Journal of Authentic Research
https://journal-center.litpam.com/index.php/jar/index

December 2025 Vol. 4, No. 2
e-ISSN: 2828-3724
pp. 2656-2669

Perlindungan Konsumen Terhadap Ancaman Deepfake dalam Transaksi Digital: Tinjauan Regulasi dan Urgensi Mitigasi

[1*]Zaenul Haq

[1]STIS Harsyi Lombok Tengah
*Corresponding Author e-mail: zaenulhaq@gmail.com
Received: October 2025; Revised: Desember 2025; Published: Desember 2025

Abstrak

Deepfake, atau konten sintetis yang sangat realistis dan sulit dibedakan dari aslinya, telah muncul sebagai hasil dari kemajuan teknologi Kecerdasan Buatan (AI). Penyalahgunaan deepfake menimbulkan risiko serius terhadap perlindungan konsumen, seperti penipuan identitas, manipulasi persetujuan, dan serangan phishing yang semakin canggih dalam transaksi digital dan layanan keuangan. Fenomena ini sangat penting secara sosial dan ekonomi di tengah percepatan transformasi digital di Indonesia. Ini karena dapat menghambat inklusi keuangan dan mengurangi kepercayaan masyarakat terhadap ekosistem ekonomi digital. Tujuan dari penelitian ini adalah untuk mengevaluasi ancaman hukum dan potensi bahaya bagi konsumen yang terkait dengan deepfake, serta untuk mengevaluasi kekuatan undang-undang yang ada di Indonesia, terutama Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Penelitian ini menggunakan metode yuridis normatif, yang didukung oleh analisis deskriptif tentang pola penyalahgunaan deepfake di industri keuangan digital dan analisis komparatif terbatas terhadap yurisdiksi lain. Hasil penelitian menunjukkan bahwa terdapat kekosongan norma terkait pencegahan dan pemulihan kerugian konsumen, meskipun peraturan saat ini dapat menjerat pelaku. Oleh karena itu, untuk menciptakan ekosistem transaksi digital yang aman dan terpercaya, regulasi harus diperkuat, dan kolaborasi lintas sektor diperlukan untuk mengurangi risiko.

Kata kunci: Deepfake, Undang-undang Perlindungan Konsumen, Transaksi Digital

Consumer Protection Against Deepfake Threats in Digital Transactions: Regulatory Review and the Urgency of Mitigation

Abstract

Deepfakes, or highly realistic synthetic content that is difficult to distinguish from the original, have emerged as a result of advances in Artificial Intelligence (AI) technology. The misuse of deepfakes poses serious risks to consumer protection, such as identity fraud, consent manipulation, and increasingly sophisticated phishing attacks in digital transactions and financial services. This phenomenon is of significant social and economic importance amidst the acceleration of digital transformation in Indonesia. This is because it can hamper financial inclusion and undermine public trust in the digital economy ecosystem. The purpose of this study is to assess the legal threats and potential harms to consumers associated with deepfakes, as well as to assess the strength of existing laws in Indonesia, particularly the Personal Data Protection Law (PDP Law) and the Information and Electronic Transactions Law (ITE Law). This study uses a normative juridical method, supported by a descriptive analysis of deepfake abuse patterns in the digital finance industry and a limited comparative analysis with other jurisdictions. The results indicate a gap in norms related to the prevention and redress of consumer losses, despite current regulations that can prosecute perpetrators. Therefore, to create a safe and trusted digital transaction ecosystem, regulations must be strengthened, and cross-sector collaboration is needed to mitigate risks.

Keywords: *Deepfake, Consumer Protection Act, Digital Transactions.*

How to Cite: Haq, Z. (2025). Perlindungan Konsumen Terhadap Ancaman Deepfake dalam Transaksi Digital: Tinjauan Regulasi dan Urgensi Mitigasi. *Journal of Authentic Research*, *4*(2), 2656–2669. https://doi.org/10.36312/m4xwcw14

https://doi.org/10.36312/m4xwcw14

PENDAHULUAN

Era digital telah membawa kemudahan yang tak terhindarkan dalam bertransaksi, mulai dari perbankan online, pinjaman daring, hingga investasi. Namun, seiring dengan kemajuan tersebut, muncul pula bentuk-bentuk kejahatan siber baru yang semakin canggih, salah satunya adalah penyalahgunaan teknologi deepfake. Deepfake (gabungan dari deep learning dan fake) memungkinkan pelaku kejahatan untuk meniru wajah dan suara seseorang dengan tingkat akurasi yang tinggi, menjadikannya alat yang sangat efektif untuk melakukan penipuan identitas dalam transaksi keuangan digital. Deepfake adalah teknik yang memanfaatkan AI untuk membuat, menggabungkan, atau memodifikasi gambar, video, atau audio sehingga tampak seperti asli, padahal merupakan hasil rekayasa. Kemampuan deepfake untuk meniru wajah dan suara individu dengan sangat meyakinkan telah menimbulkan kekhawatiran terkait penyalahgunaannya dalam berbagai bentuk kejahatan siber, termasuk penipuan, pencemaran nama baik, dan penyebaran informasi palsu (Respati *et al*., 2024).

Menurut berbagai laporan riset terbaru, jumlah konten deepfake terus melesat secara eksponensial, dari sekitar 500.000 file di 2023 menjadi proyeksi lebih dari 8 juta di akhir 2025 meningkat sekitar 900% secara tahunan yang mencerminkan percepatan penggunaan teknologi ini di berbagai domain digital, termasuk sektor keuangan. Kasus deepfake kini diperkirakan menyumbang sekitar 6–7% dari seluruh upaya penipuan identitas yang tercatat secara global, dengan lonjakan insiden terutama di wilayah Amerika Utara dan Asia-Pasifik (APAC) mencapai ribuan persen dalam beberapa tahun terakhir. Di APAC sendiri, insiden deepfake dilaporkan meningkat lebih dari 1.500%, menjadi salah satu kawasan dengan pertumbuhan tertinggi di dunia dalam ancaman ini. Pelaku kejahatan juga memanfaatkan fraud as a service dan alat otomatis lain yang mempermudah pembuatan deepfake secara murah dan cepat, sehingga meningkatkan skala ancaman bagi konsumen dan institusi keuangan (Sofia Ramirez, 2025).

