cek jurnal

202212020_NADIATUL_QOMARIYAH_085706136576.doc

jurnal

cek jurnal

Universitas Abdurachman Saleh

Document Details

Submission ID

trn:oid:::1:3606790809

Submission Date

Jul 6, 2026, 1:47 AM UTC

Download Date

Jul 6, 2026, 3:17 AM UTC

File Name

202212020_NADIATUL_QOMARIYAH_085706136576.doc

File Size

123.5 KB

10 Pages

3,409 Words

22,807 Characters

30% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Small Matches (less than 15 words)

Top Sources

26% Internet sources
19% Publications
25% Submitted works (Student Papers)

Integrity Flags

1 Integrity Flag for Review

Hidden Text
10 suspect characters on 9 pages
Text is altered to blend into the white background of the document.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Top Sources

26% Internet sources
19% Publications
25% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	repository.unars.ac.id 2%
2	Internet	digilib.unila.ac.id 2%
3	Internet	repository.ulb.ac.id 1%
4	Student papers	Academic Library Consortium 1%
5	Internet	e-journal.upm.ac.id 1%
6	Student papers	Fakultas Hukum 1%
7	Internet	ojs.uid.ac.id 1%
8	Student papers	Universitas Negeri Jakarta 1%
9	Publication	Ardi Saputra Gulo, Sahuri Lasmadi, Khabib Nawawi. "Cyber Crime dalam Bentuk P... 1%
10	Student papers	unars 1%
11	Internet	ejournal.uika-bogor.ac.id 1%

12	Student papers	
Universitas Jambi		<1%
13	Internet	
tiarramon.wordpress.com		<1%
14	Internet	
repository.unissula.ac.id		<1%
15	Student papers	
Universitas Muhammadiyah Jember		<1%
16	Student papers	
Universitas Djuanda		<1%
17	Internet	
etheses.uin-malang.ac.id		<1%
18	Student papers	
State Islamic University of Alauddin Makassar		<1%
19	Student papers	
Asia e University		<1%
20	Internet	
repository.untag-sby.ac.id		<1%
21	Publication	
Rd. Shabrina Azwa A., Divya Aliyyu, Immanuel. "Tokenisasi Properti dan Smart C...		<1%
22	Internet	
unars.ac.id		<1%
23	Internet	
www.tvonenews.com		<1%
24	Internet	
www.ojs.umb-bungo.ac.id		<1%
25	Internet	
eprints.unwahas.ac.id		<1%

26 Internet

www.suararakyat21.com <1%

27 Student papers

Universitas Muhammadiyah Palembang <1%

28 Student papers

Universitas Pendidikan Ganesha <1%

29 Internet

eprints.unram.ac.id <1%

30 Student papers

UPA Perpustakaan UNTIRTA <1%

31 Internet

journals.usm.ac.id <1%

32 Publication

Gabriel Regina Christian, Gousta Feriza. "Penerapan Asas Lex Specialis dalam Kas... <1%

33 Internet

repository.umsu.ac.id <1%

Jurnal Ilmiah
F E N O M E N A
P-ISSN; 3047-7204, E-ISSN; 0215-1448
https://unars.ac.id/ojs/index.php/fenomena/index

TANGGUNG JAWAB PIDANA PENIPUAN DENGAN TEKNIK *DEEPFAKE* PENGAKU POLISI BERDASARKAN UNDANG-UNDANG NOMOR 1 TAHUN 2024 ATAS PERUBAHAN KEDUA UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

CRIMINAL LIABILITY FOR FRAUD INVOLVING DEEPFAKE TECHNOLOGY AND IMPORSONATION OF A POLICE OFFICER UNDER LAW NUMBER 1 OF 2024 SECOND AMENDMENT TO LAW NUMBER 11 OF 2008 AN ELECTRONIC INFORMATION AND TRANSACTIONS.

