

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Kehadiran *artificial intelligence* (yang selanjutnya disebut AI) atau kecerdasan buatan dalam kemajuan teknologi tidak terlepas dari pengaruh dan keterkaitannya dengan peraturan hukum yang berlaku di suatu negara.¹ Salah satu cabang dalam teknologi AI yang menarik perhatian adalah *deepfake*. Teknologi *deepfake* memanfaatkan algoritma canggih dan pembelajaran mesin untuk menghasilkan konten digital yang sangat mirip dengan aslinya, sehingga dapat membuka peluang baru dalam bidang kreativitas, seperti pembuatan film maupun media edukasi.² Namun kini menimbulkan kekhawatiran yang serius karena rawan disalahgunakan.

Seiring dengan meningkatnya akses terhadap teknologi *deepfake*, berbagai aplikasi berbasis AI untuk merekayasa suara banyak beredar di publik, bahkan dalam versi gratis. Beberapa aplikasi *deepfake* yang dapat diakses secara gratis diantaranya yaitu Lensa AI, Deepfakes web, Wombo, Reface, MyHeritage, DeepFaceLab, Deep Art, Face Swap Live, FaceApp, Jiggy, FaceMagic, dan

¹ Muhammad Tan Abdul Rahman Haris dan Tantimin, "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence di Indonesia," *Jurnal Komunikasi Hukum (JKH)*, No. 1, Vol. 8, Program Studi Ilmu Hukum Universitas Pendidikan Ganesha, 2022, hlm. 309.

² Eko Putra Boediman, "Exploring the Impact of Deepfake Technology on Public Trust and Media Manipulation: A Scoping Review," *Jurnal Komunikasi*, No. 2, Vol. 19, Program Studi Ilmu Komunikasi Universitas Islam Indonesia, 2025, hlm. 314.

DALL-E Mini.³ Aplikasi ini memungkinkan pengguna mengedit dan mengganti wajah antar individu untuk menghasilkan foto atau video manipulatif.

Perangkat lunak seperti PlayHT, Listnr, Murf.AI, LOVO, Veed, ElevenLab menyediakan layanan sintesis suara yang mampu menghasilkan audio sangat mirip suara manusia dan mendukung berbagai bahasa, termasuk Bahasa Indonesia.⁴ Hal ini memungkinkan siapa pun, bahkan tanpa keahlian teknologi informasi, dapat membuat rekaman suara yang terdengar asli, sehingga berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab.

Bentuk penyalahgunaan yang meningkat yakni dalam modus *voice phishing* atau *vishing*, yaitu kejahatan rekayasa sosial menggunakan suara untuk memanipulasi korban agar memberikan data pribadi. Kejahatan ini sulit dideteksi karena pelaku memanfaatkan AI untuk meniru pola bicara.⁵ Pelaku kini memanfaatkan *deepfake* untuk berpura-pura menjadi pejabat publik, pegawai bank, atasan kantor, atau keluarga korban demi menipu melalui rekayasa teknologi. Fenomena ini menjadi bukti bahwa kejahatan siber telah mengalami transformasi yang sangat canggih dan kompleks.

³ Teddy Tri Seto Berty, *12 Aplikasi Deepfake yang Bisa Diakses Secara Gratis*, terdapat dalam <https://www.liputan6.com/global/read/5233909/12-aplikasi-deepfake-yang-bisa-diakses-secara-gratis>, diakses tanggal 18 November 2025, pukul 04.48.

⁴ Abigail Lewis, *6 Software Kloning Suara AI Terbaik (2025)*, terdapat dalam <https://www.guru99.com/id/best-ai-voice-cloning-software.html>, diakses tanggal 20 November 2025, pukul 23.57.

⁵ Ulfa Ladayya et al., “Kesadaran Keamanan Informasi atas Phishing, Smishing, dan Vishing pada Warga Kota Cimahi,” *Nuansa Informatika*, No. 2, Vol. 18, Fakultas Ilmu Komputer Universitas Kuningan, 2024, hlm. 116-117.

Kasus penipuan berbasis *deepfake* dilakukan oleh pelaku berinisial AMA (29 tahun) dengan memalsukan foto dan suara Presiden Prabowo Subianto, Wakil Presiden Gibran Rakabuming Raka, dan Menteri Keuangan Sri Mulyani melalui video palsu pengumuman bantuan keuangan, lalu mengarahkan korban untuk menghubungi nomor WhatsApp tertentu guna menjebak agar mentransfer uang. AMA ditangkap di Lampung Tengah pada 16 Januari 2025, setelah meraup sekitar Rp30.000.000,- (tiga puluh juta rupiah) dari 11 (sebelas) korban. AMA dijerat Pasal 51 ayat (1) *junc to* Pasal 35 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (yang selanjutnya disebut UU ITE) serta Pasal 378 Kitab Undang-Undang Hukum Pidana (yang selanjutnya disebut KUHP).⁶ Selain itu, modus *voice phishing* juga muncul dengan identitas palsu sebagai layanan pelanggan untuk meminta verifikasi data pribadi. Kasus ini menegaskan bahwa penipuan suara berbasis AI merupakan fenomena yang terus berkembang dan memerlukan kewaspadaan tinggi.⁷

Menurut laporan *National Cyber Security Index*, pada tahun 2023 Indonesia memperoleh skor 63,64 (enam puluh tiga koma enam puluh empat) dari

⁶ Devira Prastiwi, 5 Fakta Terkait Polisi Tangkap Pelaku Penipuan AI Deepfake, Catut Nama Prabowo, Gibran, hingga Sri Mulyani, terdapat dalam <https://www.liputan6.com/news/read/5896373/5-fakta-terkait-polisi-tangkap-pelaku-penipuan-ai-deepfake-catut-nama-prabowo-gibran-hingga-sri-mulyani>, diakses tanggal 28 Oktober 2025, pukul 21.45.