Di banyak negara, pelaku kejahatan telah meraup kerugian finansial besar dari modus deepfake ini. Misalnya, kasus penipuan deepfake video conference di Hong Kong menyebabkan kerugian sekitar US$25 juta pada sebuah perusahaan global, di mana pelaku meniru identitas pimpinan perusahaan untuk memerintahkan transfer dana sekaligus menipu staf internal (Cheng Leng & Chan Ho Him, 2024).

Dalam konteks Indonesia, tantangan keamanan siber semakin nyata seiring dengan penetrasi internet yang tinggi dan transformasi digital sektor finansial. Indonesia mencatat peningkatan dalam kerangka keamanan siber, di mana survei PwC Digital Trust Insights 2026 menunjukkan bahwa investasi risiko siber berada di antara prioritas tinggi para pemimpin bisnis di dalam negeri, bahkan melampaui rata-rata kawasan Asia Pacific dan global (PwC, 2025).

Menurut National Cyber Security Index *(NCSI)* terbaru, skor indeks keamanan siber Indonesia mencapai sekitar 63,6 poin, menempatkan negara ini pada peringkat ke-49 dari lebih 170 negara di dunia dan posisi kelima di kawasan ASEAN. Skor tersebut mencerminkan perkembangan signifikan namun masih menunjukkan adanya ruang perbaikan terutama pada aspek pengembangan kebijakan dan kesiapan menghadapi ancaman siber yang semakin kompleks (Infobank, 2024).

Tingkat literasi digital di Indonesia juga mengalami peningkatan, dengan indeks nasional digital literacy mencapai skor 3,54 pada 2022 (skala berbagai pilar literasi

termasuk keamanan digital), namun kapasitas literasi keamanan siber masyarakat masih menjadi titik lemah yang perlu diperkuat agar konsumen dapat lebih waspada terhadap modus penipuan seperti *deepfake* (Antara News, 2022).

Meskipun memiliki manfaat dalam industri kreatif, deepfake juga menghadirkan tantangan baru dalam dunia kejahatan siber (cybercrime) seperti ancaman terhadap penipuan identitas, pencemaran nama baik, pemerasan, penyebaran disinformasi, dan manipulasi politik (Haida & Nuriyatman, 2024).

Karena berfokus pada integritas identitas dan persetujuan otentikasi, ancaman deepfake menjadi sangat penting dalam hal perlindungan konsumen. Konsumen yang bertransaksi secara digital, terutama yang mengandalkan verifikasi biometrik atau komunikasi suara/visual dengan layanan pelanggan, berpotensi menjadi korban penipuan yang dapat menyebabkan kerugian finansial yang signifikan. Contoh kasus di banyak negara, termasuk di Asia, menunjukkan kerugian uang ratusan miliar rupiah yang disebabkan oleh penipuan deepfake yang berhasil menembus sistem keamanan lembaga keuangan.

Di Indonesia, kasus penyalahgunaan teknologi deepfake semakin marak. Salah satu insiden yang mencuri perhatian publik adalah penipuan yang melibatkan penggunaan deepfake wajah Presiden Prabowo Subianto. Pelaku menggunakan teknologi ini untuk membuat video palsu yang menampilkan Presiden Prabowo menawarkan bantuan pemerintah, namun dengan syarat korban harus mentransfer sejumlah uang terlebih dahulu. Kasus ini berhasil diungkap oleh Direktorat Tindak Pidana Siber Bareskrim Polri, dengan pelaku berinisial AMA ditangkap di Lampung Tengah pada Januari 2025 (Hukmana, 2025).

Modus operandi yang digunakan dalam kasus tersebut menunjukkan bagaimana teknologi deepfake dapat dimanfaatkan untuk menipu masyarakat dengan cara yang semakin canggih. Pelaku tidak hanya menggunakan wajah Presiden Prabowo, tetapi juga Wakil Presiden Gibran Rakabuming Raka dan Menteri Keuangan Sri Mulyani, untuk meyakinkan korban bahwa tawaran bantuan tersebut sah. Akibatnya, lebih dari 100 orang dari 20 provinsi menjadi korban, dengan total kerugian mencapai Rp 65 juta (Meilina, 2025).

Fenomena ini menyoroti urgensi pengaturan hukum yang lebih spesifik terkait penyalahgunaan teknologi deepfake di Indonesia. Saat ini, kerangka hukum yang ada belum secara komprehensif mengatur tentang deepfake, sehingga penegakan hukum terhadap pelaku seringkali menghadapi kendala. Maka dari itu diperlukan pembaruan dalam undang-undang yang ada atau bahkan pembentukan regulasi baru yang secara khusus mengatur tentang deepfake dan implikasinya (Wahyudi, 2025).

Pendidikan dan peningkatan kesadaran masyarakat juga memainkan peran penting dalam upaya pencegahan. Masyarakat perlu dibekali dengan pengetahuan tentang apa itu deepfake, bagaimana cara kerjanya, serta potensi bahayanya. Dengan demikian, individu dapat lebih waspada dan kritis terhadap konten yang mereka temui di media sosial atau platform digital lainnya, sehingga tidak mudah terperdaya oleh modus penipuan yang memanfaatkan teknologi ini (Respati et al., 2024).

Di Indonesia, undang-undang seperti UU PDP dan UU ITE memungkinkan hukuman untuk pemalsuan dan penyalahgunaan data elektronik. Namun, karena deepfake merupakan fenomena teknologi yang relatif baru dengan modus operandi tertentu, sangat penting untuk menilai kekuatan undang-undang saat ini dan

merekomendasikan solusi proaktif untuk menguranginya. Artikel ini akan membahas secara menyeluruh ancaman deepfake terhadap konsumen dalam transaksi digital dan menganalisis peran dan masalah yang dihadapi oleh undang-undang di Indonesia.