Nadiatul Qomariyah[1], Ide Prima Hadiyanto[2], Irwan Yulianto[3]
[1,2,3]Fakultas Hukum, Sarjana Hukum, Universitas Abdurachman Saleh Situbondo Email: nadiatulqomariyah163@gmail.com

Abstrak

Nadiatul Qomariyah, NPM. 202212020, Tanggung Jawab pidana penipuan dengan Teknik *deepfake* pengaku polisi berdasarkan undang undang nomor 1 tahun 2024 atas perubahan pertama undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.Penelitian yang berjudul Tanggung jawab pidana penipuan dengan Teknik *deepfake* pengaku polisi berdasarkan undang-undang nomor 1 tahun 2024 atas perubahan pertama undang undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik dilatarbelakangi oleh maraknya penipuan melalui media elektronik dengan mengaku polisi sebagai bentuk perlakuan negative agar korban memberikan imbalan terhadapnya dengan kedok aparat kepolisian.Penelitian ini bertujuan pertama untuk mengkaji pengaturan hukum terkait tindak penipuan berbasis teknologi *deepfake* dalam perspektif Undang-Undang Nomor 11 Tahun 2024 tentang perubahan kedua atas Undang-Undang Nomor 11 Tahun 2024 tentang Informasi dan transaksi Eeektronik dalam praktik tindak pidana siber. berdasarkan ketentuan hukum pidana yang berlaku. Metode penelitian yang digunakan dalam skripsi ini menggunakan metode penelitian yuridis normatif yang merupakan penelitian kepustakaan, yaitu penelitian terhadap peraturan perundang-undangan dan literatur yang berkaitan dengan materi yang dibahas.Berdasarkan hasil penelitian dapat disimpulkan Pertama, Pengaturan hukum terhadap tindak pidana penipuan dengan teknik *deepfake* berupa pengakuan sebagai polisi dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan transaksi elektronik menyatakan hukum yang jelas,pelaku kejahatan berbasis teknologi karena dikualifikasikan sebagai penyebaran informasi elektronik yang menyesatkan serta penipuan yang merugikan korban. Kedua, Ancaman pidana terhadap pelaku berupa pidana

penjara dan/atau denda dalam ketentuan Undang-Undang Informasi Dan Transaksi Elektronik(UU ITE) yang telah diperbarui, tergantung pada unsur perbuatan yang terpenuhi, seperti unsur kesengajaan, tanpa hak, serta adanya kerugian yang ditimbulkan.

Kata Kunci: Penipuan, *deepfake,* polisi.

Abstract

Nadiatul Qomariyah, NPM. 2022-12-2020, Criminal Liability for Fraud Using Deepfake Techniques Impersonating Police Officers Based on Law Number 1 of 2024, as amended by the First Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.This research, entitled "Criminal Liability for Fraud Using Deepfake Techniques Impersonating Police Officers Based on Law Number 1 of 2024, as amended by the First Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions," is motivated by the rise of fraud through electronic media using impersonators as a form of negative treatment to induce victims to pay them under the guise of police officers.This research aims, firstly, to examine the legal regulations related to deepfake technology-based fraud from the perspective of Law Number 1 of 2024, as amended by the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, in the practice of cybercrime, based on applicable criminal law provisions.The research method used in this thesis is a normative juridical research method, which is library research, namely the study of laws and regulations and literature related to the material discussed.Based on the research results, it can be concluded: First, the legal regulation for the crime of fraud using deepfake techniques, in the form of recognition as a police officer in Law Number 1 of 2024 concerning Information and Electronic Transactions, clearly defines the law, categorizing perpetrators of technology-based crimes as disseminating misleading electronic information and fraud that harms victims. Second, the criminal threat to perpetrators in the form of imprisonment and/or fines under the provisions of the updated ITE Law, depends on the elements of the act being fulfilled, such as intent, without rights, and the harm caused.

***Keywords**: Fraud, deepfake, police*

PENDAHULUAN

Komunikasi adalah proses penyampaian pesan atau informasi dari satu pihak kepada pihak lainnya sehingga pesan yang dimaksud dapat dipahami.[1] Dalam kehidupan terdapat komunikasi yang menjadi jalan dalam berinteraksi antara satu dengan lainnya. Dengan komunikasi sesuatu dapat tersampaikan dengan baik dengan berbagai media yang ada. Media elektronik yang menjadi kebutuhan masyarakat, menjadi sorotan hukum dalam penggunaannya. Hal ini dikarenakan berbagai macam hal yang dilakukan sehingga dalam proses

[1] Fakultas ilmu sosial dan ilmu politik,*"Komunkasi Adalah : pengertian, jenis dan tujuannya"*, https://fisip.umsu.ac.id/komunikasi-adalah-pengertian-jenis-dan-tujuannya/ diakses pada tanggal 05 April 2026

penggunaan elektronik dapat terarah dan tidak menjadi sesuatu yang merugikan baik bagi pengguna ataupun penerima. Banyak hal negatif yang terjadi dengan adanya elektronik terutama penggunaan HP (*Handphone*), dimana masyarakat hampir semua menggenggam media tersebut.