⁷ Dinda Charmelita Trias Maharani, Ramai Modus Penipuan Voice Phishing dengan Suara Robot ala Customer Service, Ini Penjelasan Pengamat Siber, terdapat dalam <https://www.liputan6.com/tekno/read/5283341/ramai-modus-penipuan-voice-phishing-dengan-suara-robot-ala-customer-service-ini-penjelasan-pengamat-siber>, diakses tanggal 28 Oktober 2025, pukul 22.16.

100 (seratus) dalam indeks keamanan siber. Skor ini menempatkan Indonesia sebagai peringkat ke-49 (empat puluh sembilan) dari 176 (seratus tujuh puluh enam) negara dan menduduki peringkat 10 (sepuluh) paling bawah diantara negara G20 lain.⁸ Seiring dengan kemajuan teknologi komputer yang berhasil menggabungkan berbagai bentuk teknologi digital dan media elektronik menjadi satu kesatuan yang dikenal sebagai "telematika" (gabungan dari telekomunikasi, media, dan informatika), ruang maya atau *cyberspace* pun menjadi semakin luas penggunaannya. Perkembangan ini turut memicu munculnya jenis kejahatan baru yang disebut sebagai kejahatan siber (*cyber crime*), selain itu juga sering disebut sebagai kejahatan mayantara atau kejahatan telematika.⁹

Terjadinya *cyber crime* dipicu oleh berbagai faktor yang saling berkaitan, seperti kurangnya edukasi dan pengawasan, kesenjangan sosial, ketergantungan pada internet, dorongan untuk mendapatkan pengakuan sosial, kelalaian dalam menjaga data pribadi, serta mudahnya akses internet tanpa batas ruang dan waktu.¹⁰ Meskipun keberadaan AI tercantum dalam UU ITE, hingga kini Indonesia masih belum terdapat aturan yang secara khusus dan rinci mengatur penggunaan AI. Ketentuan yang berlaku saat ini hanya mencakup peran AI sebagai

⁸ Chella Defa Anjelina dan Mahardini Nur Afifah, *Menilik Peringkat Keamanan Siber Indonesia Usai PDN, Inafis, Bais, Kemenhub Kebobolan*, terdapat dalam <https://www.kompas.com/tren/read/2024/06/26/120000865/menilik-peringkat-keamanan-siber-indonesia-usai-pdn-inafis-bais-kemenhub>, diakses tanggal 21 November 2025, pukul 02.44.

⁹ Al Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika*, Ctk. Pertama, Universitas Atma Jaya, Yogyakarta, 2010, e-book, hlm. 1-6.

¹⁰ Maskun et al., *Cyber Law: Kebijakan di Era Transformasi Digital*, Ctk. Pertama, Refika Aditama, Bandung, 2024, e-book, hlm. 67.

entitas digital, yaitu alat yang dibuat untuk secara otomatis melakukan tindakan terhadap data elektronik.¹¹ KUHP sebagai dasar utama hukum pidana Indonesia juga belum memiliki ketentuan yang mampu menjangkau kejahatan berbasis teknologi AI. Hal ini menimbulkan ketidakpastian hukum dalam penegakan hukum terhadap pelaku *voice phishing* berbasis *deepfake*.

Voice phishing yang melibatkan rekayasa suara seseorang juga menimbulkan isu serius terkait perlindungan data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (yang selanjutnya disebut UU PDP) telah memberikan jaminan terhadap hak-hak subjek data, salah satunya tercantum dalam Pasal 4 ayat (2) huruf b, yang menyatakan bahwa setiap individu berhak atas kerahasiaan data pribadinya, termasuk data pribadi yang bersifat spesifik yakni data biometrik. Suara dan raut wajah termasuk kategori data biometrik.¹² Rekayasa suara atau wajah tanpa izin merupakan bentuk pelanggaran terhadap hak tersebut dan dapat menimbulkan kerugian materiil maupun immateriil.

Pengaturan hukum terhadap *voice phishing* berbasis AI menjadi penting untuk memastikan bahwa tindakan tersebut dapat dikenai sanksi pidana secara tepat dan adil. Pengaturan hukum tersebut harus mempertimbangkan aspek niat

¹¹ Meirza Aulia Chairani et al., “Urgensi Pengaturan Hukum bagi Penyalahgunaan Aplikasi Deepfake,” *Jurnal Rechtsens*, No. 1, Vol. 13, Fakultas Hukum Universitas Islam Jember, 2024, hlm. 84-85.

¹² Annisa, *Apa itu Biometrik*, terdapat dalam <https://fikti.umsu.ac.id/apa-itu-biometrik/>, diakses tanggal 10 Maret 2026, pukul 15.03.

jahat (*mens rea*), perbuatan (*actus reus*), dan keterkaitan antara penggunaan teknologi *deepfake* dengan terwujudnya kerugian terhadap korban. Pengaturan hukum ini menjadi kebutuhan mendesak di era digital untuk mencegah penyalahgunaan teknologi.

