Volume 14
Nomor 1- Maret 2026

# KEKOSONGAN HUKUM MENGENAI TINDAK PIDANA PENIPUAN DEEPFAKE DALAM UU ITE NOMOR 1 TAHUN 2024 MENURUT PERSFEKTIF HUKUM PIDANA ISLAM

**Indra Mulyana**[*)]
Indramulyanaa674@gmail.com

**Yayan Muhamad Royani**[*)]
yayanmroyani@uinsgd.ac.id

**Tia Ludiana**[*)]
tia.ludiana@uinsgd.ac.id

(Diterima 30Januari 2026, disetujui 14 Februari 2026)

***ABSTRACT***

*The current transformation of cybercrime is dominated by the use of Deepfake technology, which exploits the biometric identities of public officials for financial gain. However, Indonesia's positive legal instruments, specifically Article 28 paragraph (1) juncto Article 45A of Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law), demonstrate a significant legal lag. This study focuses on analyzing the vacuum of norm arising because the a quo article still necessitates elements of "false news" and "consumer loss," which are irrelevant to the nature of this crime. Employing a normative juridical method with statutory and conceptual approaches, this research finds that the current application of the ITE Law potentially creates impunity. This is because Deepfake constitutes a fabrication of synthetic reality, rather than merely the dissemination of hoaxes within electronic transactions. From the perspective of Fiqh Jinayah, this act is categorized as severe Al-Ghash and At-Tadlis, which violate the principles of Maqashid Sharia, specifically the protection of intellect and property. Due to the absence of specific scriptural provisions, this offense falls within the realm of Jarimah Ta'zir, necessitating judges to impose maximum sanctions to close the loopholes for harm (Sadd ad-Dzari'ah) and uphold substantive justice.*

**Keywords:** *Deepfake*, *Legal Vacuum, ITE Law, Jarimah Ta'zir, Maqashid Sharia*.

[*)] Mahasiswa Hukum Pidana Islam Universitas Islam Negeri Sunan Gunung Djati Bandung
[*)] Dosen Universitas Islam Negeri Sunan Gunung Djati Bandung
[*)] Dosen Universitas Islam Negeri Sunan Gunung Djati Bandung

**ABSTRAK**

Transformasi tindak pidana siber saat ini didominasi oleh penggunaan teknologi Deepfake yang menyalahgunakan identitas biometrik pejabat publik demi keuntungan finansial. Sayangnya, instrumen hukum positif di Indonesia, terutama Pasal 28 ayat (1) juncto Pasal 45A UU ITE Nomor 1 Tahun 2024, menunjukkan adanya kesenjangan norma (*legal lag*) yang signifikan. Studi ini difokuskan pada analisis kekosongan hukum (*vacuum of norm*) yang timbul karena pasal a quo masih mensyaratkan unsur berita bohong dan kerugian konsumen yang tidak relevan dengan sifat kejahatan ini. Dengan menggunakan metode yuridis normatif melalui pendekatan perundang-undangan dan konseptual, penelitian ini menemukan bahwa penerapan UU ITE saat ini berpotensi menciptakan impunitas. Hal ini karena Deepfake merupakan fabrikasi realitas sintetik, bukan sekadar penyebaran hoaks dalam transaksi elektronik. Dalam tinjauan Fiqh Jinayah, perbuatan ini dikategorikan sebagai *Al-Ghash* dan *At-Tadlis* berat yang mencederai prinsip *Maqashid Syariah*, khususnya pelindungan akal dan harta. Karena belum adanya dalil yang spesifik, tindak pidana ini masuk dalam ranah *Jarimah Ta'zir*, yang menuntut hakim menerapkan sanksi maksimal demi menutup celah kerusakan (*Sadd ad-Dzari'ah*) dan mewujudkan keadilan substantif.

**Kata Kunci:** *Deepfake*, Kekosongan Hukum, UU ITE, *Jarimah Ta'zir*, *Maqashid Syariah*.

## I. Pendahuluan

Transformasi digital yang begitu pesat telah mengubah lanskap kejahatan siber dari metode konvensional seperti *phising* berbasis teks atau tautan, menjadi modus yang jauh lebih canggih berupa *impersonation* atau penyamaran identitas menggunakan teknologi *Deepfake* (Trust 2025). Fenomena ini bukan lagi sekadar penyebaran disinformasi, melainkan telah berevolusi menjadi instrumen rekayasa sosial (*social engineering*) dan penipuan finansial (*fraud*) yang mengeksploitasi kepercayaan publik terhadap otoritas pejabat negara. Realitas ini menunjukkan bahwa manipulasi wajah pejabat negara tersebut bukan digunakan untuk tujuan politik atau penyebaran berita bohong semata, melainkan digunakan sebagai alat untuk meyakinkan korban agar memberikan atau mentransfer sejumlah dana.

Hal ini terbukti dari terungkapnya berbagai kasus manipulasi video pejabat tinggi seperti, Presiden Prabowo Subianto, Wakil Presiden Gibran Rakabuming Raka, hingga Menteri Keuangan Sri Mulyani yang direkayasa seolah-olah menawarkan bantuan sosial atau meminta transfer dana (Detikcom 2025).