Berbagai macam hal terjadi, dari pelaku bisnis *online* sampai adanya penipuan *online*. Maraknya penipuan yang merajalela dalam media elektronik terlebih penggunaan *Handphone* dan sejenisnya yang menjadikan sebagian masyarakat menjadi korban penipuan tersebut. Penipuan ini ada yang dikemas dengan hal yang sederhana bahkan sampai difikirkan secara matang. Salah satu penipuan yang terjadi adalah penipuan *(Deepfake)*. Diantara penipuan ini yaitu pelaku mengaku sebagai seorang anggota oknum polisi dengan proses menelpon korban tujuannya untuk mendapatkan keuntungan dari korban dengan cara menakut nakuti dengan kisah ingin membantu dan kemudian mendapatkan imbalan dari proses bantuan tersebut.

29 Undang – undang Nomor 1 Tahun 2024 tentang Informasi Dan Transaksi Elektronik yang merupakan perubahan kedua dari Undang-undang nomor 11 tahun 2008 merupakan sebuah aturan untuk pengguna elektronik yang dengan sengaja melakukan sebuah hal yang merugikan orang lain dengan media elektronik yang ada. Kejahatan yang orang lakukan dengan media tersebut semakin mudah dilakukan karena adanya media yang mudah diakses tanpa perlu adanya usaha yang berat. Teknologi yang memadai menjadi jalan baru untuk melakukan perbuatan yang lebih baru. Penggunaan *deepfake* dalam penipuan dengan mengaku aparat kepolisian menunjukkan adanya penyalahgunaan otoritas secara tidak langsung. Pelaku memanfaatkan citra dan kewenangan aparat hukum untuk menekan psikologis korban agar patuh. Hal ini memperlihatkan bahwa kejahatan tidak hanya menyerang aspek ekonomi, tetapi juga aspek psikologis serta kepercayaan masyarakat terhadap negara.

Dari perspektif hukum pidana, perbuatan tersebut dapat dikualifikasikan sebagai tindak pidana penipuan melalui media elektronik. Namun, diperlukan analisis lebih lanjut terkait pertanggungjawaban pidana pelaku, khususnya dalam pembuktian unsur kesengajaan (dolus) dan perbuatan melawan hukum. Hal ini menjadi penting karena penggunaan teknologi *deepfake* dapat menyamarkan identitas pelaku.[2]

METODE PENELITIAN

8 Metode penelitian menurut Woody Adalah suatu metode untuk menemukan sebuah pemikiran kritis. Penelitian meliputi pemberian definisi dan redefinisi terhadap masalah, memformulasikan hipotesis atau jawaban sementara, membuat Kesimpulan dan sekurang-kurangnya mengadakan pengujian yang hati-hati atas semua kesimpulan yang diambil untuk menentukan apakah kesimpulan tersebut cocok dengan hipotesis.[3]

Penelitian ini menggunakan metode penelitian hukum normatif karena fokus terhadap peraturan perundang-undangan, undang-undang informasi dan teknologi

[2] Muljatno, 2008, *Asas Hukum Pidana*, Rineka Cipta : Jakarta , hal 171
[3] Sandu Siyoto. M. Ali Sodik, 2015, *Dasar Metodologi Penelitian*, Literasi Media Publishing: Yogyakarta, Hal. 5

eletronik (ITE) yang mengkaji dan menelaah norma hukum terkait *deepfake* dan penipuan tanpa melakukan penelitian secara langsung ke lapangan. Metode ini digunakan untuk memahami bagaimana undang-undang informasi dan teknolgi elektornuik (ITE) melihat *deepfake* menngaku sebagai polisi.[4]

Metode pengumpulan bahan hukum dalam penelitian ini dilakukan melalui studi kepustakaan *(library research)*. Studi kepustakaan dilakukan dengan mengumpulkan, membaca, dan mengkaji secara sistematis berbagai bahan hukum primer dan sekunder yang relevan dengan permasalahan penelitian. Pengumpulan bahan hukum dilakukan melalui penelusuran peraturan perundang-undangan, buku teks, jurnal ilmiah, serta sumber akademik lain yang kredibel.[5]

