diperoleh, diisolasi, serta diuji melalui tata cara yang memenuhi standar legalitas agar dapat diakui secara sah di muka persidangan. Mengingat karakter bukti digital yang rentan dimanipulasi atau dimusnahkan secara kilat, penguasaan kapabilitas forensik digital oleh penyidik menjadi pilar vital dalam menopang efektivitas penegakan hukum.

Di samping penguasaan keahlian teknis, efektivitas penindakan kejahatan siber mensyaratkan keterhubungan sinergis antar-aktor, mencakup institusi kepolisian, korps kejaksaan, majelis hakim, pakar informatika, penyedia layanan sistem elektronik, hingga instansi terkait lainnya. Kolaborasi ini krusial mengingat penanganan perkara siber acap kali menuntut spesialisasi khusus serta akses data lintas sektoral yang tak dikuasai secara tunggal oleh satu lembaga. Pada skenario di mana eksekutor atau lokasi *server* berada di luar yurisdiksi Indonesia, mekanisme kerja sama internasional menjadi instrumen wajib guna menghimpun data serta memperlancar tahapan penegakan hukum.

## 2.2.9 Kebijakan pencegahan

Strategi preventif dalam menanggulangi tindak pidana siber merupakan langkah proaktif guna meminimalisasi potensi lahirnya kejahatan di alam siber sebelum mendatangkan dampak kerugian bagi publik. Upaya pencegahan tak sebatas bersandar

pada penetapan regulasi dan eksekusi sanksi atas para pelanggar, melainkan juga bertumpu pada penguatan kesadaran publik terkait urgensi keselamatan bertransaksi teknologi. Khalayak luas perlu dibekali pemahaman mendalam mengenai tata cara memproteksi privasi data, mendeteksi indikasi penipuan siber, menerapkan kombinasi kata sandi yang tangguh, mengamankan akses akun, serta bersikap cermat saat membagikan informasi di jagat maya. Melalui akselerasi pemahaman literasi digital, publik diharapkan lebih sigap mengenali sekaligus membentengi diri dari aneka ancaman kejahatan siber.

Di samping itu, tindakan pencegahan wajib direalisasikan lewat penguatan benteng pertahanan pada sistem elektronik milik instansi pemerintah, entitas bisnis, hingga penyedia layanan digital. Setiap infrastruktur siber harus disokong instrumen keamanan yang mumpuni demi memblokir peretasan tanpa hak, insiden kebocoran data, pencurian informasi sensitif, hingga kerusakan operasional sistem. Pengelola platform juga dituntut untuk mengeksekusi pembaruan keamanan secara berkala, mengawasi gerak-gerik lalu lintas data yang mencurigakan, serta menyiagakan skema mitigasi darurat tatkala serangan siber menerjang. Langkah antisipatif ini teramat vital mengingat celah kerentanan pada sistem digital acap kali menjelma menjadi pintu masuk yang dimanfaatkan oleh para pelaku kejahatan.

Pada ranah yang sama, negara memegang peranan sentral dalam merancang ekosistem digital yang kondusif melalui program edukasi, sosialisasi intensif, pengawasan terpadu, serta penguatan sinergi lintas sektoral. Langkah pencegahan dapat diwujudkan lewat edukasi literasi digital secara masif kepada masyarakat, khususnya mengenai proteksi kerahasiaan data serta tata cara berinteraksi di media sosial secara bijak dan bertanggung jawab. Kerangka kerja ini perlu dipadukan dengan kemitraan erat antara otoritas pemerintah, korps penegak hukum, institusi pendidikan, pelaku industri swasta, hingga elemen masyarakat agar pembentukan benteng kejahatan siber tidak hanya ditumpukan pada satu instansi saja.

Oleh sebab itu, perumusan kebijakan preventif terhadap kejahatan siber harus dieksekusi secara holistik dan berkesinambungan. Penanggulangan dini tidak akan berjalan optimal apabila sekadar mengandalkan wawasan masyarakat atau kecanggihan sistem keamanan semata, melainkan membutuhkan integrasi harmonis antarelemen tersebut.

## KESIMPULAN

Berdasarkan hasil penelitian, penyebaran hoaks politik berbasis AI dapat terjadi dalam dua bentuk utama, yaitu human error dan intentional misuse. Human error lebih banyak berkaitan dengan ketidaktahuan, kelalaian, rendahnya literasi digital, serta tindakan membagikan informasi tanpa melakukan pemeriksaan terlebih dahulu. Sementara itu, intentional misuse dilakukan secara sadar dan terencana dengan memanfaatkan AI untuk membuat atau menyebarkan informasi palsu, seperti deepfake, audio palsu, gambar sintetis, maupun narasi yang dibuat untuk memengaruhi opini publik

atau merugikan pihak tertentu. Perbedaan keduanya terletak pada unsur kesalahan dan kesengajaan yang dimiliki oleh pelaku.