Ketertinggalan hukum (*legal lag*) menjadi isu krusial dalam sistem hukum positif Indonesia saat menghadapi urgensi ancaman ini. Ketiadaan aturan spesifik mendorong aparat untuk tetap menggunakan Undang-Undang Republik Indonesia

Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun, analisis anatomi pasal menunjukkan adanya ketidakcocokan elemen. Pasal ini secara spesifik mengatur larangan berita bohong yang berdampak pada kerugian konsumen di ranah transaksi elektronik. *Ratio legis* atau alasan pembentukan pasal tersebut sebenarnya difokuskan pada perlindungan masyarakat dalam ekosistem *e-commerce*, seperti wanprestasi barang, bukan untuk jenis kejahatan yang sedang dibahas (Indonesia 2024).

Di sinilah letak inti permasalahan hukum yang menjadi fokus penelitian ini yaitu terdapat kekosongan norma (*vacuum of norm*) yang signifikan karena pasal tersebut tidak didesain untuk menjerat kejahatan manipulasi identitas biometrik.(Ruhtiani dan Istikharoh 2025) Kekosongan hukum ini terlihat dari dua ketidakcocokan unsur pasal dengan fakta material kejahatan *deepfake*:

1) Disparitas Ontologis Berita Bohong**,** Pasal 28 ayat (1) mensyaratkan adanya unsur menyebarkan berita bohong. Padahal, secara ontologis, *deepfake* adalah fabrikasi realitas sintetik atau impersonasi biometrik, bukan aktivitas jurnalistik atau penyebaran kabar (berita). Jika hakim memandang video manipulasi tersebut bukan sebagai berita dalam definisi hukum, maka unsur delik tidak terpenuhi.
2) Limitasi unsur konsumen dan transaksi. Pasal ini secara limitatif mensyaratkan adanya kerugian konsumen dalam transaksi elektronik. Konstruksi ini sejatinya dirancang untuk perlindungan *e-commerce*. Padahal, korban penipuan *deepfake* (seperti dalam kasus bansos palsu atau *love scamming*) seringkali bukan konsumen yang sedang melakukan transaksi dagang, melainkan warga negara yang diperdaya secara personal.

Memaksakan penerapan pasal perlindungan konsumen untuk mengadili kejahatan pencurian identitas biometrik adalah sebuah konstruksi hukum yang dipaksakan (*forced construction*) yang mencederai asas kepastian hukum. Situasi ini menciptakan celah hukum di mana pelaku kejahatan dapat bebas demi hukum (*vrijspraak*) apabila unsur berita bohong dan transaksi elektronik gagal dibuktikan secara rigid di pengadilan, meskipun kerugian finansial korban sangat nyata. Ketiadaan pasal yang secara spesifik mengatur tentang manipulasi identitas digital

membuat regulasi yang ada menjadi tumpul dan tidak relevan menghadapi kompleksitas kejahatan berbasis kecerdasan buatan (AI).

Ketiadaan pasal yang secara spesifik mengatur tentang manipulasi identitas digital atau pencurian biometrik membuat regulasi yang ada menjadi tumpul dan tidak relevan dalam menghadapi kompleksitas kejahatan berbasis kecerdasan buatan. Akibat kekosongan hukum ini, memunculkan urgensi penelitian yang mendesak karena bahaya laten dalam sistem peradilan pidana. Terdapat resiko besar bahwa pelaku kejahatan dapat bebas demi hukum apabila unsur-unsur berita bohong dalam konteks transaksi elektronik tidak dapat dibuktikan secara rigid di pengadilan, padahal fakta materiil menunjukkan telah terjadi penipuan yang merugikan korban secara finansial. Situasi ini tidak hanya mencedarai rasa keadilan tetapi juga menciptakan celah bagi pelaku untuk terus mengeksploitasi ketertinggalan kebijakan formulasi hukum pidana yang gagal menangkap esensi kejahatan manipulasi wajah tersebut.

Di sisi lain, Dalam kondisi kekosongan hukum positif tersebut, perspektif Hukum Pidana Islam (*Fiqh Jinayah*) menjadi sangat relevan untuk dikaji sebagai landasan etis dan solutif. Islam memandang fenomena ini melalui kacamata perlindungan substantif *Maqashid Syariah*, yakni perlindungan terhadap akal (*Hifdz Al-Aql*) dari manipulasi yang menyesatkan dan perlindungan harta (*Hifdz Al-Mal*) dari penipuan.(Khatib 2018) Karena belum adanya *nash* spesifik, perbuatan ini diklasifikasikan sebagai *Jarimah Ta'zir*, yang mewajibkan pemerintah (*Ulil Amri*) untuk melakukan pembaruan hukum guna menutup celah kemadharatan .

Keberadaan *Deepfake* meruntuhkan dua sendi perlindungan utama dalam Islam. Pertama, ia mencederai akal (حِفْظُ الْعَقْلِ) melalui distorsi audio-visual yang membuat masyarakat kehilangan orientasi kebenaran. Kedua, ia melanggar perlindungan harta (حِفْظٌ الْمَالِ) karena digunakan sebagai instrumen untuk mengambil hak orang lain secara melawan hukum, atau yang dikenal sebagai اَكْلُ الْاَمْوَالِ بِالْبَاطِلِdalam terminologi Al-Qur'an. Pada konstruksi hukum Islam, karena belum adanya *nash* (dalil) yang spesifik mengatur sanksi bagi kejahatan *Deepfake*, perbuatan ini diklasifikasikan sebagai *Jarimah Takzir*.