Penelitian ini menjadi penting untuk memahami modus operandi dan pengaturan hukum pidana tindak pidana siber melalui *voice phishing* berbasis AI. Selain itu, penelitian ini diharapkan dapat memberikan rekomendasi terhadap rekonstruksi Hukum Pidana Indonesia agar mampu mengantisipasi perkembangan kejahatan siber yang semakin kompleks dan berbasis teknologi tinggi. Negara harus hadir untuk merespons potensi bahaya dari teknologi *deepfake*.

B. Rumusan Masalah

Merujuk pada uraian latar belakang yang telah dijelaskan di atas, maka permasalahan yang menjadi fokus dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana modus operandi tindak pidana siber yang dilakukan melalui *voice phishing* berbasis *artificial intelligence*?
2. Bagaimana pengaturan hukum pidana terhadap tindak pidana siber yang dilakukan melalui *voice phishing* berbasis *artificial intelligence* di Indonesia?

C. Tujuan Penelitian

Berdasarkan rumusan permasalahan di atas. Adapun tujuan penelitian ini dilakukan yakni sebagai berikut:

1. Untuk menganalisis modus operandi tindak pidana siber yang dilakukan melalui *voice phishing* berbasis *artificial intelligence*.
2. Untuk menganalisis pengaturan hukum pidana terhadap tindak pidana siber yang dilakukan melalui *voice phishing* berbasis *artificial intelligence* di Indonesia.

D. Orisinalitas Penelitian

Penelitian ini memiliki kemiripan topik dengan penelitian lain yang telah dilakukan untuk membahas mengenai *voice phishing* berbasis AI yaitu sebagai berikut:

No.	Detail Karya Ilmiah	Temuan	Perbedaan
1.	Ist'na Rizqi Alamsyah dan Arief Rahman Yusuf, <i>Vishing Sebagai Ancaman Rekayasa Sosial: Analisis Teknik, Dampak, dan Upaya Perlindungan Pengguna, Jurnal Multidisiplin Teknik,</i>	Jurnal ini mengkaji teknik <i>vishing</i> klasik dan modern, dampak terhadap individu dan organisasi, serta strategi perlindungan pengguna. Penelitian ini menyatukan perspektif teknis, psikologis, edukatif,	Penelitian ini menghadirkan kebaruan dengan menganalisis modus operandi dan pengaturan hukum pidana terhadap <i>voice phishing</i> sebagai penipuan siber berbasis AI. Penulis menyoroti bahwa <i>voice phishing</i> belum diatur

	<i>Sains, Pendidikan dan Teknologi</i> , Nomor 2, Volume 2, Juli 2025.	dan regulatif.	secara eksplisit dalam peraturan perundang-undangan Indonesia.
2.	Patricia Morisa Banfatin, Karolus Kopong Medan, dan Debi F.Ng. Fallo, Pengaturan Hukum Pidana di Indonesia Terhadap Penyalahgunaan Teknologi <i>Artificial Intelligence Deepfake</i> dalam Melakukan Tindak Pidana <i>Cyber Crime</i> , <i>Pemuliaan Keadilan</i> , Nomor 1, Volume 2, Januari 2025.	Jurnal ini membahas mengenai beberapa pasal dalam KUHP dan UU ITE yang dapat mengatur penyalahgunaan <i>deepfake</i> dalam <i>cyber crime</i> .	Penelitian ini lebih khusus mengangkat penggunaan AI dalam <i>voice phishing</i> sebagai modus operandi tindak pidana siber melalui manipulasi suara. Selain itu, penelitian ini tidak hanya menyoroti ketentuan dalam KUHP dan UU ITE, namun juga menganalisis UU PDP yang dikaitkan dengan perlindungan data pribadi korban <i>voice phishing</i> .
3.	Alya Alviani dan	Jurnal ini membahas	Fokus utama penelitian

	<p>Yenny Fitri Z., Pengaturan Hukum Tindak Pidana terhadap Penyalahgunaan Teknologi AI (<i>Artificial Intelligence</i>) dalam Penipuan Suara (<i>Voice Phishing</i>) melalui Telepon Seluler, <i>Jurnal Hukum De'Rechtsstaat</i>, Issue 2, Volume 10, September 2024.</p>	<p>pengaturan hukum positif di Indonesia terhadap penyalahgunaan AI dalam penipuan suara melalui telepon seluler, dengan menitikberatkan pada ketentuan dalam UU ITE, KUHP, dan perlindungan terhadap korban.</p>	<p>ini yaitu pada modus operandi dan pengaturan hukum pidana <i>voice phishing</i> berbasis AI sebagai bentuk penipuan. Kebaruan lainnya adalah pembahasan mengenai perlindungan data pribadi korban dengan mengkaji UU PDP, mengingat rekayasa suara sebagai bagian dari data biometrik termasuk ke dalam kategori data pribadi yang dilindungi.</p>
4.	<p>Maulida Diah Laurentina, Modus Operandi Tindak Pidana <i>Phishing</i> dan Pertanggungjawaban</p>	<p>Skripsi ini meneliti modus operandi dan pertanggungjawaban pelaku tindak pidana <i>phishing</i> di Surabaya</p>	<p>Penulis mengangkat isu yang lebih kompleks yakni kejahatan berupa <i>voice phishing</i> berbasis AI dalam tindak pidana</p>