Teknik analisis bahan hukum menggunakan analisis kualitatif dengan menginventarisasi aturan hukum yaitu dengan melakukan proses pendataan, pencatatan dan pengelompokan secara sistematis terhadap peraturan perundang-undangan, produk hukum, atau norma-norma yang berlaku terkait penelitian ini. Kemudian menafsirkan pasal-pasal (interpretasi hukum) yaitu memahami aturan yang terdapat dalam pasal penipuan serta dalam aturan Undang Undang informasidan transaksi elektronik (UU ITE) terkait *Deepfake* mengaku sebagapolisi. Setelah itu Mengaitkan dengan fenomena *deepfake* dan menarik Kesimpulan.[6]

HASIL DAN PEMBAHASAN

Perkembangan teknologi kecerdasan buatan (*artificial intelligence*) telah melahirkan berbagai inovasi yang tidak sekadar membawa manfaat, melainkan juga membuka celah bagi tindak kejahatan baru. Salah satu produk teknologi yang paling rawan disalahgunakan adalah *deepfake*, yakni teknik manipulasi media digital yang memungkinkan seseorang untuk menciptakan wajah, suara, dan identitas palsu secara sangat realistis menggunakan algoritma pembelajaran mendalam (*deep learning*). Bentuk hasil dari deepfake ini adalah *user interface* yang membuat tampilan muka dengan sebuah gambar dan video di gabungkan sehingga tampak lebih nyata. *Deepfake* saat ini menggunakan teknik *deep learning* yang merupakan cabang dari machine learning yang dimana *machine learning* ini adalah suatu cara atau bagian dari kecerdasan buatan atau *AI* untuk mencapai tujuannya.[7] Di Indonesia, penyalahgunaan teknologi ini telah mulai marak digunakan dalam modus penipuan, termasuk oleh pelaku yang berpura-pura menjadi anggota kepolisian demi memperoleh kepercayaan korban dan pada akhirnya mengambil keuntungan secara finansial secara melawan hukum.[8]

Dalam konteks hukum positif Indonesia, tindak pidana penipuan berbasis teknologi informasi telah diatur secara khusus dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut hadir

[4] Peter Mahmud Marzuki, 2019, *Penelitian Hukum*, Kencana : Jakarta, hal. 32–35
[5] *Ibid*, hal 194-198
[6] *Ibid*, hal 213-217
[7] Rindang Gici Oktavianti, Abdurrahman Muqsith, Isma Nadia, 2025, *Penyalahgunaan Deepfake Era Canggihnya Teknologi Memicu Kejahatan Media*, Jurnal IUS Vol.XIII No.01, hal. 119
[8] Tanda Firmansyah dan Putri Ayu Lestari, 2023, "*Deepfake sebagai Ancaman Kejahatan Digital: Perspektif Hukum Pidana Indonesia*,"Jurnal Hukum dan Teknologi Informasi,Vol. 5, No. 1,hlm. 12

sebagai respons atas perkembangan kejahatan siber yang semakin canggih dan kompleks, termasuk kejahatan yang memanfaatkan teknologi manipulasi konten digital seperti *deepfake*. Kehadiran regulasi ini menjadi landasan hukum yang lebih kokoh dalam menjerat pelaku kejahatan digital yang sebelumnya sulit dijangkau oleh ketentuan pidana konvensional.[9]

Pasal yang paling relevan untuk menjerat pelaku penipuan deepfake pengaku polisi adalah Pasal 28 ayat (1) Undang undang informasi dan transaksi elektronik (UU ITE) yang melarang setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Ketentuan ini diperkuat dengan ancaman pidana dalam Pasal 45A ayat (1) Undang undang informasi dan transaksi elektronik (UU ITE) yang menegaskan bahwa pelanggaran atas larangan tersebut dikenai pidana penjara paling lama enam tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Pelaku penipuan yang menggunakan *deepfake* untuk menyamar sebagai polisi dan kemudian meminta uang kepada korban dengan dalih tertentu, seperti mengancam akan menangkap korban jika tidak membayar sejumlah uang, secara substansial telah memenuhi rumusan delik dalam pasal ini.[10]