Tetapi, belum adanya kodifikasi hukum Islam yang diadopsi secara penuh dalam hukum positif terkait kejahatan siber menciptakan kebutuhan mendesak untuk mengintegrasikan nilai-nilai keadilan Islam ke dalam perbaikan regulasi

nasional. Untuk memposisikan tulisan ini, penulis menggunakan beberapa literatur dari penelitian terdahulu sehingga didapatkan bahwa kajian mengenai kejahatan siber mayoritas masih berkutat pada modus operandi konvensional atau aspek perlindungan korban semata, dan belum menyentuh inti permasalahan manipulasi biometrik.

Literatur terdahulu seperti ditulis oleh A. Mufti Abdul Malik A mahasiswa UIN Sunan Gunung Djati Bandung dalam skripsinya, ia lebih berfokus pada aspek pembuktian dalam transaksi online trandisional tanpa melibatkan elemen kecerdasan buatan, sementara studi lain dari Nur Halizah mahasiswa UIN Raden Fatah Palembang menitikberatkan pada perlindungan hukum bagi korban *Deepfake* tanpa membedah konstruksi delik bagi pelakunya. Disisi lain, kajian mengenai pertanggungjawaban AI, sebagaimana ditulis oleh Robby dalam skripsinya di UIN Maulana Malik Ibrahim Malang, cenderung melihat mesin sebagai subjek hukum melalui teori *vicarious liability*, bukan menempatkan manusia sebagai aktor intelektual yang menyalahgunakan teknologi sebagai instrumen kejahatan (*Instrument of crime*).

Dari literatur tersebut nampak Belum ada penelitian yang secara komprehensif menguji kekosongan hukum akibat ketidakrelevanan Pasal 28 ayat (1) UU ITE terhadap modus *deepfake* bila ditinjau dari perspektif hukum pidana Islam. Maka dari itu, berangkat dari urgensi dan kesenjangan teoretis tersebut penelitian ini bertujuan untuk menganalisis secara mendalam mengapa konstruksi hukum dalam Pasal 28 ayat (1) UU ITE mengalami *over-criminalization* atau pemaksaan makna yang berujung pada kekosongan hukum dalam penanganan *deepfake*. Penelitian ini juga menawarkan perspektif Hukum Pidana Islam sebagai solusi keadilan substantif dalam mengisi kevakuman regulasi tersebut, serta merumuskan bagaimana konsep *Ta'zir* dapat memberikan fleksibilitas bagi hakim dalam memutus perkara kejahatan teknologi baru ini.

Penulis berupaya menemukan titik temu atau rekonsiliasi antara hukum negara dan hukum agama, serta mengidentifikasi bagaimana konsep *Takzir* dalam Islam dapat memberikan fleksibilitas bagi hakim dalam memutus perkara teknologi baru yang belum diatur secara rigid dalam undang-undang. Ketiga, penelitian ini bermaksud menelaah relevansi sanksi pidana yang ada saat ini dengan prinsip keadilan substantif. Apakah ancaman pidana penjara dan denda

dalam UU ITE sudah cukup memenuhi rasa keadilan, ataukah diperlukan formulasi sanksi baru yang lebih adaptif terhadap dampak psikologis dan finansial yang ditimbulkan oleh teknologi AI? Dengan menjawab tujuan-tujuan ini, penelitian diharapkan dapat memberikan kontribusi teoritis bagi pembaharuan hukum pidana nasional dan kontribusi praktis bagi aparat penegak hukum dalam menangani gelombang kejahatan digital di masa depan.

Melalui analisis ini, diharapkan tercipta kontribusi pemikiran yang dapat meluruskan penerapan hukum positif agar tidak terjebak pada pasal yang tidak relevan, serta memberikan landasan etis-religius dalam merespon kejahatan siber di masa depan. Selain itu penelitian ini diharapkan bisa melengkapi penelitian terdahulu yang umumnya berfokus pada beberapa aspek saja tanpa menyentuh inti persoalan mengenai ketidakcocokan konstruksi delik dalam Undang-Undang yang berlaku dengan modus operandi manipulasi biometrik modern yang kini marak terjadi.

## II. Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif dengan spesifikasi deskriptif analitis.(Soekanto dan Mamudji 2015) Inti pembahasan mengarah pada analisis yuridis terkait *vacuum of norm* (kekosongan norma) sehingga menyebabkan ketidaktepatan dalam implementasi Pasal 28 ayat (1) juncto Pasal 45A UU ITE terhadap kejahatan *Deepfake*, serta bagaimana Hukum Pidana Islam memandangnya. Alih-alih mengkaji perilaku masyarakat secara sosiologis, penelitian ini berbasis pada studi data sekunder (kepustakaan). Metode analisisnya dibangun di atas tiga pilar pendekatan: *statute approach* (perundang-undangan), *conceptual approach* (konseptual), dan *comparative approach* (perbandingan) antara hukum negara dan hukum agama.(Marjuki 2017).

Metode pengumpulan data bertumpu pada studi literatur (*library research*) terhadap naskah-naskah hukum. Material hukum yang diolah terdiri dari sumber primer (Al-Qur'an, Hadis, UU ITE), sumber sekunder (kitab *Fiqh Jinayah*, literatur pidana, jurnal), serta sumber tersier (kamus dan berita valid) untuk memperkuat analisis.(Sahir 2021) Selanjutnya, data dianalisis secara kualitatif menggunakan logika deduktif, dimulai dari premis mayor berupa dalil hukum Islam dan UU ITE, dihubungkan dengan fakta kejahatan *Deepfake*, untuk menarik kesimpulan

mengenai konstruksi hukum yang ideal.