Berdasarkan uraian di atas, penelitian ini dirumuskan dalam masalah-masalah utama berikut:

1. Aspek Hukum: Apakah regulasi yang ada di Indonesia termasuk Undang-Undang Perlindungan Data Pribadi (UU PDP), UU Informasi dan Transaksi Elektronik (UU ITE), dan peraturan sektoral keuangan cukup memadai untuk mengatur dan menindak penyalahgunaan teknologi deepfake dalam transaksi keuangan digital? Di mana letak kekosongan hukum dan tantangan dalam penegakan hukum terhadap pelaku yang memanfaatkan deepfake?
2. Aspek Teknologi dan Keamanan: Sejauh mana sistem keamanan di sektor keuangan Indonesia mampu mendeteksi, mencegah, dan merespons ancaman dan insiden deepfake yang semakin kompleks? Bagaimana efektivitas adopsi teknologi deteksi dan mitigasi *AI* dalam infrastruktur keamanan informasi lembaga keuangan?
3. Aspek Edukasi dan Literasi Digital: Seberapa efektif tingkat literasi digital masyarakat Indonesia mengenai risiko keamanan siber, terutama pengetahuan tentang deepfake dan teknik pengenalan penipuan digital? Apa peran pendidikan konsumen dan program literasi digital dalam mengurangi kerentanan konsumen terhadap modus penipuan ini?

Penelitian ini memiliki tujuan operasional sebagai berikut:

1. Menganalisis regulasi yang berlaku di Indonesia terkait deepfake dan identifikasi celah hukum yang menghambat perlindungan konsumen serta penindakan pelaku, termasuk rekomendasi perbaikan dan harmonisasi kebijakan yang lebih eksplisit menangani deepfake.
2. Mengevaluasi kesiapan teknologi dan sistem keamanan di sektor keuangan untuk mendeteksi serta mengantisipasi ancaman deepfake, dan mengidentifikasi praktik terbaik atau teknologi mitigasi yang dapat diadaptasi lembaga keuangan.
3. Mengukur tingkat literasi dan kesadaran digital masyarakat mengenai ancaman deepfake, khususnya pemahaman tentang risiko keamanan siber dalam transaksi digital, serta merekomendasikan strategi edukasi yang lebih efektif untuk meningkatkan ketahanan konsumen terhadap penipuan semacam ini.

Dengan struktur rumusan masalah dan tujuan operasional yang jelas tersebut, penelitian ini akan membahas secara komprehensif ancaman deepfake dalam konteks transaksi digital, serta mengevaluasi peran, tantangan, dan arah kebijakan yang perlu diambil di Indonesia.

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah yuridis normatif yaitu pendekatan yang berfokus pada norma dan asas hukum dengan mengandalkan sumber-sumber kepustakaan serta peraturan perundang-undangan yang didukung oleh analisis deskriptif tentang pola penyalahgunaan deepfake di industri keuangan digital dan analisis komparatif terbatas terhadap yurisdiksi lain.

Dalam penelitian ini, digunakan berbagai jenis bahan hukum, termasuk bahan hukum primer, seperti peraturan perundang-undangan dan bahan hukum sekunder,

seperti buku, jurnal, dan literatur terkait serta bahan hukum tersier, seperti kamus, ensiklopedia, dan sumber referensi lainnya dengan mengkaji regulasi yang terkait dengan objek penelitian yang sedang menjadi fokus yang dikaji untuk selanjutnya dibenturkan dengan realita yang ada di lapangan. Dengan menggunakan penelitian ini diharapkan dapat ditemukan hasil yang yang sesuai dengan apa menjadi tujuan daripada penelitian di atas. Penelitian ini menggunakan pendekatan yuridis **normatif**, yaitu penelitian hukum yang berfokus pada kajian terhadap norma, asas, dan sistem hukum yang berlaku dengan menempatkan hukum sebagai kaidah. Pendekatan ini dipilih karena tujuan utama penelitian adalah menganalisis kecukupan dan relevansi regulasi dalam menghadapi penyalahgunaan teknologi deepfake dalam transaksi keuangan digital, serta merumuskan rekomendasi normatif bagi penguatan perlindungan konsumen. Oleh karena itu, pendekatan empiris atau sosiologis yang menitikberatkan pada perilaku masyarakat atau praktik lapangan tidak menjadi fokus utama dalam penelitian ini.

Jenis penelitian yang digunakan adalah penelitian kepustakaan (library research). Pengumpulan bahan hukum dilakukan melalui penelusuran sistematis terhadap sumber-sumber hukum yang relevan. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan teknologi informasi, perlindungan data pribadi, dan transaksi keuangan digital, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta peraturan sektoral yang dikeluarkan oleh otoritas terkait. Bahan hukum sekunder terdiri atas buku teks hukum, artikel jurnal ilmiah, hasil penelitian terdahulu, dan publikasi akademik yang membahas kejahatan siber, deepfake, kecerdasan buatan, serta perlindungan konsumen digital. Adapun bahan hukum tersier digunakan sebagai penunjang, berupa kamus hukum, ensiklopedia, dan sumber referensi lain yang relevan untuk memperjelas konsep dan terminologi hukum.

Seleksi bahan hukum sekunder dilakukan berdasarkan kriteria:

1. relevansi substansial dengan isu penyalahgunaan deepfake dan transaksi keuangan digital;
2. kredibilitas dan otoritas akademik penulis atau lembaga penerbit;
3. aktualitas sumber untuk menangkap perkembangan teknologi dan regulasi terkini; serta
4. kontribusi analitis terhadap pengembangan argumentasi hukum dalam penelitian. Dengan kriteria tersebut, bahan hukum yang digunakan diharapkan mampu memberikan landasan teoritis dan normatif yang kuat.

Analisis bahan hukum dilakukan secara kualitatif dengan metode deskriptif-analitis, yaitu dengan mengkaji dan menafsirkan ketentuan hukum yang relevan untuk mengidentifikasi ruang lingkup pengaturan, potensi kekosongan hukum, serta tantangan dalam penerapannya. Selain itu, penelitian ini juga menggunakan pendekatan komparatif **terbatas** dengan menelaah praktik pengaturan atau kebijakan di beberapa yurisdiksi lain sebagai bahan perbandingan, guna memperkaya perspektif dan memberikan alternatif rekomendasi kebijakan bagi Indonesia.

Penelitian ini memiliki beberapa keterbatasan, antara lain tidak digunakannya data primer berupa wawancara atau survei terhadap pemangku kepentingan, seperti regulator, lembaga keuangan, maupun korban penipuan deepfake. Akibatnya, analisis mengenai implementasi dan efektivitas regulasi lebih bertumpu pada sumber

sekunder dan laporan terdokumentasi. Oleh karena itu, hasil penelitian ini bersifat normatif-konseptual dan diharapkan dapat menjadi dasar bagi penelitian lanjutan dengan pendekatan empiris untuk melengkapi temuan yang diperoleh.