Selain Pasal 28 ayat (1), perbuatan pelaku juga dapat dikenai Pasal 35 Undang undang informasi dan transaksi elektronik (UU ITE) yang mengatur tentang manipulasi, penciptaan, perubahan, penghilangan, dan pengrusakan informasi elektronik atau dokumen elektronik dengan tujuan agar informasi elektronik atau dokumen elektronik tersebut dianggap seolah-olah data yang autentik. Penggunaan teknologi *deepfake* oleh pelaku untuk menciptakan video atau rekaman audio palsu yang menampilkan sosok polisi fiktif merupakan bentuk manipulasi konten elektronik yang secara tegas dilarang oleh pasal ini. Ketentuan ini merupakan salah satu perubahan krusial yang dihadirkan oleh Undang undang Nomor 1 Tahun 2024 Tentang informasi dan transaksi elektronik (UU ITE) yang memperluas cakupan perbuatan yang dapat dipidana dalam ranah kejahatan siber.[11]

Terhadap pelanggaran ketentuan Pasal 35 UU ITE, ancaman pidana yang dapat dijatuhkan kepada pelaku diatur dalam Pasal 51 ayat (1) Undang undang informasi dan transaksi elektronik (UU ITE), yaitu pidana penjara paling lama dua belas tahun dan denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). Ancaman pidana yang lebih berat ini mencerminkan tingkat bahaya yang lebih tinggi dari perbuatan manipulasi konten elektronik dibandingkan sekadar penyebaran berita bohong biasa. Hal ini juga menunjukkan komitmen pembentuk undang-undang untuk memberikan efek jera yang signifikan bagi pelaku kejahatan digital yang memanfaatkan teknologi canggih seperti *deepfake* dalam melakukan aksinya.[12]

---

[9] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 35 jo. Pasal 51 ayat (1).

[10] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 28 ayat (1) jo. Pasal 45A ayat (1).

[11] Ahmad Sofian, "*Pertanggungjawaban Pidana dalam Tindak Pidana Penipuan Berbasis Teknologi Informasi*," *Jurnal Hukum Pidana dan Kriminologi,* Vol. 4, No. 2, 2023, hlm. 87.

[12] Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11

Aspek penting lainnya dalam pengenaan pidana terhadap pelaku adalah pembuktian unsur mens rea atau niat jahat. Dalam tindak pidana penipuan dengan *deepfake*, mens rea pelaku sangat jelas terbukti dari rangkaian tindakannya: mulai dari proses persiapan yang mencakup pembuatan konten *deepfake*, pemilihan target korban, hingga komunikasi aktif dengan korban menggunakan identitas palsu seorang polisi. Seluruh rangkaian perbuatan ini menunjukkan adanya niat yang sudah terencana dan kesengajaan penuh dari pelaku untuk merugikan korban. Hal ini memenuhi syarat pertanggungjawaban pidana yang diatur dalam hukum pidana Indonesia, di mana niat jahat merupakan salah satu elemen esensial untuk menjatuhkan pemidanaan.

Perkembangan teknologi *deepfake* telah menciptakan tantangan baru bagi sistem hukum pidana Indonesia. Teknologi ini memungkinkan manipulasi wajah, suara, maupun video seseorang sehingga tampak asli dan sulit dibedakan dari konten autentik. Dalam praktiknya, teknologi tersebut tidak hanya digunakan untuk tujuan hiburan, tetapi juga dimanfaatkan sebagai sarana melakukan penipuan, pencurian identitas digital, penyebaran disinformasi, dan berbagai bentuk kejahatan siber lainnya. Oleh karena itu, penyalahgunaan teknologi *deepfake* memerlukan perhatian serius karena berpotensi menimbulkan kerugian materiil maupun immateriil bagi masyarakat.[13]

Dari perspektif pertanggungjawaban pidana, pelaku yang secara sengaja membuat, menyebarluaskan, dan menggunakan konten *deepfake* untuk memperoleh keuntungan secara melawan hukum dapat dimintai pertanggungjawaban atas seluruh akibat yang ditimbulkan. Kesengajaan tersebut tercermin dari adanya proses perencanaan, pengumpulan data identitas korban atau pihak yang ditiru, penggunaan perangkat lunak kecerdasan buatan, hingga pelaksanaan komunikasi yang bertujuan mengelabui korban. Dengan demikian, unsur kesalahan (*mens rea*) dalam tindak pidana penipuan berbasis *deepfake* pada umumnya dapat dibuktikan melalui rangkaian tindakan yang dilakukan pelaku sebelum dan selama kejahatan berlangsung.[14]