## III. Hasil dan Pembahasan

### 3.1. Kekosongan Norma Dalam Pasal 28 Ayat 1 UU ITE

Kemajuan pesat teknologi *Artificial Intelligence* (AI) kini menempatkan diskursus hukum pidana di Indonesia pada titik disrupsi yang fundamental. Fenomena kejahatan siber yang berevolusi dari manipulasi teks menuju manipulasi biometrik melalui teknologi *Deepfake* menuntut adanya respons hukum yang adaptif. Namun, realitas yuridis menunjukkan adanya ketertinggalan hukum atau *legal lag* sebagaimana diteorikan oleh William F. Ogburn, di mana perubahan sosial dan teknologi berlari jauh lebih cepat dibandingkan perubahan regulasi.(Budhijanto 2025)

Hal ini sejalan dengan pandangan Iwan Setiawan dkk dalam kajiannya di *Jurnal Galuh Justisi*, yang menyoroti kompleksitas penanggulangan kejahatan dunia maya. Iwan Setiawan menekankan bahwa *cybercrime* merupakan kejahatan yang memanfaatkan teknologi tinggi dimana batas-batas teritorial dan definisi fisik menjadi kabur (*borderless*). Karakteristik unik ini menuntut adanya instrumen hukum yang spesifik dan dinamis, bukan sekadar memaksakan pasal-pasal konvensional pada fenomena virtual yang terus bermetamorfosis.(Setiawan 2022) Pada konteks penegakan hukum terhadap kasus penipuan *Deepfake* yang mencatut pejabat negara, aparat penegak hukum seringkali merujuk pada Pasal 28 ayat 1 juncto Pasal 45A ayat 1 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Penerapan pasal ini, jika ditelaah menggunakan pendekatan dogmatik hukum dan interpretasi gramatikal, mengandung cacat bawaan yang berpotensi menciptakan kekosongan norma atau *vacuum of norm*. Rumusan delik dalam Pasal 28 ayat (1) UU ITE menitikberatkan pada kriminalisasi perbuatan menyebar kabar bohong secara melawan hukum, di mana unsur konstitutifnya adalah adanya dampak kerugian bagi konsumen dalam aktivitas ekonomi digital. Frasa pertama yang menjadi hambatan yuridis fundamental adalah *menyebarkan berita bohong*. Dalam teori hukum pidana materiil, setiap

unsur delik atau *bestanddeel* harus terpenuhi secara kumulatif. Ketidaktepatan terjadi pada level ontologis dalam mendefinisikan *Deepfake*. Berdasarkan perspektif ilmu komunikasi dan hukum telematika, *Deepfake* yang menggunakan teknologi *Generative Adversarial Networks* (GANs) sejatinya bukan memproduksi berita dalam arti jurnalistik maupun informasi naratif. *Deepfake* adalah fabrikasi realitas visual atau penciptaan sintetik yang melakukan impersonasi terhadap subjek hukum tertentu.(Hamzah 2008)

Edmon Makarim dalam kajian hukum telematika menegaskan bahwa keaslian dokumen elektronik berkaitan erat dengan integritas data. Dalam *Deepfake*, yang terjadi adalah manipulasi integritas biometrik, bukan sekadar penyebaran rumor atau disinformasi tekstual.(Makarim 2010) Memaksakan terminologi *berita bohong* pada video manipulasi wajah pejabat yang meminta transfer dana adalah bentuk *extensive interpretatie* atau penafsiran ekstensif yang berlebihan dan berpotensi melanggar asas legalitas (*nullum crimen sine lege*). Jika Jaksa Penuntut Umum memaksakan dakwaan ini, pembuktian di pengadilan akan menjadi sangat rapuh.

Penasihat hukum terdakwa dapat dengan mudah mematahkan argumen tersebut dengan dalil bahwa kliennya tidak sedang menyebarkan berita, melainkan menciptakan karya seni visual manipulatif atau parodi, terlepas dari niat jahat (*mens rea*) yang menyertainya. Barda Nawawi Arief dalam teori kebijakan hukum pidana mengingatkan bahwa ketidakjelasan perumusan delik dapat menyebabkan *over-criminalization* atau sebaliknya, ketidakmampuan hukum menjangkau perbuatan jahat yang sebenarnya (*under-criminalization*)(Arief 2013). Dalam kasus *Deepfake*, risiko yang terjadi adalah yang kedua, di mana pelaku dapat lolos karena perbuatannya tidak memenuhi unsur berita secara limitatif.

Kelemahan kedua yang lebih fundamental terletak pada frasa *“Mengakibatkan kerugian konsumen dalam Transaksi Elektronik”*. Unsur ini merupakan unsur konstitutif yang membatasi keberlakuan pasal hanya pada ranah perlindungan konsumen. Sutan Remy Sjahdeini dalam analisis kejahatan komputer menyatakan bahwa karakteristik kejahatan siber seringkali melintasi batas-batas definisi konvensional. Definisi konsumen menurut Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan

Konsumen mensyaratkan adanya hubungan pemakaian barang atau jasa yang tersedia dalam masyarakat. Sementara itu, modus operandi *Deepfake* yang marak terjadi, seperti *impersonation* pejabat untuk meminta sumbangan fiktif atau *love scamming*, seringkali tidak terjadi dalam koridor transaksi elektronik komersial.