Dari perspektif kriminologi, penyebaran hoaks politik berbasis AI dapat dipahami melalui routine activity theory dan rational choice theory. AI membuat pembuatan konten palsu menjadi lebih mudah, cepat, murah, dan memiliki jangkauan yang luas. Kondisi tersebut semakin memungkinkan terjadinya kejahatan ketika terdapat pelaku yang memiliki motivasi, target yang mudah dipengaruhi, serta pengawasan yang belum memadai. Di sisi lain, pelaku juga dapat mempertimbangkan keuntungan yang diperoleh dengan risiko yang mungkin diterima.

Dalam hukum pidana Indonesia, penggunaan AI tidak menghilangkan pertanggungjawaban pidana manusia yang berada di balik penggunaan teknologi tersebut. AI pada dasarnya hanya menjadi alat, sehingga yang perlu dibuktikan adalah peran, pengetahuan, kehendak, serta kesalahan dari orang yang membuat atau menyebarkan konten tersebut. UU ITE dan KUHP telah dapat digunakan sebagai dasar hukum dalam menangani beberapa bentuk penyebaran informasi palsu, tetapi perkembangan AI menimbulkan persoalan baru, terutama dalam membuktikan unsur kesengajaan, menemukan identitas pelaku, memperoleh bukti digital, serta menentukan pihak yang harus bertanggung jawab ketika terdapat banyak pihak yang terlibat.

Dengan demikian, persoalan hoaks politik berbasis AI tidak cukup ditangani hanya melalui pemberian sanksi pidana. Penanganannya juga membutuhkan peningkatan kemampuan forensik digital, penguatan kerja sama antarpenghak hukum dan penyedia platform, pembaruan kebijakan yang mengikuti perkembangan teknologi, serta peningkatan literasi digital masyarakat. Pendekatan tersebut diperlukan agar perkembangan teknologi AI tetap dapat dimanfaatkan secara positif tanpa mengabaikan perlindungan hukum dan kepentingan masyarakat.

## SARAN

Berdasarkan hasil penelitian, pemerintah perlu terus melakukan pembaruan dan penyempurnaan regulasi yang berkaitan dengan penggunaan AI, khususnya untuk menghadapi penyebaran deepfake dan hoaks dalam konteks politik. Pengaturan yang lebih jelas diperlukan agar batas antara penggunaan AI yang sah, human error, dan intentional misuse dapat lebih mudah dibedakan dalam proses penegakan hukum.

Aparat penegak hukum juga perlu meningkatkan kemampuan dalam bidang forensik digital dan penelusuran kejahatan berbasis AI. Hal ini penting karena pelaku dapat menggunakan akun anonim, bot, maupun teknologi lain untuk menyamarkan identitas dan menghilangkan jejak digital. Kerja sama antara kepolisian, kejaksaan, lembaga penyelenggara pemilu, ahli teknologi, dan penyedia platform digital juga perlu diperkuat agar penanganan kasus dapat dilakukan secara lebih cepat dan tepat.

Selain penegakan hukum, upaya pencegahan juga perlu mendapat perhatian. Masyarakat perlu diberikan edukasi mengenai cara mengenali konten hasil manipulasi AI dan pentingnya melakukan verifikasi sebelum membagikan informasi, terutama informasi

yang berkaitan dengan politik. Dengan peningkatan literasi digital dan kesadaran hukum, masyarakat diharapkan tidak mudah menjadi penyebar hoaks secara tidak sengaja.

Bagi penelitian selanjutnya, pembahasan mengenai hoaks politik berbasis AI dapat dikembangkan melalui penelitian empiris dengan melihat secara langsung pola penyebaran konten, kemampuan aparat dalam melakukan pembuktian digital, serta perkembangan kasus-kasus yang terjadi di Indonesia. Dengan demikian, penelitian mengenai pertanggungjawaban pidana dalam penggunaan AI dapat terus menyesuaikan diri dengan perkembangan teknologi dan praktik di lapangan.

## DAFTAR PUSTAKA

### Buku:

- Ariman, M. Rasyid, dan Fahmi Raghieb. *Hukum Pidana*. Malang: Setara Press, 2015.
- Cornish, Derek B., dan Ronald V. Clarke, eds. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag, 1986.
- Ibrahim, Johnny. *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia Publishing, 2006.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2014.
- Pane, Musa Darwin. *Pengganti Kerugian Negara dalam Tindak Pidana Korupsi: Alternatif Pengganti Pidana Penjara dan Pidana Mati dalam Perspektif Pemberantasan Korupsi*. Bandung: Logos Publishing, 2017.
- Saleh, Roeslan. *Perbuatan Pidana dan Pertanggungjawaban Pidana: Dua Pengertian Dasar dalam Hukum Pidana*. Cetakan ke-3. Jakarta: Aksara Baru, 1983.
- Soekanto, Soerjono, dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, 2011.