	Pidana terhadap Pelaku Tindak Pidana <i>Phishing</i> di Surabaya (Studi Putusan Pengadilan), <i>Skripsi</i> <i>Universitas Islam</i> <i>Indonesia</i> , 2022.	dengan menganalisis putusan pengadilan di Surabaya.	siber. Penelitian ini menyoroti pengaturan hukum pidana terhadap <i>voice phishing</i> yang belum diatur secara eksplisit dalam UU ITE maupun KUHP.
--	---	---	---

E. Tinjauan Pustaka

1. *Voice Phishing* berbasis AI

Voice phishing atau *vishing* sering disebut sebagai penipuan melalui telepon, yakni metode kejahatan di mana pelaku berpura-pura menjadi pihak yang dipercaya korban untuk mengelabui dan memperoleh informasi atau keuntungan tertentu. Perkembangan teknologi membuat modus ini semakin canggih dengan menggunakan rekayasa suara *deepfake* dan kloning suara berbasis AI agar terdengar asli.¹³ *Deepfake* merupakan salah satu turunan dari AI.

Istilah *deepfake* berasal dari gabungan dua kata dalam bahasa Inggris, yaitu “*deep learning*” dan “*fake*”. *Deep learning* merupakan teknologi yang menjadi dasar terciptanya perangkat lunak pembentuk *deepfake*, sedangkan

¹³ Alya Alviani dan Yenny Fitri.Z, “Legal Regulations on Criminal Acts Against Misuse of AI (Artificial Intelligence) Technology in Voice Phishing Fraud Via Mobile Phones,” *Jurnal Hukum De'rechtsstaat*, No. 2, Vol. 10, Fakultas Hukum Universitas Djuanda Bogor, 2024, hlm. 210.

kata “fake” menggambarkan hasil akhirnya berupa konten palsu yang tidak bersifat asli.¹⁴ Teknologi ini telah menarik perhatian luas dari masyarakat karena kemampuannya dalam menghasilkan video, gambar, dan audio yang menyerupai individu tertentu, sehingga menampilkan seolah-olah orang tersebut melakukan tindakan yang sebenarnya tidak pernah mereka lakukan.¹⁵

Penipuan suara berbasis AI memanfaatkan kemampuan kecerdasan buatan untuk menghasilkan tiruan suara seseorang. Melalui algoritme pembelajaran mendalam, sistem dapat menyalin karakteristik vokal dengan mudah sehingga panggilan palsu seolah-olah terdengar berasal dari individu yang asli.¹⁶ Hingga saat ini, Indonesia belum menetapkan aturan yang secara eksplisit mengatur penggunaan maupun pertanggungjawaban hukum atas teknologi AI. Kekosongan regulasi tersebut berpotensi menimbulkan persoalan hukum di kemudian hari, terutama jika teknologi AI dimanfaatkan untuk melakukan perbuatan yang bertentangan dengan ketentuan hukum positif yang berlaku.

2. Tindak Pidana Siber

Berdasarkan pengelompokannya, KUHP membagi tindak pidana ke dalam dua kategori, yakni kejahatan (*misdrifven*) dan pelanggaran

¹⁴ Chiquita Thefirstly Noerman dan Aji Lukman Ibrahim, “Kriminalisasi Deepfake di Indonesia Sebagai Bentuk Pelindungan Negara,” *Jurnal Usm Law Review*, No. 2, Vol. 7, Magister Hukum Universitas Semarang, 2024, hlm. 604.

¹⁵ Rendi Syaputra Nur Haida dan Eko Nuriyatman, “Urgensi Pengaturan Perlindungan Hukum terhadap Korban Deepfake Melalui Artificial Intelligence (AI) dari Perspektif Hukum Pidana Indonesia,” *Jurnal Hukum Respublica*, No. 1, Vol. 24, Universitas Lancang Kuning, 2024, hlm. 4.

¹⁶ Alya Alviani dan Yenny Fitri.Z, *Loc. Cit.*

(*overtredingen*).¹⁷ Dengan berkembangnya teknologi informasi dan komunikasi secara cepat, kejahatan siber kini menjadi ancaman serius yang berdampak luas terhadap keamanan pribadi, institusi bisnis, hingga stabilitas negara. Kejahatan siber disebut sebagai *cyber crime*.¹⁸

Menurut Interpol (2022), kejahatan siber merupakan bentuk tindak kriminal yang dilakukan melalui jaringan komputer, internet, atau perangkat digital lainnya dengan tujuan mencuri, menipu, merusak, atau menghambat sistem informasi milik individu maupun organisasi. Ruang lingkup kejahatan ini sangat luas, mencakup penipuan daring, peretasan, pencurian identitas digital, distribusi *malware*, hingga serangan yang menargetkan infrastruktur digital yang bersifat kritis.¹⁹

Cyber crime merupakan bentuk kejahatan yang memiliki beberapa unsur pokok. Pertama, tindakan yang dilakukan bertentangan dengan hukum, melanggar etika, serta dilakukan tanpa izin atau kewenangan yang sah. Kedua, kejahatan ini memanfaatkan teknologi canggih, khususnya perangkat digital. Ketiga, teknologi informasi dan komputer dapat berperan sebagai sasaran maupun sebagai alat untuk melakukan tindak kejahatan tersebut. Keempat,

¹⁷ Firdaus Renuat et al., *Pengantar Hukum Pidana*, Ctk. Pertama, Gita Lentera, Padang, 2023, e-book, hlm. 19.