HASIL DAN PEMBAHASAN

Ancaman Deepfake dalam Transaksi Digital

Deepfake menghadirkan dimensi baru dalam risiko transaksi digital, melampaui metode penipuan konvensional seperti *phishing* email atau SMS. Ancaman utamanya berpusat pada tiga aspek:

1. Penipuan Identitas (*Identity Fraud*)
   Kecerdasan buatan terus mengalami kemajuan besar. Semakin banyak produk dan layanan yang mengintegrasikan teknologi ini menunjukkan hal ini. Ini adalah kemajuan yang sangat menguntungkan karena AI memiliki kemampuan untuk meningkatkan efisiensi dalam berbagai bidang. Selain itu, menggunakannya membuat banyak pekerjaan lebih mudah. Dengan teknologi ini, siapa saja sekarang dapat melakukan pekerjaan yang sebelumnya membutuhkan keahlian khusus. Teknologi ini dapat memahami dan menganalisis data secara cepat dan akurat berkat kemampuan untuk menjalankan model dan algoritma canggih. Oleh karena itu, kecerdasan buatan telah mengubah cara kita berkomunikasi dan bekerja, dan melakukan hal-hal yang sebelumnya hanya dapat dilakukan oleh manusia.
   Sebaliknya, berbagai keuntungan dan kemudahan yang dihasilkan oleh penerapan kecerdasan buatan juga dapat disalahgunakan untuk tujuan yang tidak baik, seperti penggunaan deepfake dalam penipuan. Pelaku kejahatan siber semakin sering menggunakan teknologi deepfake sebagai alat untuk melakukan aksi mereka. Deepfake membuat video atau audio terlihat seperti asli, tetapi sebenarnya dibuat dengan kecerdasan buatan (AI) (Kristiyenda *et al*., 2025).
   Kasus penipuan yang melibatkan deepfake semakin meningkat, dengan pelaku memanfaatkan teknologi ini untuk menipu korban dengan cara yang lebih meyakinkan. Salah satu contohnya adalah penggunaan wajah tokoh publik untuk menyebarkan informasi palsu demi keuntungan pribadi (H. J. Salim, 2025).
2. Manipulasi Persetujuan dan Otorisasi
   Berulang kali, konfirmasi suara atau video diperlukan sebagai bukti otorisasi. Pelaku deepfake dapat meniru pelanggan, memberikan petunjuk untuk transfer dana, atau menyetujui kontrak investasi yang tidak masuk akal. Konsumen menjadi lebih waspada karena sulit untuk membedakan arahan layanan keuangan asli dari manipulasi deepfake, yang dapat menyebabkan kerugian langsung.
3. Rusaknya Kepercayaan Konsumen dan Penghambatan Inklusi Keuangan
   Penipuan deepfake mengancam korban dan seluruh ekosistem keuangan digital. Karena masyarakat enggan menggunakan layanan yang dianggap tidak aman, keraguan ini dapat menghambat adopsi teknologi keuangan baru dan mengurangi upaya pemerintah untuk mendorong inklusi keuangan.

Kerangka Hukum dan Tantangan Regulasi di Indonesia

Meskipun belum ada regulasi yang secara eksplisit menyebut istilah "deepfake", terdapat beberapa undang-undang yang dapat digunakan sebagai landasan hukum dalam menangani kasus penyalahgunaan teknologi ini:

1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

   UU PDP berfungsi sebagai alat preventif utama. Jika seseorang membuat data pribadi palsu, Artikel 66 melarang dan mengancam pidana. Data pribadi yang dilindungi mencakup data wajah dan suara yang digunakan dalam pembuatan deepfake. Kerangka hukum ini memungkinkan konsumen untuk menuntut kompensasi atas penyalahgunaan data biometrik. Pasal 66 UU PDP secara tegas melarang seseorang untuk membuat atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau merugikan orang lain. Data wajah dan suara yang direkayasa melalui teknologi deepfake dapat diklasifikasikan secara yuridis sebagai data pribadi spesifik, yang berarti mereka harus dilindungi dengan ketat.

   Dalam hal sanksi, UU PDP mengatur ancaman pidana penjara yang relatif besar dan denda. Namun, masih ada beberapa masalah yang menghalangi sanksi tersebut untuk berhasil menjerat pelaku deepfake. Pertama, UU PDP belum secara eksplisit mengatur tanggung jawab pelaku tidak langsung, seperti penyedia platform atau pengembang teknologi, yang dalam praktiknya dapat melakukan apa yang disebut sebagai "membuat data pribadi palsu". Kedua, rumusan delik dalam UU PDP masih bersifat umum dan teknologi-netral, sehingga pembuktian pelanggaran sangat bergantung pada kemampuan penegak hukum untuk membuktikan adanya perbuatan "membuat data pribadi palsu" dan hubungan langsung antara penggunaan Akibatnya, meskipun sanksi yang diatur cukup ketat, mereka masih efektif hanya untuk pelaku utama dan belum sepenuhnya menggambarkan kompleksitas ekosistem kejahatan deepfake.
2. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

   Tidak diizinkan untuk membuat, mengubah, atau menghilangkan Dokumen Elektronik dan/atau Informasi Elektronik dengan tujuan agar informasi tersebut dianggap sebagai data asli, menurut Pasal 35 UU ITE. Ini mungkin berlaku untuk mereka yang melakukan deepfake yang mencoba memalsukan transaksi atau identitas digital. UU ITE, khususnya Pasal 35, melarang setiap orang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, atau penghilangan Dokumen Elektronik dan/atau Informasi Elektronik dengan tujuan agar informasi tersebut dianggap sebagai data asli. Mereka yang menggunakan identitas digital, rekaman suara, atau visual untuk menipu pelanggan dalam transaksi keuangan dapat dikenakan ketentuan ini secara normatif.