### Jurnal dan Artikel Ilmiah:

- Adhryansyah, et al. "Elaboration of the Concept of Serious Human Rights Violations in Indonesia: Jus Cogens in the Framework of Corporations Criminal Responsibility." *Yuridika* 40, no. 2 (2025): 227-252. <https://doi.org/10.20473/ydk.v40i2.60820>.
- Cohen, Lawrence E., dan Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44, no. 4 (1979): 588-608.
- Jubaidi, Didi, dan Khoirunnisa Khoirunnisa. "Corporate Criminal Liability: An Analysis of Corporate Crime Perpetrators under Positive Law in Indonesia." *SSRN Electronic Journal* (2025). <https://doi.org/10.2139/ssrn.5068437>.

- Muhtadi, Burhanuddin, dan Maria Monica Wihardja. "Deepfakes and Selective Belief: How Partisanship Affects Voters' Exposure and Susceptibility to Deepfake Content." *ISEAS Perspective*, no. 58 (2024): 2-3.
- Natalis, Aga, dan Naufal Hasanuddin Djohan. "Cybersex Trafficking: Legal Challenges and Protection for Women and Children in Indonesia." *International Cybersecurity Law Review* 6, no. 3 (2025): 421-456. <https://doi.org/10.1365/s43439-025-00149-1>.
- Rosadi, Sinta Dewi. "The Use of AI and Social Media for 'Black Campaign' in Indonesia." Yale Law School, 2024.
- Sumaryanto, A. Djoko, et al. "Penerapan Hukum Terhadap Penyebaran Hoaks Berbasis AI (AI-Generated Misinformation)." *Unes Law Review* 8, no. 4 (2026): 1449.
- Widijowati, Rr. Dijan. "A Comparative Study of Principle of Guilt in the Provision of Indonesian and English Criminal Law." *KRTHA BHAYANGKARA* 18, no. 3 (2024): 559-568. <https://doi.org/10.31599/krtha.v18i3.3302>.

#### Peraturan Perundang-Undangan:

- Indonesia. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.
- Indonesia. *Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum*.
- Indonesia. *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.
- Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.

#### Laporan, Dokumen, dan Sumber Lembaga:

- ANFREL. *Elections and Technology Reader*. Juli-Agustus 2024.
- Badan Pembinaan Hukum Nasional. "Jaringan Dokumentasi Informasi Hukum." Diakses 22 September 2026. <https://jdih.setneg.go.id>.
- Badan Pengawas Pemilihan Umum. "Bawaslu Tekankan Urgensi Pengaturan AI dalam Pemilu." 4 September 2026. <https://jatim.antaranews.com/berita/994453/bawaslu-tekanan-urgensipengaturan-ai-dalam-pemilu>.
- Kementerian Komunikasi dan Digital Republik Indonesia. *Kajian Pemanfaatan Kecerdasan Artifisial dalam Komunikasi Pemerintah*. Jakarta: Direktorat Jenderal Komunikasi Publik dan Media, tanpa tahun.
- Komisi Pemilihan Umum Republik Indonesia. "Tantangan Integritas Pemilu di Tengah Kemajuan Artificial Intelligence." 17 Mei 2026.

<https://www.kpu.go.id/berita/baca/13661/tantangan-integritas-pemilu-di-tengah-kemajuan-artificial-intelligence>.

MAFINDO. “Siaran Pers: Hoaks Politik Meningkatkan Tajam Jelang Pemilu 2024.” 2 Februari 2024.

<https://mafindo.or.id/2024/02/02/siaran-pers-mafindo-hoaks-politik-meningkat-tajam-jelang-pemilu-2024-ganggu-demokrasi-indonesia/>.

Tempo. “CekFakta #271: Membaca Penyebab Kecenderungan Percaya Hoaks dan Deepfake saat Pemilu.” 2 Agustus 2024. <https://www.tempo.co/newsletter/cekfakta-271-membaca-penyebab-kecenderungan-percaya-hoaks-dan-deepfake-saat-pemilu-32439>.

Tempo. “CekFakta #299: Ketika Disinformasi AI Mengintai.” 14 Februari 2025.

<https://www.tempo.co/newsletter/cekfakta-299-ketika-disinformasi-ai-mengintai-kilas-balik-cek-fakta-2024-1206902>.