¹⁸ Maskun et al., *Op. Cit.* hlm. 45-46.

¹⁹ Kiki Kristanto dan Rakhmat Baihaki, *Tindak Pidana Siber: Regulasi, Tantangan, dan Penegakan Hukum*, Ctk. Pertama, Media Penerbit Indonesia, Medan, 2025, e-book, hlm. 2.

seluruh aktivitas ini terjadi di ruang siber (*cyberspace*), yakni lingkungan virtual yang terbentuk melalui jaringan digital dan internet.²⁰

Adapun bentuk-bentuk *cyber crime* yakni sebaga berikut:²¹

- a. *Cyber Stalking.*
- b. *Cyber Squatting.*
- c. *Data Diddling.*
- d. *Cyber Defamation.*
- e. *Trojan Attack.*
- f. *Cyber Forgery.*
- g. *Financial Cyber Crimes.*
- h. *Internet Time Theft.*
- i. *Worm Virus.*
- j. *Cross-Site Scripting.*
- k. *Ransomware.*
- l. *Salami Attack.*
- m. *Web Jacking.*
- n. *Cyber Terrorism.*
- o. *Cyber Porn.*
- p. *Phishing Attack.*



²⁰ Aroma Elmina Martha, *Dimensi Kejahatan Teknologi Informasi Kontemporer*, Laksbang Pustaka, Yogyakarta, 2022, hlm. 6-7.

²¹ Budi Agus Riswandi dan Alif Muhammad Gultom, *Cyber Crime, Cyber Law, dan Cyber Profession*, Ctk. Pertama, Rajawali Pers, Depok, 2023, hlm. 52-66.

- q. Berita Bohong (*Hoax*).
- r. *Potentially Unwanted Program* (PUPs).
- s. *SIM Swap*.
- t. *Distributed denial of Service* (DDoS).

Tindak pidana siber kerap disebut dengan istilah “*old wine in a new bottle*” dan “*new wine in new bottles*”. Istilah “*old wine*” merujuk pada kejahatan konvensional seperti pencurian, pemerasan, dan penghinaan yang kini terjadi di ruang digital, karena jenis kejahatan tersebut sudah lazim terjadi sebelumnya. Sementara itu, “*new wine*” menggambarkan kejahatan baru seperti *malware* yang muncul seiring dengan perkembangan teknologi. Kejahatan siber memiliki ciri khas tersendiri karena dilakukan dengan memanfaatkan teknologi informasi dan komunikasi sebagai alat utama. Selain itu, kejahatan ini tidak terjadi di ruang fisik yang dapat disentuh, melainkan berlangsung di ruang digital (siber) yang tersambung melalui jaringan perangkat teknologi informasi dan komunikasi.²²

3. Pengaturan dalam UU ITE

UU ITE mengatur berbagai perbuatan yang tergolong sebagai tindak pidana di bidang informasi dan transaksi elektronik di Indonesia. Tujuan dari diterbitkannya undang-undang ini adalah sebagai bentuk perlindungan bagi masyarakat terhadap kejahatan di dunia digital, sekaligus mencegah

²² Wenggedes Frensh, “Penanggulangan Tindak Pidana Siber dengan Menggunakan Teori Jendela Pecah,” *Doktrina: Journal of Law*, No. 2, Vol. 4, Universitas Medan Area, 2021, hlm. 161.

masyarakat agar tidak terlibat dalam sisi negatif dari penggunaan teknologi elektronik, termasuk dalam konteks tindak pidana siber.

Dalam konsideran Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dijelaskan bahwa pembangunan nasional Indonesia, sejak era orde baru hingga sekarang merupakan proses berkelanjutan yang harus responsif terhadap berbagai perubahan dalam masyarakat. Perkembangan masyarakat tersebut, yang dipengaruhi oleh arus globalisasi informasi menjadikan Indonesia bagian dari masyarakat informasi dan transaksi elektronik di tingkat nasional. Oleh karena itu, pengembangan teknologi informasi perlu dilaksanakan secara optimal, merata, dan menjangkau seluruh lapisan masyarakat demi meningkatkan kecerdasan bangsa.²³

UU ITE menetapkan berbagai perbuatan yang dilarang atau tergolong sebagai tindak pidana di bidang informasi dan transaksi elektronik (*cyber crime*), dengan penentuan sifat melawan hukumnya serta bentuk serangan terhadap kepentingan hukum tertentu melalui rumusan pasal-pasal.²⁴ Menurut Ajaran Simon, suatu perbuatan yang dilarang setidaknya harus memenuhi beberapa unsur, yaitu:²⁵

²³ Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari*, Rineka Cipta, Jakarta, 2009, hlm. 40.

²⁴ Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik: Penyerangan terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, Ctk. Pertama, Bayumedia Publishing, Malang, 2011, hlm. 3.

²⁵ Siswanto Sunarso, *Op. Cit.* hlm. 90.

- a. Terdapat perbuatan manusia, termasuk sikap pasif berupa mengabaikan.
- b. Perbuatan tersebut, baik perbuatan maupun mengabaikan, ditetapkan oleh undang-undang sebagai perbuatan terlarang dan diancam dengan sanksi pidana.
- c. Perbuatan itu dilakukan oleh individu yang dapat diminta pertanggungjawaban pidana, yakni seseorang yang secara hukum dapat dipersalahkan atas perbuatannya.