   Karena disertai dengan ancaman pidana penjara dan denda yang relatif tinggi, UU ITE memberikan alat represif yang cukup kuat dari segi efektivitas sanksi. Namun demikian, masih ada hambatan interpretasi untuk menerapkan Pasal 35 terhadap kejahatan deepfake. Karena standar tersebut tidak secara eksplisit mengantisipasi kecerdasan buatan generatif, deepfake sering dianggap sebagai bentuk manipulasi data elektronik biasa. Kondisi ini dapat menyebabkan perdebatan hukum, terutama dalam membuktikan unsur kesengajaan dan tujuan untuk membuat informasi dianggap asli, terutama ketika pelaku menggunakan sistem otomatis atau jaringan lintas negara.

   Secara umum, baik UU PDP maupun UU ITE telah menyediakan kerangka hukuman yang dapat diterapkan untuk menjerat pelaku kejahatan deepfake.

Sanksi tersebut, bagaimanapun, masih bersifat parsial dan mungkin berubah-ubah karena tidak dimaksudkan untuk menangani fitur deepfake yang berbasis kecerdasan buatan, berskala lintas batas, dan sulit dideteksi. Oleh karena itu, untuk memastikan bahwa sanksi saat ini tidak hanya bersifat simbolik, tetapi juga efektif dalam memberikan efek jera dan perlindungan hukum bagi konsumen, diperlukan penguatan regulasi melalui penafsiran progresif, pembentukan pedoman penegakan hukum, atau bahkan penetapan standar khusus yang secara eksplisit mengatur deepfake.

Tantangan Regulasi dan Urgensi Mitigasi

Meskipun tersedia kerangka hukum, terdapat tantangan signifikan:

1. Kekosongan Peraturan Spesifik: Tidak adanya pasal yang secara eksplisit mengatur deepfake membuat pembuktian lebih sulit bagi penegak hukum. Kejahatan berbasis AI seperti deepfake membutuhkan mekanisme deteksi dan pembuktian digital khusus.
2. Sifat Lintas Batas: Deepfake seringkali melibatkan sindikat kejahatan siber lintas negara, yang membuat proses hukum dan ekstradisi lebih sulit.
3. Beban Pembuktian Konsumen: Ketika terjadi kerugian, konsumen seringkali dikenakan biaya untuk membuktikan bahwa transaksi yang terjadi bukanlah hasil dari deepfake sebuah proses yang sangat mahal dan kompleks secara teknologi.

Untuk memperkuat perlindungan konsumen dari ancaman deepfake, diperlukan langkah-langkah proaktif dan kolaboratif dari regulator, industri, dan masyarakat.

1. Peran Otoritas Jasa Keuangan (OJK)

   Sebagai regulator industri jasa keuangan dan pelindung konsumen, OJK memainkan peran penting. OJK harus menetapkan regulasi yang mewajibkan penyedia jasa keuangan (PJK) untuk menerapkan teknologi deteksi deepfake yang canggih (seperti verifikasi multimodal dan deteksi liveness) dalam proses onboarding dan otentikasi transaksi. Selain itu, OJK harus meningkatkan peran Pusat Anti-Scam Indonesia (IASC), yang berfungsi untuk melaporkan dan memblokir rekening yang terkait dengan penipuan deepfake.

2. Peningkatan Standar Teknologi Keamanan Industri

   Industri keuangan harus beralih ke verifikasi berbasis tunggal (verifikasi satu faktor) ke verifikasi berlapis (verifikasi berbagai faktor), dan solusi anti-deepfake berbasis AI yang dapat mendeteksi manipulasi audio atau visual secara real-time. Sangat penting bagi perusahaan teknologi identitas digital (GovTech/FinTech) untuk bekerja sama untuk membangun Deepfake Shield atau teknologi pelindung yang lebih responsif.

   Pemerintah perlu bekerja sama dengan ahli teknologi, akademisi, serta sektor industri dalam mengembangkan alat deteksi deepfake yang dapat digunakan oleh aparat penegak hukum dan masyarakat umum (Fadillah et al., 2025).

   Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber (RUU KKS) memiliki peran penting dalam membangun sistem pertahanan siber nasional yang kuat terhadap ancaman teknologi deepfake dalam hal keamanan siber. RUU KKS bertujuan untuk meningkatkan kemampuan negara untuk melawan serangan siber dan penyebaran informasi palsu yang dapat mengancam stabilitas sosial, politik, dan ekonomi. Karena deepfake telah banyak digunakan dalam kampanye disinformasi politik di dalam dan luar negeri, peraturan ini semakin penting, terutama menjelang pemilu dan peristiwa politik lainnya yang

signifikan. RUU KKS harus mengatur pencegahan dan penindakan penyalahgunaan deepfake, termasuk kolaborasi dengan platform digital untuk menemukan dan menghapus konten yang terbukti merugikan masyarakat.

RUU KKS harus memberikan pedoman bagi institusi pemerintah dalam menangani ancaman deepfake, termasuk dengan membentuk pusat deteksi deepfake nasional untuk mengawasi dan menangani penyebaran konten deepfake yang berpotensi membahayakan kepentingan nasional. Selain itu, RUU KKS harus memastikan bahwa alat ini dapat diakses secara luas, memiliki tingkat akurasi tinggi, dan dapat membedakan konten deepfake yang berbahaya dari manipulasi digital yang sah (Kristiyenda et al., 2025).

3. Edukasi dan Literasi Konsumen

Pendidikan adalah pertahanan pertama. Kampanye literasi digital harus ditingkatkan untuk memberi tahu orang-orang tentang tanda-tanda deepfake, seperti gerakan bibir yang tidak sinkron, pencahayaan aneh, atau kualitas suara yang buruk. Mereka juga harus memberi tahu orang-orang tentang pentingnya tidak membagikan data biometrik atau melakukan transaksi sensitif tanpa verifikasi lintas kanal yang ketat.

Edukasi masyarakat memegang peranan penting dalam mencegah penipuan yang memanfaatkan teknologi deepfake. Dengan pemahaman yang baik mengenai cara kerja dan ciri-ciri konten deepfake, masyarakat dapat lebih waspada dan kritis terhadap informasi yang diterima. Salah satu langkah yang penting adalah meningkatkan literasi digital, sehingga individu mampu mengenali tanda-tanda manipulasi dalam konten multimedia (Fauzi *et al*., 2023).