Selain itu, perkembangan kejahatan *deepfake* menunjukkan perlunya pembaruan hukum pidana yang lebih spesifik. Meskipun saat ini Undang undang informasi dan transaksi elektronik (UU ITE) dapat digunakan untuk menjerat pelaku melalui ketentuan mengenai manipulasi informasi elektronik dan penyebaran informasi menyesatkan, sejumlah akademisi menilai bahwa pengaturan khusus mengenai *deepfake* diperlukan untuk memberikan kepastian hukum yang lebih jelas, terutama terkait definisi, ruang lingkup perbuatan, serta mekanisme pembuktian dalam perkara yang melibatkan teknologi kecerdasan buatan.[15]

Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 35 jo. Pasal 51 ayat (1).

[13] Supuan Sultan Al Alif, Anis Rindiani, dan Cik Marhayati, 2025, "*Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake di Indonesia*," Legal Standing: Jurnal Ilmu Hukum, Vol. 9, No. 5, hlm. 2–4.

[14] Muhammad Syafiq Wafi, Aloysius Wisnubroto, dan Yudi Prayudi, 2025, "*Artificial Intelligence-Based Deepfake Crimes*: A Conception of Culpability Principle as a Criminal Liability Reform," Reformasi Hukum, Vol. 29, No. 2, hlm. 210–214.

[15] Trisno Ariwibowo, Ismaidar, Abdul Rahman M.S., Sahidan Angga Nurdana, dan Pian Rostani Waruwu, 2026, "*Analisis Hukum Pidana Terhadap Penyebaran Deepfake Berbasis Artificial Intelligence (AI) Dalam Perspektif Pembaruan Hukum Pidana di* Indonesia," YUSTISI, Vol. 13, No.

turnitin Page 11 of 15 - Integrity Submission Submission ID trn:oid:::1:3606790809

Mengenai pembuktian tindak pidana penipuan berbasis *deepfake,* Undang undang informasi dan transaksi elektronik (UU ITE) telah memberikan landasan hukum yang memadai untuk mengakui bukti elektronik sebagai alat bukti yang sah. Berdasarkan Pasal 5 Undang undang informasi dan transaksi elektronik (UU ITE), informasi elektronik atau dokumen elektronik merupakan alat bukti yang sah sepanjang menggunakan sistem elektronik yang memenuhi ketentuan yang diatur dalam undang-undang ini. Dengan demikian, rekaman video *deepfake*, riwayat percakapan elektronik, serta metadata digital dari perangkat yang digunakan pelaku dapat dijadikan sebagai alat bukti yang kuat dalam proses peradilan. Penjelasan Pasal 35 Undang undang informasi dan transaksi elektronik (UU ITE) secara khusus menegaskan bahwa dokumen elektronik yang dimanipulasi dengan cara apapun, termasuk melalui teknologi kecerdasan buatan, tetap dapat dijadikan objek delik.[16]

Dalam hal pelaku melakukan tindak pidana penipuan *deepfake* melewati batas yurisdiksi nasional, yakni pelaku berdomisili di luar negeri namun korban berada di Indonesia, Undang undang informasi dan transaksi elektronik (UU ITE) tetap dapat diterapkan berdasarkan asas perlindungan pasif (*passive personality principle*). Berdasarkan asas ini, hukum pidana Indonesia berlaku terhadap setiap orang yang di luar wilayah Indonesia melakukan tindak pidana yang menimbulkan kerugian terhadap warga negara Indonesia. Selain itu, Pasal 2 Undang undang informasi dan transaksi elektronik (UU ITE), secara tegas menyatakan bahwa undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia.