Korban yang tertipu oleh video *Deepfake* Presiden atau Menteri bukanlah konsumen yang sedang membeli jasa pemerintahan, melainkan warga negara yang diperdaya. Hubungan yang terjadi adalah hubungan sepihak berbasis tipu muslihat, bukan hubungan kontraktual jual-beli. Jika hakim menerapkan asas *lex stricta* dimana hukum harus ditafsirkan secara ketat, maka dakwaan yang menggunakan Pasal 28 ayat 1 UU ITE akan gugur demi hukum karena korban tidak memiliki *legal standing* sebagai konsumen. Hal ini menciptakan celah impunitas bagi pelaku. Dikdik M. Arief Mansur dalam kajian *cyber law* menyoroti bahwa ketergantungan pada pasal-pasal keranjang sampah yang tidak spesifik justru melemahkan sistem peradilan pidana siber di Indonesia.(Mansur dan Gultom 2007)

Kekosongan ini menegaskan bahwa Indonesia belum memiliki regulasi yang secara spesifik mengatur tentang pencurian identitas biometrik (*biometric identity theft*), berbeda dengan Uni Eropa yang telah merancang *AI Act* yang secara spesifik mengatur transparansi konten manipulatif.Sigid Suseno, Yurisdiksi Tindak Pidana Siber (Refika Aditama, 2012).

### 3.2. Manipulasi Biometrik Dalam Hukum Pidana Islam

Di tengah stagnasi dan kebuntuan hukum positif Indonesia, Hukum Pidana Islam atau *Fiqh Jinayah* hadir menawarkan perspektif yang lebih substantif dan berorientasi pada nilai. Islam tidak terpaku pada formalitas istilah berita atau konsumen, melainkan menukik langsung pada esensi kerusakan (*mafsadah*) yang ditimbulkan oleh perbuatan tersebut. Dalam khazanah hukum Islam, *Deepfake* dapat dianalisis melalui pendekatan *Qiyas* atau analogi hukum dan prinsip-prinsip *Maqashid Syariah*.(Qardhawi 2000)

Secara spesifik, perbuatan memanipulasi wajah untuk menipu masuk dalam kategori اَلْغَصُّ atau kecurangan dan اَلتَّدْ لِيسُ atau penipuan. Istilah *At-Tadlis* dalam fiqh muamalah sering digunakan untuk menggambarkan

tindakan penjual yang menyembunyikan cacat barang agar terlihat sempurna. Dalam konteks *Deepfake*, pelaku melakukan *Tadlis* tingkat tinggi ia menyembunyikan identitas aslinya yang cacat sebagai penipu dengan menyelubunginya menggunakan visual digital pejabat yang sempurna, berotoritas, dan dipercaya. Wahbah Az-Zuhaili menegaskan bahwa segala bentuk penipuan yang merugikan pihak lain hukumnya haram dan wajib dikenai sanksi, baik penipuan dalam jual beli maupun dalam interaksi sosial lainnya(Az-Zuhaili 2010).

Selain itu, konsep *Ghash* sangat relevan dengan hadis Nabi Muhammad SAW yang berbunyi: *"Barangsiapa yang menipu kami, maka ia bukan golongan kami"* (HR. Muslim). Para ulama sepakat bahwa larangan ini bersifat umum (*'am*) mencakup segala bentuk manipulasi, baik di dunia nyata maupun dunia maya. Abdul Qadir Audah dalam mahakaryanya *At-Tasyri' Al-Jina'i Al-Islami* menjelaskan bahwa perlindungan harta (حِفْظُ الْمَالِ) adalah salah satu pilar utama hukum pidana Islam (Audah 2014).

Penggunaan Deepfake demi keuntungan materiil adalah pelanggaran berat atas hak kekayaan. Metode akuisisi harta yang didasari pada manipulasi kesadaran korban lewat video palsu ini, menurut hukum Islam, adalah manifestasi dari *Akl al-amwal bil bathil*. Dasar hukum pelarangannya merujuk pada firman Allah dalam QS. Al-Baqarah ayat 188:

وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ وَتُدْلُواْ بِهَآ إِلَى ٱلْحُكَّامِ لِتَأْكُلُواْ فَرِيقًا مِّنْ أَمْوَٰلِ ٱلنَّاسِ بِٱلْإِثْمِ وَأَنتُمْ تَعْلَمُونَ ١٨٨

*“Dan janganlah sebagian kamu memakan harta sebagian yang lain di antara kamu dengan jalan yang batil, dan janganlah kamu membawa (urusan) harta itu kepada hakim, supaya kamu dapat memakan sebahagian daripada harta benda orang lain itu dengan (jalan berbuat) dosa, padahal kamu mengetahui”*

Lebih mendalam lagi, *Deepfake* menyerang aspek *Hifdz Al-Aql* atau perlindungan akal. Islam sangat memuliakan akal manusia dan mewajibkan penjagaannya dari segala sesuatu yang memabukkan atau menyesatkan. Imam Al-Ghazali dalam *Al-Mustasfa* menempatkan perlindungan akal sebagai prioritas dharuriyat (Al-ghazali 2021). Teknologi *Deepfake* bekerja dengan

cara mengacaukan persepsi kognitif dan nalar kritis manusia, membuat akal sulit membedakan antara kebenaran (*haq*) dan kepalsuan (*batil*). Serangan terhadap kemampuan verifikasi akal ini merupakan kejahatan intelektual yang dampaknya bisa lebih destruktif daripada penipuan fisik biasa, karena merusak kepercayaan sosial (*social trust*). Oleh karena itu, dalam pandangan Islam, bobot kejahatan *Deepfake* sangat berat karena ia merusak dua sendi sekaligus yakni harta dan akal (Amrani dan Ali 2015).