Pemerintah dan lembaga terkait perlu menginisiasi program sosialisasi yang menyasar berbagai lapisan masyarakat. Program ini dapat berupa seminar, workshop, atau kampanye melalui media sosial yang menjelaskan bahaya deepfake dan cara mengidentifikasinya. Dengan demikian, masyarakat akan lebih siap menghadapi ancaman penipuan yang semakin canggih dan tidak mudah terperdaya oleh konten palsu yang beredar (Jufri & Putra, 2021).

Selain itu, kolaborasi antara sektor pendidikan dan teknologi juga penting dalam upaya mencegah tindakan kriminal berbasis deepfake. Jika materi tentang keamanan digital dan deteksi deepfake dimasukkan ke dalam kurikulum sekolah, itu dapat membekali generasi muda dengan kemampuan yang diperlukan untuk menghadapi tantangan di era digital. Mengajarkan siswa bagaimana teknologi kecerdasan buatan digunakan dalam deepfake dan bagaimana mengidentifikasi manipulasi digital dapat meningkatkan kesadaran dan kewaspadaan masyarakat. Oleh karena itu, orang tidak hanya menggunakan teknologi tetapi juga memahami bagaimana mereka dapat menyalahgunakannya.

Metode ini memastikan bahwa orang belajar tentang ancaman deepfake sejak kecil, membuat masyarakat lebih tahan terhadap penipuan digital. Pelatihan literasi digital bagi masyarakat luas juga diperlukan, termasuk kampanye kesadaran publik yang melibatkan sektor swasta, komunitas, dan media sosial. Kerja sama antara pemerintah, lembaga pendidikan, dan perusahaan teknologi dalam menyediakan alat dan sumber daya untuk mendeteksi deepfake dapat meningkatkan ekosistem keamanan digital. Upaya yang terorganisir dan berkelanjutan dapat menurunkan kemungkinan penyebaran konten manipulatif berbasis deepfake, melindungi masyarakat dari dampak buruk kejahatan siber (Kristiyenda *et al*., 2025).

Platform media sosial dan perusahaan teknologi juga memiliki tanggung jawab dalam mengedukasi pengguna mereka. Dengan menyediakan alat dan sumber daya yang membantu pengguna mengenali dan melaporkan konten deepfake, platform dapat berkontribusi dalam mengurangi penyebaran informasi palsu. Langkah proaktif ini tidak hanya melindungi pengguna, tetapi juga menjaga integritas ekosistem digital secara keseluruhan (Banfatin *et al*., 2024).

Pendidikan dan literasi digital adalah garis pertahanan pertama dalam menghadapi ancaman deepfake. Untuk menjadikan kempanye literasi digital lebih efektif, kampanye harus meningkatkan pencahayaan yang tidak wajar, distorsi visual, ketidaksinkronan gerakan bibir, dan kualitas suara yang tidak konsisten. Pendidikan juga harus menekankan pentingnya perlindungan data biometrik dan penerapan verifikasi lintas kanal juga dikenal sebagai verifikasi multi-channel sebelum melakukan transaksi keuangan sensitif. Konsumen sangat rentan terhadap penipuan berbasis rekayasa identitas digital jika mereka tidak memahami dasar ini.

Namun demikian, ada kelangkaan aturan yang signifikan dalam upaya pendidikan tersebut. Di Indonesia, undang-undang belum secara eksplisit menetapkan bahwa perusahaan atau platform teknologi harus menerapkan program literasi deepfake untuk melindungi konsumen digital. Indonesia masih menggunakan pendekatan fragmentaris yang tersebar dalam UU ITE, UU PDP, dan kebijakan sektoral. Ini berbeda dengan beberapa negara lain, seperti Uni Eropa, yang menggunakan peraturan berbasis risiko dalam UU AI, yang mewajibkan transparansi konten hasil kecerdasan buatan dan penandaan (labeling) konten sintetis. Ada perbedaan hukum dalam pencegahan dini dan pembagian tanggung jawab antar aktor karena kondisi norma khusus ini.

Tidak boleh diabaikan bahwa Indonesia menghadapi masalah dengan deteksi deepfake dalam hal penggunaan teknologi. Untuk mengimbangi perkembangan teknik deepfake, teknologi pendeteksi deepfake berbasis kecerdasan buatan membutuhkan infrastruktur komputasi yang kuat, dataset yang besar dan representatif, serta pembaruan algoritma yang berkelanjutan. Di Indonesia, penerapan sistem deteksi real-time belum merata karena banyak lembaga keuangan dan lembaga publik menghadapi keterbatasan sumber daya teknis dan anggaran. Selain itu, ancaman falsifikasi positif dalam sistem deteksi juga dapat menyebabkan ancaman hukum baru, seperti penolakan transaksi yang sah atau pelanggaran hak konsumen. Pada akhirnya, hal ini memerlukan kerangka akuntabilitas yang jelas.

Dalam situasi seperti ini, keterlibatan sektor swasta sangat penting untuk rencana mitigasi berbasis tanggung jawab bersama. Bank dan lembaga keuangan tidak hanya harus mematuhi prinsip kehati-hatian (prinsip kehati-hatian), tetapi juga harus memasukkan teknologi autentikasi berlapis, seperti deteksi kehidupan, analisis perilaku transaksi, dan pengawasan fraud yang digerakkan oleh kecerdasan buatan. Sementara itu, platform media sosial dan perusahaan teknologi harus menerapkan sistem moderasi konten, sistem pelaporan, dan teknologi yang digerakkan oleh kecerdasan buatan untuk mendeteksi indikasi deepfake. Metode ini menegaskan bahwa perlindungan konsumen digital memerlukan kerja sama lintas sektor daripada semata-mata negara atau individu.

Pembentukan Pusat Anti Penipuan Indonesia atau Indonesia Anti Scam Centre (IASC) merupakan langkah awal yang positif di Indonesia untuk menangani meningkatnya kejahatan siber, termasuk penipuan berbasis deepfake. IASC bertanggung jawab untuk mengkoordinasikan pelaporan, memblokir rekening, dan menangani penipuan dengan cepat. Namun, IASC masih tidak efektif dalam hal deepfake. Saat ini, mekanisme IASC belum sepenuhnya terintegrasi dengan sistem deteksi deepfake berbasis teknologi atau basis data lintas platform. Itu juga lebih sensitif terhadap laporan penipuan konvensional. Selain itu, respons yang cepat dan menyeluruh juga terhambat oleh kurangnya kewajiban hukum bagi platform digital dan penyedia layanan keuangan untuk berbagi data secara real-time dengan IASC.