Berdasarkan seluruh uraian di atas, dapat disimpulkan bahwa ancaman pidana yang dapat dikenakan terhadap pelaku penipuan dengan teknik *deepfake* pengaku polisi berdasarkan UU Nomor 1 Tahun 2024 Tentang informasi dan transaksi elektronik (UU ITE) adalah sebagai berikut: Pertama, berdasarkan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) Undang undang informasi dan transaksi elektronik (UU ITE), pelaku dapat diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Kedua, berdasarkan Pasal 35 jo. Pasal 51 ayat (1) Undang undang informasi dan transaksi elektronik (UU ITE) atas manipulasi konten elektronik berupa pembuatan video atau audio *deepfake* palsu, pelaku dapat diancam dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). Ketiga, apabila kejahatan dilakukan oleh korporasi atau sindikat terorganisir, pidana pokok tersebut dapat ditambah dua pertiga berdasarkan Pasal 51 ayat (2) Undang undang informasi dan transaksi elektronik (UU ITE). Selain itu, secara kumulatif pelaku juga dapat dijerat dengan Pasal 492 KUHP tentang penipuan dengan ancaman pidana penjara paling lama 4 (empat) tahun.

2, hlm. 150–154.

[16]Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Penjelasan Pasal 35.

Dengan memperhatikan seluruh ketentuan yang telah diuraikan, maka Undang undang Nomor 1 Tahun 2024 atas Perubahan Kedua Undang undang informasi dan transaksi elektronik (UU ITE) telah menyediakan instrumen hukum yang cukup memadai untuk menjerat pelaku penipuan dengan teknik *deepfake*. Namun demikian, efektivitas penerapan ketentuan-ketentuan tersebut sangat bergantung pada kapasitas aparat penegak hukum dalam memahami dan mengidentifikasi kejahatan siber berbasis teknologi canggih, serta ketersediaan sarana dan prasarana forensik digital yang memadai. Oleh karena itu, penguatan kapasitas penegak hukum melalui pendidikan dan pelatihan dalam bidang forensik digital merupakan prasyarat penting bagi penerapan hukum yang efektif dalam menghadapi kejahatan teknologi yang terus berkembang.

Kesimpulannya, hukum pidana Indonesia melalui Undang undang Nomor 1 Tahun 2024 Tentang informasi dan transaksi elektronik (UU ITE) telah mampu menjawab tantangan penipuan siber berbasis *deepfake* dengan menyediakan ancaman pidana yang tegas dan berjenjang. Dalam menjerat pelaku penipuan deepfake pengaku polisi, penegak hukum memiliki pilihan untuk menerapkan Pasal 28 ayat (1) jo. Pasal 45A Undang undang informasi dan transaksi elektronik (UU ITE) dan Pasal 35 jo. Pasal 51 Undang undang informasi dan transaksi elektronik (UU ITE), baik secara alternatif maupun kumulatif dengan Kitab Undang Undang Hukum Pidana (KUHP) tentang penipuan, tergantung pada konstruksi perbuatan konkret yang dilakukan pelaku. Sinergi antara ketentuan Undang undang informasi dan transaksi elektronik (UU ITE) dan Kitab Undang Undang Hukum Pidana (KUHP), disertai penguatan bukti elektronik dan kerjasama lintas negara dalam penanganan kejahatan siber transnasional, akan memperkuat posisi hukum Indonesia dalam menghadapi ancaman penipuan digital yang semakin canggih di era teknologi kecerdasan buatan saat ini.[17]

PENUTUP

Berdasarkan pembahasan diatas, dapat disimpulkan bahwa:

1. Pengaturan hukum terhadap tindak pidana penipuan dengan teknik *deepfake* berdasarkan Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Tindak pidana penipuan dengan teknik *deepfake* yang dilakukan dengan mengaku sebagai anggota kepolisian merupakan bentuk kejahatan siber yang memanfaatkan teknologi kecerdasan buatan untuk menipu korban dan memperoleh keuntungan secara melawan hukum. Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah memberikan dasar hukum yang cukup jelas untuk menjerat pelaku melalui ketentuan mengenai penyebaran informasi bohong, manipulasi informasi elektronik, perlindungan data pribadi, serta kewenangan penegakan hukum terhadap kejahatan digital. Selain itu, pengaturan tersebut juga didukung oleh Undang-Undang Perlindungan Data Pribadi dalam melindungi data biometrik yang sering digunakan dalam

[17]Henny Mono, *Teknik Menyusun Dakwaan,* Pustaka Yustisia, Yogyakarta, 2011, hlm. 78; lihat pula Undang-Undang Nomor 1 Tahun 2024, Pasal 45A ayat (1) dan Pasal 51 ayat (1).

pembuatan *deepfake*. Meskipun demikian, efektivitas penerapannya masih memerlukan dukungan berupa peningkatan kemampuan aparat penegak hukum, penguatan regulasi, serta peningkatan kesadaran dan literasi digital masyarakat agar penanggulangan tindak pidana penipuan berbasis *deepfake* dapat dilakukan secara optimal.