Mengingat *Deepfake* adalah kejahatan kontemporer (مُسْتَفِيْدَة) yang belum ada di zaman Rasulullah SAW, maka tidak ditemukan sanksi *Had* atau hukuman pasti yang spesifik untuknya. Perbuatan ini tidak memenuhi syarat *Sariqah* atau pencurian yang mewajibkan potong tangan karena tidak ada pengambilan harta dari tempat penyimpanannya (*hirz*) secara fisik-sembunyi, melainkan melalui transfer sukarela yang didasari tipu daya. Oleh karena itu, konsensus ulama mengkategorikan kejahatan siber semacam ini sebagai *Jarimah Ta'zir*.

Jarimah *Ta'zir* didefinisikan sebagai kategori delik di mana penentuan bentuk serta bobot sanksinya tidak ditetapkan secara baku oleh nash, melainkan menjadi hak prerogatif penguasa ( أُولِي الْأَمْرِ) atau majelis hakim. Fleksibilitas ini adalah kekuatan hukum Islam untuk beradaptasi dengan perkembangan zaman. Ibn Taimiyah dalam *As-Siyasah As-Syari'iyyah* menekankan bahwa tujuan utama hukuman *Ta'zir* adalah *Ta'dib* atau pendidikan dan *Az-Zajr* atau pencegahan.(Ali 2012)

Mengingat dampak *Deepfake* yang masif dan merusak, hakim memiliki wewenang untuk menjatuhkan hukuman *Ta'zir* yang sangat berat, yang bisa melebihi hukuman *Hudud* jika kemaslahatan menuntut demikian. Hukuman tersebut bisa berupa penjara dalam waktu lama, denda finansial yang memiskinkan pelaku, hingga hukuman publikasi nama pelaku untuk sanksi sosial. Di sinilah peran vital pemerintah dalam koridor *Siyasah Syari'iyyah* atau politik hukum Islam. Adanya kekosongan hukum positif dalam UU ITE adalah sebuah *Dharar* atau bahaya bagi umat. Kaidah Fiqh menyebutkan:

تَصَرُّفُ الْإِمَامِ عَلَى الرَّعِيَّةِ مَنُوطٌ بِالْمَصْلَحَةِ

*“kebijakan pemimpin terhadap rakyatnya harus berorientasi pada kemaslahatan.”* (As-Suyuthi 2018)

Membiarkan celah hukum ini berlarut-larut sama dengan membiarkan rakyat terus menjadi korban. Oleh karena itu, berdasarkan prinsip

الضَّرَرُ يُزَال

*"Segala bentuk kemadharatan harus dihilangkan"*(Mubarok dan Faizal 2004)

Ijtihad legislasi ini dapat berupa revisi UU ITE dengan memasukkan pasal spesifik tentang manipulasi biometrik, atau penerbitan Peraturan Mahkamah Agung (PERMA) yang memberikan pedoman bagi hakim untuk menafsirkan Pasal 35 UU ITE secara progresif agar dapat menjangkau kasus *Deepfake*. Merujuk pada teori penemuan hukum yang dikemukakan Sudikno Mertokusumo, tugas hakim melampaui sekadar menjadi corong peraturan perundang-undangan. Hakim diharuskan peka dan mampu menggali norma-norma yang hidup dalam realitas sosial untuk menghadirkan keadilan substantif. Dalam konteks Indonesia yang relijius, nilai-nilai *Maqashid Syariah* yang melindungi akal dan harta dapat diadopsi oleh hakim sebagai pertimbangan sosiologis dan filosofis untuk memberatkan hukuman bagi pelaku *Deepfake*, mengisi kekosongan rasa keadilan yang gagal dipenuhi oleh teks undang-undang yang kaku.

### 3.3. Urgensi Pembaruan Hukum Pidana Siber

Analisis terhadap kekosongan hukum ini tidak lengkap tanpa meninjau aspek viktimologi atau perlindungan korban. Dalam konstruksi Pasal 28 ayat 1 UU ITE saat ini, posisi korban sangat lemah. Jika unsur konsumen tidak terbukti, maka status korban dalam persidangan menjadi kabur, yang berdampak pada hak-hak restitusi atau ganti rugi. Muladi dalam kapita selekta hukum pidana menegaskan bahwa sistem peradilan pidana modern harus bergeser dari orientasi retributif atau pembalasan terhadap pelaku menuju restoratif atau pemulihan korban.(Muladi 2002)

Ketiadaan pasal spesifik tentang *Deepfake* membuat korban kesulitan menuntut ganti rugi atas kerugian imateriil, seperti rusaknya reputasi atau trauma psikologis akibat manipulasi wajah. Dalam hukum Islam, hak korban (*Haqqul Adami*) sangat dihormati. Pelaku *Ta'zir* tidak hanya dihukum badan oleh negara, tetapi juga wajib mengganti kerugian finansial yang dialami

korban (*Dhaman*). Integrasi konsep perlindungan korban dari hukum Islam ini perlu diserap ke dalam pembaruan hukum nasional.