Pengaturan tindak pidana informasi dan transaksi elektronik tercantum dalam Pasal 27 hingga Pasal 35, Pasal 36 tidak mengatur bentuk perbuatan pidana tertentu, melainkan memberikan dasar pemberatan pidana apabila perbuatan dalam Pasal 30 sampai Pasal 34 menimbulkan kerugian materiil bagi orang lain. Pasal 37 juga memuat ketentuan mengenai pemberatan pidana, namun dengan pertimbangan yang berbeda dari Pasal 36 karena berlaku untuk tindak pidana dalam Pasal 27 hingga Pasal 36 dan dilakukan di luar wilayah Indonesia. Adapun ketentuan mengenai ancaman pidananya diatur dalam Pasal 45 sampai dengan Pasal 52.

UU ITE mengatur berbagai aspek informasi dan transaksi elektronik. Namun, regulasi tersebut belum memuat ketentuan spesifik mengenai penyalahgunaan AI dalam kejahatan *voice phishing*. Hal ini karena regulasi

tersebut masih pada tahap awal, sehingga cakupan pidana terkait penipuan melalui suara berbasis teknologi belum mencakup tingkat tersebut.²⁶

4. Penipuan

Penipuan merupakan tindakan menyampaikan pernyataan palsu atau rangkaian kebohongan yang dibuat seolah-olah benar untuk mengelabui seseorang. Pelaku biasanya memberikan informasi yang tidak sesuai kenyataan guna meyakinkan korban agar mengikuti keinginannya.²⁷ Menurut Kamus Besar Bahasa Indonesia (yang selanjutnya disebut KBBI), Penipuan adalah perbuatan, cara, hal menipu, atau dapat didefinisikan sebagai perbuatan yang bertujuan untuk mengecoh orang lain.²⁸

Penipuan termasuk kejahatan yang diatur dalam Bab XXV KUHP tentang Perbuatan Curang, khususnya dalam Pasal 378 sampai Pasal 395 KUHP. Pasal 378 KUHP mengatur tindak pidana “*oplichting*” yang berarti penipuan dalam arti lebih sempit. Sementara itu, pasal-pasal lainnya dalam bab yang sama memuat bentuk-bentuk tindak pidana lain yang juga berkaitan dengan penipuan dalam cakupan yang lebih luas.²⁹ Adapun bunyi Pasal 378 KUHP yakni “barang siapa dengan maksud untuk menguntungkan diri sendiri

²⁶ Alya Alviani dan Yenny Fitri.Z, *Op. Cit.* hlm. 212.

²⁷ Muhammad Ridwan Lubis et al., “Peningkatan Kesadaran Hukum Masyarakat: Memahami Perbedaan Tindak Pidana Penipuan dan Penggelapan,” *Bulletin of Community Engagement*, No. 2, Vol. 3, Institut Agama Islam Ma'arif NU Metro Lampung, 2023, hlm. 265.

²⁸ Kamus Besar Bahasa Indonesia, terdapat dalam <https://www.kbbi.web.id/tipu>, diakses tanggal 06 Desember 2025, pukul 00.25.

²⁹ Alwan Hadiyanto et al., *Tindak Pidana Penipuan Menurut KUHP dan Syariat Islam*, Edisi Pertama, Damera Press, Jakarta Selatan, 2023, e-book, hlm. 8.

atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun.”

Sementara itu, menurut Brigjen Drs. H. A. K. Moch. Anwar, S.H. dalam bukunya yaitu Hukum Pidana Bagian Khusus, tindak pidana penipuan diartikan sebagai tindakan membujuk orang lain melalui tipu muslihat, rangkaian kebohongan, penggunaan nama palsu, atau keadaan palsu untuk memperoleh suatu pemberian. Selain itu, tindak pidana penipuan memiliki dua unsur, yaitu unsur objektif dan unsur subjektif.³⁰ Unsur subjektif dalam penipuan mencakup niat untuk memperoleh keuntungan bagi diri sendiri atau orang lain serta kesadaran untuk bertindak melawan hukum. Sedangkan, unsur objektif yaitu perbuatan yang dilakukan, pelaku, objek yang menjadi sasaran (misalnya penyerahan barang, pemberian utang, atau penghapusan piutang), serta cara-cara yang digunakan seperti memakai nama palsu, tipu muslihat, kedudukan palsu, atau rangkaian kebohongan.³¹

F. Definisi Operasional

Penelitian ini memberikan batasan makna untuk beberapa istilah yakni sebagai berikut:

³⁰ *Ibid.* hlm. 9-10.

³¹ Muhammad Ridwan Lubis et al., *Op. Cit.* hlm. 263.

1. *Voice Phishing* adalah bentuk penipuan berbasis suara melalui panggilan telepon yang dilakukan dengan tujuan untuk mengelabui korban agar memberikan informasi sensitif, seperti kata sandi, data pribadi, hingga uang. Kejahatan ini memanfaatkan manipulasi psikologis terhadap manusia sebagai celah keamanan, terutama di era digital yang semakin maju.³²
2. *Artificial Intelligence (AI)* atau kecerdasan buatan adalah kemampuan sistem komputer atau mesin untuk menirukan kemampuan kognitif manusia, termasuk belajar, berpikir, bernalar, serta memecahkan masalah.³³ AI menggambarkan kemampuan mesin untuk bertindak dan membuat keputusan secara mandiri tanpa instruksi yang diprogram secara rinci.³⁴ Tujuan utamanya adalah membantu manusia dalam berbagai aktivitas dengan memproses data dan mengambil keputusan secara mandiri berdasarkan instruksi yang diberikan.
3. Tindak Pidana Siber adalah bentuk kejahatan yang terjadi di dunia maya atau ruang virtual dengan memanfaatkan teknologi canggih. Kejahatan ini dapat pula diartikan sebagai tindak pidana yang menjadikan teknologi informasi

³² Istna Rizqi Alamsyah dan Arief Rahman Yusuf, “Vishing Sebagai Ancaman Rekayasa Sosial: Analisis Teknik, Dampak, dan Upaya Perlindungan Pengguna,” *SULIWA: Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi*, No. 2, Vol. 2, SULIWA, 2025, hlm. 65.