2. Ancaman pidana yang dapat dikenakan terhadap pelaku penipuan dengan teknik *deepfake* pengaku polisi berdasarkan Undang Undang nomor 1 tahun 2024 atas perubahan kedua Undang Undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Pelaku penipuan dengan teknik *deepfake* yang mengaku sebagai anggota kepolisian dapat dimintai pertanggungjawaban pidana berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Perbuatan tersebut memenuhi unsur penyebaran informasi bohong dan menyesatkan serta manipulasi informasi elektronik yang dibuat seolah-olah autentik untuk memperoleh keuntungan secara melawan hukum. Oleh karena itu, pelaku dapat dijerat dengan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) Undang-Undang Informasi dan Transaksi Elektrioni (UU ITE) dengan ancaman pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah), serta Pasal 35 jo. Pasal 51 ayat (1) UU ITE dengan ancaman pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). Selain itu, pelaku juga dapat dikenakan ketentuan dalam KUHP apabila perbuatannya memenuhi unsur tindak pidana penipuan atau pemalsuan. Dengan demikian, Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua Undang-Undang nomor 11 tahun 2008 tentang informasi dan transaksi elektrionik,yang telah memberikan dasar hukum yang cukup kuat dalam menanggulangi kejahatan penipuan berbasis *deepfake*, meskipun efektivitas penegakannya tetap memerlukan dukungan kapasitas aparat penegak hukum, kemampuan forensik digital, serta peningkatan kesadaran masyarakat terhadap bahaya kejahatan siber.

DAFTAR PUSTAKA

Buku

Henny Mono, *Teknik Menyusun Dakwaan,* Pustaka Yustisia, Yogyakarta,

Muljatno, 2008, *Asas Hukum Pidana*, Rineka Cipta : Jakarta: Rineka Cipta

Peter Mahmud Marzuki, 2019, *Penelitian Hukum*, Kencana : Jakarta

Sandu Siyoto. M. Ali Sodik, 2015, *Dasar Metodologi Penelitian*, Literasi Media Publishing: Yogyakarta

Undang-Undang

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Jurnal

Ahmad Sofian, "Pertanggungjawaban Pidana dalam Tindak Pidana Penipuan Berbasis Teknologi Informasi," *Jurnal Hukum Pidana dan Kriminologi,* Vol. 4, No. 2

Undang undang
Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Muhammad Syafiq Wafi, Aloysius Wisnubroto, dan Yudi Prayudi, 2025, "Artificial Intelligence Based Deepfake Crimes: A Conception of Culpability Principle as a Criminal Liability Reform," Reformasi Hukum, Vol. 29, No. 2

Rindang Gici Oktavianti, Abdurrahman Muqsith, Isma Nadia, 2025, *Penyalahgunaan Deepfake Era Canggihnya Teknologi Memicu Kejahatan Media*, Jurnal IUS Vol.XIII No.01,

Supuan Sultan Al Alif, Anis Rindiani, dan Cik Marhayati, 2025, "Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake di Indonesia," Legal Standing: Jurnal Ilmu Hukum, Vol. 9, No. 5

Tanda Firmansyah dan Putri Ayu Lestari, 2023, "Deepfake sebagai Ancaman Kejahatan Digital: Perspektif Hukum Pidana Indonesia,"Jurnal Hukum dan Teknologi Informasi,Vol. 5, No.1

Trisno Ariwibowo, Ismaidar, Abdul Rahman M.S., Sahidan Angga Nurdana, dan Pian Rostani Waruwu, 2026, "Analisis Hukum Pidana Terhadap Penyebaran Deepfake Berbasis Artificial Intelligence (AI) Dalam Perspektif Pembaruan Hukum Pidana di Indonesia," YUSTISI, Vol. 13,No,02

Website

Fakultas ilmu sosial dan ilmu politik*,"Komunkasi Adalah : pengertian, jenis dan tujuannya*",https://fisip.umsu.ac.id/komunikasi-adalah-pengertian-jenis-dan-tujuannya/ diakses pada tanggal 05 April 2026