Perbandingan dengan instrumen hukum internasional menunjukkan betapa mendesaknya pembaruan ini. Uni Eropa melalui *Artificial Intelligence Act* telah menetapkan kewajiban transparansi yang ketat bagi penyedia sistem AI yang menghasilkan konten *Deepfake*. Pelanggaran terhadapnya dikenai denda administratif yang besar. Sementara di Amerika Serikat, terdapat *Deepfakes Accountability Act* yang mewajibkan *watermarking* pada konten manipulasi. Indonesia, melalui revisi UU ITE tahun 2024, belum menyentuh aspek ini secara detail. Ahmad M. Ramli mencatat bahwa konvergensi hukum telematika global menuntut harmonisasi regulasi (Ramli 2021).

Ketertinggalan Indonesia menjadikan netizen Indonesia rentan menjadi objek eksploitasi kejahatan transnasional. Oleh karena itu, urgensi pembaruan hukum pidana siber bukan sekadar wacana akademis, melainkan kebutuhan mendesak untuk menjaga kedaulatan digital dan keamanan warga negara. Pemerintah perlu merumuskan delik baru yang secara spesifik mengkriminalisasi Pencurian dan Manipulasi Identitas Biometrik tanpa bergantung pada unsur transaksi elektronik atau berita bohong. Delik ini harus dirumuskan sebagai delik formil, di mana perbuatan memanipulasi itu sendiri sudah dapat dipidana tanpa menunggu timbulnya kerugian, sebagai langkah preventif (*Sadd ad-Dzari'ah*) untuk menutup jalan menuju kejahatan yang lebih besar.(Ali 2022)

## IV. Kesimpulan dan Saran

### 4.1. Kesimpulan

Hasil kajian yang telah diuraikan, dapat ditarik kesimpulan bahwa kerangka regulasi nasional saat ini tengah menghadapi persoalan serius berupa ketiadaan norma hukum (*vacuum of norm*) yang nyata. Pasal 28 ayat (1) *juncto* Pasal 45A UU ITE Nomor 1 Tahun 2024 terbukti memiliki ketidakrelevanan yuridis (*irrelevant*) ketika dipaksakan untuk menjerat kejahatan *Deepfake*. Unsur-unsur dalam pasal tersebut, yakni menyebarkan berita bohong dan kerugian konsumen dalam transaksi elektronik, gagal menjangkau esensi kejahatan *Deepfake* yang sejatinya merupakan fabrikasi

realitas sintetik dan pencurian identitas biometrik, bukan sekadar aktivitas jurnalistik ataupun sengketa dagang *e-commerce*. Pemaksaan penerapan pasal ini mengakibatkan *legal lag* dan ketidakpastian hukum, yang berpotensi membebaskan pelaku dari jerat pidana karena unsur delik tidak terpenuhi secara limitatif. Pada tinjauan *Fiqh Jinayah*, kejahatan *Deepfake* diklasifikasikan sebagai tindakan *Al-Ghash* (kecurangan) dan *At-Tadlis* (penipuan) tingkat tinggi. Perbuatan ini secara nyata melanggar dua prinsip utama *Maqashid Syariah*, yaitu perlindungan terhadap akal (*Hifdz Al-Aql*) karena memanipulasi kebenaran, serta perlindungan terhadap harta (*Hifdz Al-Mal*) karena mengambil aset korban secara batil (*akl al-amwal bil bathil*). Mengingat belum adanya *nash* yang spesifik mengatur teknologi ini, maka perbuatan tersebut masuk dalam kategori *Jarimah Ta'zir*. Oleh karena itu, konsep *Ta'zir* dalam Hukum Pidana Islam hadir sebagai solusi integratif yang memberikan fleksibilitas bagi hakim dan penguasa (*Ulil Amri*) untuk menetapkan sanksi berat demi kemaslahatan umum dan menutup celah kerusakan (*Sadd ad-Dzari'ah*). Ketiadaan aturan spesifik dalam hukum positif mewajibkan negara melakukan ijtihad legislasi untuk menghilangkan kemadharatan (*Adh-Dhararu Yuzal*), sehingga keadilan substantif dapat ditegakkan melampaui sekadar keadilan prosedural teks undang-undang yang kaku.

### 4.2. Saran

Pertama, urgensi pembaruan hukum menuntut lembaga legislatif untuk segera merevisi UU ITE atau mengintegrasikan delik khusus dalam Rancangan Undang-Undang Kecerdasan Buatan yang secara eksplisit mengkriminalisasi pencurian dan manipulasi identitas biometrik. Perumusan norma baru ini harus melepaskan ketergantungan pada unsur berita bohong dan kerugian konsumen yang selama ini menjadi hambatan yuridis, dan menggantinya dengan konstruksi delik formil yang menitikberatkan pada perbuatan fabrikasi realitas sintetik itu sendiri. Langkah legislasi ini sangat krusial dan sejalan dengan prinsip *Sadd ad-Dzari'ah* dalam hukum Islam, yakni sebagai upaya preventif hukum untuk menutup celah kerusakan atau mafsadah yang lebih besar sebelum meluas dan merugikan masyarakat.