Oleh karena itu, diperlukan penyempurnaan dan penguatan mandat IASC agar ia dapat berfungsi sebagai pusat pengaduan dan pusat intelijen penipuan nasional yang terhubung dengan bank, platform digital, dan aparat penegak hukum nasional. Penguatan ini dapat mencakup laporan insiden deepfake, interoperabilitas sistem deteksi, dan pembuatan protokol yang khusus menangani penipuan berbasis AI. Mitigasi ancaman deepfake dapat dilakukan secara lebih efisien dan berkelanjutan dengan menggunakan pendekatan yang terkoordinasi, berbasis regulasi yang jelas, dan didukung oleh teknologi dan edukasi publik.

KESIMPULAN

Tindakan komprehensif diperlukan untuk menangani ancaman deepfake terhadap perlindungan konsumen dalam transaksi digital. Meskipun UU PDP dan UU ITE memberikan dasar hukum, ada peraturan khusus, standar keamanan industri yang lebih ketat, dan kesadaran konsumen yang tinggi. Kolaborasi antara otoritas (OJK) dan masyarakat dapat memperkuat ekosistem transaksi digital di Indonesia untuk mencegah kecerdasan buatan mengubah identitas. Ini akan melindungi uang konsumen.

Oleh karena itu, untuk mengatasi ancaman deepfake, peraturan yang lebih ketat diperlukan serta peningkatan literasi digital masyarakat. Pemerintah, lembaga penegak hukum, dan platform media sosial harus bekerja sama untuk menemukan, mencegah, dan menangani konten deepfake yang merugikan. Untuk mengurangi dampak negatif deepfake, masyarakat juga harus dididik tentang artinya. Ini akan meningkatkan kritik mereka dan mencegah mereka tertipu oleh berita palsu.

Selain itu, dari perspektif penegakan hukum, undang-undang harus menetapkan sanksi yang tegas dan proporsional bagi mereka yang menyalahgunakan teknologi deepfake untuk tujuan yang melanggar hukum. Hukuman pidana yang tegas diperlukan untuk penipuan berbasis deepfake, yaitu ketika seseorang menggunakan identitas palsu untuk melakukan tindak pidana. Pelaku tidak hanya harus menjalani hukuman penjara, tetapi juga harus dikenakan denda yang signifikan dan bertanggung jawab untuk memulihkan reputasi korban. Exploitasi seksual digital melalui penggunaan deepfake, seperti membuat konten pornografi tanpa izin korban, juga harus dikategorikan sebagai kejahatan serius dan harus dihukum setimpal dengan dampak psikologis dan sosial yang ditimbulkannya.

Tindakan kebijakan yang komprehensif, terukur, dan lintas sektor diperlukan untuk menangani ancaman deepfake yang membahayakan perlindungan konsumen dalam transaksi digital. Regulasi yang lebih khusus, fleksibel, dan berbasis risiko

diperlukan untuk kemajuan teknologi kecerdasan buatan, meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah memberikan dasar hukum yang umum. Kerangka hukum saat ini dapat tertinggal jika tidak ada intervensi kebijakan yang jelas. Ini karena ancaman deepfake sangat cepat, tersebar luas, dan sulit dideteksi.

Pemerintah harus membuat undang-undang nasional khusus untuk mengelola dan mengurangi risiko deepfake. Ini setidaknya harus mencakup:

1. Definisi hukum deepfake dan konten sintetis berbasis kecerdasan buatan;
2. Kewajiban untuk transparan dan menandai (labeling) konten sintetis;
3. Meningkatkan sanksi administratif dan pidana sesuai dengan kerugian dan dampak sosial; dan
4. Mengatur tanggung jawab aktor dalam ekosistem digital, termasuk pengembang teknologi dan platform distribusi.

Metode ini bertujuan untuk menutup kelangkaan peraturan sekaligus memberikan kepastian hukum kepada penegak hukum, pelaku usaha, dan konsumen.

Selain itu, pemerintah harus meningkatkan tanggung jawab kelembagaan dan kerja sama lintas sektor, terutama dengan memasukkan penanganan deepfake ke dalam kebijakan keamanan siber dan perlindungan konsumen digital nasional. Peningkatan jumlah insiden penipuan berbasis identitas digital, peningkatan kecepatan respons penanganan kasus, dan peningkatan tingkat kepercayaan publik terhadap sistem transaksi digital adalah semua indikator keberhasilan kebijakan yang dapat diukur.

Untuk memulai penerapan teknologi deteksi deepfake di sektor jasa keuangan, Otoritas Jasa Keuangan (OJK) memerlukan garis besar kebijakan yang jelas dan bertahap. Garis besar ini dapat mencakup:

1. Tahap jangka pendek: pembuatan pedoman teknis mengenai risiko deepfake dalam proses know your customer, autentikasi transaksi, dan layanan pelanggan digital.
2. Tahap jangka menengah: penerapan standar verifikasi multimodal, seperti kombinasi biometrik dan wajar.
3. Tahap jangka panjang: berbagi intelijen ancaman antar lembaga keuangan dan otoritas pengawas dan penggabungan sistem deteksi deepfake berbasis kecerdasan buatan secara real time.

Rekomendasi ini menuntut bank dan lembaga keuangan untuk beralih dari pendekatan keamanan reaktif ke pendekatan proaktif dan preventif. Pendekatan preventif ini harus diukur dengan indikator kinerja seperti tingkat keberhasilan deteksi penipuan, penurunan kerugian finansial, dan kepuasan pelanggan. Agar inklusi keuangan digital tidak terhambat, OJK harus memastikan bahwa standar tersebut diterapkan secara merata.

Dari sudut pandang penegakan hukum, undang-undang harus menetapkan sanksi yang tegas, proporsional, dan berfokus pada pemulihan korban bagi mereka yang melakukan penyalahgunaan deepfake. Penipuan berbasis deepfake yang memalsukan identitas untuk tujuan kriminal harus dianggap sebagai kejahatan serius yang melibatkan sanksi pidana penjara, denda yang signifikan, serta kewajiban untuk membayar ganti rugi kepada korban dan memperbaiki reputasinya. Metode ini

sangat penting untuk menjamin bahwa sanksi tidak hanya represif tetapi juga memiliki efek jera dan restoratif keadilan.