³³ Muhammad Afdan Rojabi, *Pengantar Artificial Intelligence (AI)*, Afdan Rojabi Publisher, Bogor, 2025, hlm. 7.

³⁴ Ambuj Agrawal, *No-Code Artificial Intelligence: The New Way to Build AI Powered Applications (English Edition)*, BPB Publications, India, 2023, hlm. 1.

sebagai sasaran utama atau sebagai alat bantu dalam melakukan tindakan melanggar hukum.³⁵

4. Modus Operandi adalah rangkaian tindakan yang dilakukan pelaku saat melaksanakan suatu kejahatan. Pola ini berupa perilaku yang secara sengaja dikembangkan dan digunakan oleh pelaku sebagai cara untuk mencapai tujuan tindak kejahatan tersebut.³⁶
5. Hukum Pidana adalah keseluruhan ketentuan yang mengatur syarat-syarat yang harus dipenuhi oleh negara ketika negara bermaksud membentuk hukum mengenai pidana, serta aturan yang menetapkan jenis-jenis pidana yang dapat diterapkan. Dalam pengertian ini, hukum pidana merujuk pada hukum pidana positif.³⁷

G. Metode Penelitian

1. Tipologi Penelitian

Jenis penelitian yang digunakan dalam skripsi ini adalah penelitian hukum normatif, yaitu penelitian yang bertumpu pada studi pustaka. Penelitian hukum normatif disebut sebagai penelitian hukum doktrinal, karena jenis penelitian ini pada dasarnya berfokus pada kajian terhadap peraturan

³⁵ Aroma Elmina Martha, *Loc. Cit.*

³⁶ Johannes Ibrahim dan Yohanes Hermanto Sirait, *Kejahatan Transfer Dana: Evolusi dan Modus Kejahatan Melalui Sarana Lembaga Keuangan Bank*, Ctk. Pertama, Sinar Grafika, Jakarta, 2018, e-book, hlm. 146.

³⁷ Jan Remmelink, *Hukum Pidana*, Ctk. Pertama, Gramedia Pustaka Utama, Jakarta, 2003, e-book, hlm. 1.

perundang-undangan yang tertulis maupun berbagai bahan-bahan hukum.³⁸ Hukum merupakan seperangkat norma yang bersifat mengikat, dimana orang yang melanggar akan dikenai sanksi yang tegas dan nyata. Oleh karena itu, salah satu elemen paling fundamental dari hukum adalah hukum bersifat normatif, karena hukum menetapkan kewajiban, kewajiban yang diatur dalam norma hukum tersebut merupakan kewajiban yang bersifat yuridis.³⁹ Penelitian ini dilakukan untuk mengkaji norma-norma hukum yang berkaitan dengan fenomena *voice phishing* berbasis teknologi AI, khususnya dalam konteks tindak pidana siber di Indonesia.

2. Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini meliputi Pendekatan Perundang-Undangan (*Statute Approach*), yakni dengan menelaah berbagai peraturan perundang-undangan yang relevan seperti KUHP, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (yang selanjutnya disebut KUHP Nasional), Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana (yang selanjutnya disebut UU PP), UU ITE, dan UU PDP. Selain itu, penelitian ini juga menggunakan Pendekatan Konseptual (*Conceptual Approach*) untuk mengkaji konsep-konsep hukum yang berkaitan dengan *voice phishing*, teknologi AI, dan pengaturan hukum pidana.

³⁸ Iman Jalaludin Rifa'i et. al., *Metodologi Penelitian Hukum*, Sada Kurnia Pustaka, Banten, 2023, e-book, hlm. 126.

³⁹ Johnny Ibrahim, *Teori dan Metode Penelitian: Hukum Normatif*, Ctk. Kedua, Bayumedia, Malang, 2006, e-book, hlm. 48-51.

Selanjutnya, menggunakan Pendekatan Kasus (*Case Approach*) yang berperan dalam membangun argumen hukum secara sistematis, memberikan wawasan untuk memperkuat perlindungan hukum, khususnya terhadap kejahatan siber berupa *voice phishing* berbasis *deepfake*.

3. Objek Penelitian

Objek dari penelitian ini adalah:

- a. Modus operandi tindak pidana siber yang dilakukan melalui *voice phishing* berbasis *artificial intelligence*.
- b. Pengaturan hukum pidana terhadap tindak pidana siber yang dilakukan melalui *voice phishing* berbasis *artificial intelligence* di Indonesia.