Kedua, dalam ranah penegakan hukum praktis, aparat penegak hukum

dan yudikatif disarankan untuk tidak terpaku pada interpretasi tekstual Pasal 28 ayat 1 UU ITE yang memiliki keterbatasan unsur. Jaksa Penuntut Umum dan Hakim perlu menerapkan penemuan hukum atau rechtsvinding dengan menggunakan dakwaan alternatif atau kumulatif yang menekankan pada aspek tipu muslihat dan rangkaian kebohongan agar lebih relevan dengan modus deepfake. Dalam perspektif Fiqh Jinayah, hakim didorong menggunakan kewenangan diskresionernya untuk menjatuhkan sanksi Ta'zir maksimal yang berorientasi pada perlindungan akal dan harta. Pendekatan ini bertujuan agar putusan pengadilan tidak hanya memenuhi formalitas undang-undang, tetapi juga mewujudkan keadilan substantif serta memberikan efek jera yang nyata bagi pelaku kejahatan berbasis teknologi.

## Daftar Pustaka

### A. Buku

Al-ghazali, Imam. 2021. *Al-Mustashfa: Rujukan Utama Ushul Fikih*. Jakarta: Pustaka Al-Kautsar.

Ali, Mahrus. 2022. *Dasar-Dasar Huum Pidana*. Jakarta: Sinar Grafika.

Ali, Zainudin. 2012. *Hukum Pidana Islam*. Jakarta: Sinar Grafika.

Amrani, Hanafi, dan Mahrus Ali. 2015. *Sistem Pertanggung Jawaban Pidana*. Cetakan 1. Jakarta: Rajawali Pers.

Arief, Barda Nawawi. 2013. *Kapita Selekta Hukum Pidana*. Bandung: Citra Aditya Bakti.

As-Suyuthi, Imam Jalaluddin. 2018. *As-Suyuthi, Jalaluddin. Al-Asybah wa An-Nazhair. Beirut: Dar Al-Kutub Al-Ilmiyah, 1983. Terjemahan oleh Munirul Abidin, Al-Asybah Wan Nazhair: Kaidah-Kaidah Fiqih Mazhab Syafii.* Jakarta: Pustaka Al-Kautsar.

Audah, Abdul Qadir. 2014. *Ensiklopedia Hukum Pidana Islam (At-Tasyri' al-Jina'i al-Islami)*. Jilid 1. Bogor: Kharisma Ilmu.

Az-Zuhaili, Wahbah. 2010. *Fiqih Islam Wa Adillatuhu*. Jilid 5. Depok: Gema Insani.

Budhijanto, Danrivanto. 2025. *Hukum Cybercrime 4.0 : Kejahatan Digital dan Artificial Intelligence (AI)*. Bandung: PT Refika Aditama.

Hamzah, Andi. 2008. *Azas-Azas Hukum Pidana*. Jakarta: Rineke Cipta.

Makarim, Edmon. 2010. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: Rajawali Pers.

Mansur, Dikdik M. Arief, dan Elisatris Gultom. 2007. *Urgensi Perlindungan Korban Kejahatan Antara Norma dan Realita*. Bandung: Raja Grafindo Persada.

Marjuki, Peter. 2017. *Penelitian Hukum (Edisi Revisi)*. Jakarta: Kencana Prenada media.

Mubarok, Jaih, dan Enceng Arif Faizal. 2004. *Kaidah Fiqh Jinayah (Asas-asas hukum pidana Islam)*. Cetakan Pertama. Bandung: Pustaka Bani Quraisy.

Muladi. 2002. *Hak Asasi Manusia, Politik dan Sistem Peradilan Pidana*. Semarang: Badan Penerbit Universitas Diponegoro.

Qardhawi, Yusuf. 2000. *Fiqh Prioritas*. Jakarta: Robbani Press.

Ramli, Ahmad M. 2021. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama.

Sahir, Syafrida Hafni. 2021. *Metodologi Penelitian*. Yogyakarta: Penerbit KBM Indonesia

Soekanto, Soerjono, dan Sri Mamudji. 2015. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers.

Suseno, Sigid. 2012. *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama.

**B. Peraturan Perundang-Undangan**

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

**C. Jurnal**

Khatib, Suansar. 2018. "Konsep Maqashid Al-Syari`Ah: Perbandingan Antara Pemikiran Al-Ghazali Dan Al-Syathibi." *Jurnal MIZANI: Wacana Hukum, Ekonomi dan Keagamaan IAIN Bengkulu* 5 (.1). http://dx.doi.org/10.29300/mzn.v5i1.1436

Ruhtiani, Maya, dan Istikharoh. 2025. "Hukum Pidana Dan Hak Cipta Di Era Kecerdasan Artifisial: Analisis Pertanggungjawaban Dalam Hukum Positif Dan Hukum Islam." *Jurnal Al Wasith: Jurnal Studi Hukum Islam* 10 (1):63. https://doi.org/10.52802/wst.v10i1.1463

Setiawan, Iwan dkk. 2022. "Jejak Digital Sebagai Alat Bukti Petunjuk Menurut Pasal 184 Kitab Undang Undang Hukum Acara Pidana. *Jurnal Ilmiah Galuh Justisi*. 10 (1).119–132. http://dx.doi.org/10.25157/justisi.v10i1.7236

**Sumber Lain**

Detikcom, Tim. 2025. *Babak Baru Perkara Deepfake Catut Prabowo*. Jakarta. https://news.detik.com/berita/d-7884867/babak-baru-perkara-deepfake-catut-prabowo

Trust, Team. 2025. "Deepfake & AI Voice Cloning: Penipuan Digital Semakin Canggih." *Dtrust*. Diambil 1 September 2025 https://resources.dtrust.co.id/blog/deepfake-voice-penipuan-digital/