Untuk penelitian lebih lanjut, disarankan untuk menggunakan metodologi empiris atau socio-legal, antara lain melalui wawancara dengan regulator, penegak hukum, lembaga keuangan, dan korban deepfake. Untuk melengkapi temuan normatif penelitian ini, juga diperlukan studi kuantitatif mengenai seberapa efektif teknologi deteksi deepfake dan seberapa tinggi literasi digital masyarakat. Perumusan kebijakan yang lebih kontekstual dan aplikatif akan diperkuat dengan pendekatan multidisipliner yang menggabungkan ilmu sosial, teknologi, dan hukum.

Pada akhirnya, tidak mungkin untuk membangun ketahanan digital nasional secara sektoral atau parsial. Untuk menghadapi ancaman deepfake, perlu ada kerja sama antara pemerintah, sektor industri dan keuangan, akademisi, dan masyarakat sipil. Masyarakat berfungsi sebagai pengguna dan pengawas ekosistem digital, pemerintah mengawasi kebijakan, sektor swasta mengembangkan dan menerapkan teknologi, dan akademisi memberikan pengetahuan. Upaya mitigasi deepfake berisiko tidak efektif dan terfragmentasi jika keempat komponen tidak bekerja sama. Oleh karena itu, strategi utama untuk membangun ekosistem transaksi digital yang aman, terpercaya, dan berkelanjutan di Indonesia adalah penguatan kerjasama semua pihak.

REFERENSI

Antara (2023). Indonesia's Digital Literacy Index Climbed To 3.54 In 2022. *Antaranews.Com*

Banfatin, P. M., Medan, K. K., & Fallo, D. F. N. (2024). Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi artificial intelligence deepfake dalam melakukan tindak pidana cybercrime. Pemuliaan Keadilan, 2(1), 60–73.

Cheng, L., & Chan, H.H. (2024). Arup Lost $25mn in Hongkong Deepfake Video Conference Scam. *Financial Times.com.*

Fadillah, M. F., Nazar, & Setiawan, H. (2025). Dampak teknologi deepfake terhadap kepercayaan publik dan penyebaran informasi di media sosial. *ResearchGate*.

Fauzi, A. M., Wahyuni, A. T., Chintia, G., Nenci, I. S., Nurwahidah, N., & Sari, P. N. (2023). Edukasi pencegahan penipuan online berbasis sosial media di Desa Mekarwangi. *Jurnal Pengabdian Kepada Masyarakat*, *3*(2), 60–73.

Haida, R. S. N., & Nuriyatman, E. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (AI) Dari Perspektif Hukum Pidana Indonesia. *Jurnal Hukum Respublica*, *24*(1), 2–3.

Hukmana, S. Y. (2025). Penipuan dengan AI deepfake wajah Prabowo, warga tertipu tawaran bantuan pemerintah. *Media Indonesia*.

Infobankstore. (2024). Keamanan Siber Indonesia Peringkat Ke-5 di Asean, di bawah Malaysia dan filipina. *Infobankstore.Com*

Jufri, M. A. A., & Putra, A. K. (2021). Aspek hukum internasional dalam pemanfaatan deepfake technology terhadap perlindungan data pribadi. *Uti Possidetis: Journal of International Law*, *1*(31–57).

Kristiyenda, Y. S., Faradila, J., & Basanova, C. (2025). Pencegahan Kejahatan *Deepfak*e: Studi Kasus terhadap Modus Penipuan *Deepfake* Prabowo Subianto dalam Tawaran Bantuan Uang. *Jurnal Politik, Sosial, Hukum dan Humaniora*. 3(2).

Meilina, K. (2025). Penipuan bansos pakai AI wajah Prabowo, ratusan korban rugi puluhan juta. *Katadata.Co.Id*.

Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi deepfake di Indonesia sebagai bentuk pelindungan negara. *Jurnal USM Law Review*, *7*(2).

Octavia, S., & Prabowo, D. (2025). Wajah hingga suara Gibran dan Sri Mulyani ikut dicatut untuk tipu korban via video "deepfake." *Kompas.Com*.

Patikasari, T. (2024). *Pelindungan hukum bagi korban deepfake pornografi (studi perbandingan Indonesia dan Korea Selatan)*. UIN Syarif Hidayatullah Jakarta.

PwC (2025). Indonesia Prioritises Cyber Readiness, Says Pwc's Digital Trust Insights 2026. *PwC.Com*

Rahman, A. N. F., Syarifudin., & Bari, F. (2025). Perlindungan Hukum terhadap Penyalahgunaan Teknik Deep. *Jurnal Perspektif Administrasi Publik dan Hukum*. 2(1).

Respati, A. A., Setyarini, A. D., Parlagutan, D., Rafli, M., Mahendra, R. S., & Nugroho, A. A. (2024). Analisis hukum terhadap pencegahan kasus deepfake serta perlindungan hukum terhadap korban. *Media Hukum Indonesia (MHI)*, *2*(2), 586.

Rifauddin, M., & Halida, A. N. (2018). Waspada cybercrime dan informasi hoax pada media sosial facebook. *Khizanah Al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, *6*(2).

Salim, H. J. (2025). Pelaku penipuan deepfake AI Prabowo ditangkap, begini modus kejahatannya. *Liputan6.Com.*

Salim, M. P. (2024). Apa Itu Deepfake? Pahami Cara Kerja,Kontroversi Penyalahgunaannya, Serta Regulasi Penggunaannya. *Liputan6.Com.*

Setiarma, A. (2023). Disrupsi Teknologi Hukum Terhadap Jasa Advokat Dalam Pandangan Hukum Pembangunan Mochtar Kusumaatmadja: The Disruption of Legal Technology to the Advocates Services in the Perspective of Mochtar Kusumaatmadja's Legal Development. *Reformasi Hukum*, *27*(2), 88.

Sofia, R. (2025). Deepfake Statistics 2025 : The Hidden Cyber Threat. *SQ Magazine*.

Wahyudi, B. R. (2025). Tantangan penegakan hukum terhadap kejahatan berbasis teknologi AI. *Innovative: Journal of Social Science Research*, *5*(1), 3436–3450.