4. Sumber Data Penelitian

Sumber data adalah asal atau tempat diambilnya data yang digunakan dalam penelitian. Dalam penelitian hukum normatif, data diperoleh dari sumber data sekunder, yaitu data yang berasal dari studi kepustakaan atau literatur yang memiliki keterkaitan dengan objek penelitian.⁴⁰ Penelitian ini menggunakan data sekunder dari bahan hukum yang terbagi menjadi 3 (tiga), yakni sebagai berikut:

- a. Bahan Hukum Primer

⁴⁰ Ishaq, *Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, serta Disertasi*, Ctk. Pertama, Alfabeta, Bandung, 2017, e-book, hlm. 66.

Bahan hukum primer yaitu bahan-bahan hukum yang memiliki kekuatan mengikat secara langsung.⁴¹ Penelitian ini menggunakan bahan hukum primer berupa KUHP, KUHP Nasional, UU PP, UU PDP, UU ITE, dan peraturan lainnya yang relevan.

b. Bahan Hukum Sekunder

Bahan hukum sekunder yaitu bahan yang berkaitan erat dengan bahan hukum primer dan berfungsi mendukung analisis serta pemahaman terhadap bahan hukum primer.⁴² Seperti buku, jurnal, hasil karya ilmiah para sarjana, hasil-hasil penelitian, dan lain sebagainya.

c. Bahan Hukum Tersier

Bahan hukum tersier yaitu bahan yang menyediakan informasi tambahan mengenai bahan hukum primer maupun sekunder.⁴³ Seperti Kamus Besar Bahasa Indonesia dan Kamus Hukum.

5. Teknik Pengumpulan Data

Dalam proses pengumpulan data, penulis melakukan studi literatur dan studi dokumen dengan mengumpulkan dan menelaah bahan-bahan hukum yang relevan, baik berupa peraturan perundang-undangan, buku, artikel, jurnal ilmiah maupun dokumen pendukung lainnya yang berkaitan dengan topik *voice phishing* dan pemanfaatan teknologi AI dalam tindak pidana siber.

⁴¹ Suratman dan Philips Dillah, *Metode Penelitian Hukum*, Ctk. Kedua, Alfabeta, Bandung, 2014, e-book, hlm. 67.

⁴² *Ibid.*

⁴³ *Ibid.*

6. Teknik Analisis Data

Analisis data yang digunakan dalam penelitian ini adalah analisis deskriptif kualitatif, yaitu teknik yang digunakan untuk mengolah dan menafsirkan data hukum secara sistematis guna menjawab rumusan masalah penelitian. Analisis ini dilakukan melalui tahapan pengklasifikasian data hingga penyajian hasil analisis dalam bentuk uraian naratif, hingga penarikan kesimpulan. Data yang telah dikumpulkan dari hasil studi kepustakaan, baik berupa peraturan perundang-undangan, literatur hukum, maupun dokumen-dokumen relevan lainnya, diolah dan dikaji dengan menggunakan pendekatan konseptual, perundang-undangan, serta pendekatan kasus.

H. Kerangka Skripsi

Penting untuk memberikan gambaran umum mengenai kerangka penulisan skripsi ini, mengingat kerangka tersebut disusun secara runtut guna memudahkan pemahaman terhadap alur pembahasan dan fokus kajian dalam penelitian yang dilakukan. Kerangka penulisan hasil penelitian ini dibagi menjadi 4 (empat) bab yang tidak dapat dipisahkan. Adapun uraian kerangka penulisan dalam skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

BAB I merupakan pengantar terhadap permasalahan yang diangkat dalam skripsi. Dimulai dengan uraian latar belakang yang

menjelaskan fenomena *voice phishing* berbasis kecanggihan teknologi AI dan *deepfake*. Selanjutnya dirumuskan permasalahan, tujuan penelitian, orisinalitas penelitian, tinjauan pustaka, definisi operasional, metode penelitian yang digunakan, serta ditutup dengan kerangka penulisan skripsi secara umum.

BAB II TINJAUAN UMUM TENTANG *ARTIFICIAL INTELLIGENCE*, TINDAK PIDANA SIBER, DAN PENGATURAN HUKUM *VOICE PHISHING* BERBASIS *DEEPAKE*

BAB II menguraikan tinjauan umum tentang dasar-dasar konseptual dan rumusan masalah yang ada. Penulis akan menjelaskan mengenai teori-teori yang relevan seperti teori modus operandi, tindak pidana siber, dan tindak pidana siber dalam Islam. Selain itu, bab ini memuat penjelasan umum mengenai *voice phishing*, teknologi AI dan *deepfake*.

BAB III HASIL PENELITIAN DAN PEMBAHASAN

BAB III merupakan bagian inti dari skripsi yang membahas secara mendalam fenomena *voice phishing* berbasis AI dalam sistem hukum pidana di Indonesia. Penulis akan menguraikan analisis hasil penelitian mengenai modus operandi tindak pidana siber yang

dilakukan melalui *voice phishing* berbasis AI dan pengaturan hukum pidana terhadap tindak pidana siber yang dilakukan melalui *voice phishing* berbasis AI di Indonesia. Penulis juga akan mengkaji penerapan hukum positif yang ada saat ini dan menyampaikan analisis yuridis serta memberikan alternatif solusi regulatif.

BAB IV PENUTUP

BAB IV berisi kesimpulan dari hasil analisis yang telah dilakukan, yang menjawab rumusan masalah dalam bentuk narasi padat. Selain itu, bab ini memuat saran-saran dari penulis agar dapat merespons tantangan hukum mengenai *voice phishing* secara komprehensif.

