SIMULASI RISIKO SIBER DAN VERIFIKASI DIGITAL:
ex-ante regulatory sandbox OJK-Komdigi guna menanggulangi penipuan deepfake perbankan

Oleh: **Mitan Tennagi Putri Prawira**[1,*]

[1] *Universitas Negeri Jakarta, Jl. Rawamangun Muka Raya, Kec. Pulo Gadung, Kota Jakarta Timur, Jakarta 13220, Indonesia*

email: mitannagi@gmail.com

Informasi Artikel Received: 07-08-2026 **Accepted:** 25-10-2026

ABSTRAK

Penipuan berbasis kecerdasan buatan generatif, khususnya melalui manipulasi wajah, suara, dan video (deepfake), menimbulkan tantangan serius terhadap keandalan verifikasi biometrik pada sektor perbankan Indonesia. Penelitian ini bertujuan menganalisis keterbatasan kerangka hukum yang masih berorientasi ex-post serta merumuskan desain pengawasan preventif melalui pendekatan Ex-Ante Regulatory Sandbox yang melibatkan Otoritas Jasa Keuangan dan Kementerian Komunikasi dan Digital. Penelitian menggunakan metode hukum sosio-legal dengan pendekatan perundang-undangan, konseptual, perbandingan, dan kebijakan publik. Bahan penelitian meliputi peraturan perundang-undangan, regulasi OJK, dokumen kebijakan, standar teknis autentikasi konten, laporan regulator, serta penelitian terdahulu mengenai bukti digital dan deepfake. Hasil penelitian menunjukkan bahwa ketidaktersediaan kewajiban pengujian risiko, penilaian legalitas algoritma, dan standar autentikasi konten sebelum teknologi generatif dipasarkan menciptakan celah pengawasan pada titik hulu. Penelitian ini mengusulkan empat tahap, yaitu pra-registrasi, simulasi risiko cyber-fraud, penerapan digital watermarking dan metadata provenans, serta pemantauan berkelanjutan. Kerangka tersebut memberikan dasar bagi penguatan perlindungan konsumen, integritas sistem keuangan, dan kepastian hukum tanpa menghambat inovasi teknologi.

Kata kunci: *regulatory sandbox, deepfake, bukti elektronik, verifikasi digital, kecerdasan buatan*

ABSTRACT

Generative artificial intelligence, particularly the manipulation of faces, voices, and videos through deepfake technology, poses a serious challenge to the reliability of biometric verification in Indonesia's banking sector. This study examines the limitations of Indonesia's predominantly ex-post cyber-law framework and proposes a preventive oversight model through an Ex-Ante Regulatory Sandbox jointly administered by the Financial Services Authority and the Ministry of Communication and Digital Affairs. The study employs socio-legal research using statutory, conceptual, comparative, and public-policy approaches. Its materials consist of legislation, Financial Services Authority regulations, policy documents, technical standards on content authentication, regulatory reports, and previous studies on digital evidence and deepfakes. The findings demonstrate that the absence of mandatory risk testing, algorithmic legality assessment, and pre-market content-authentication standards creates a significant upstream regulatory gap. This study proposes four stages: mandatory pre-registration, cyber-fraud risk simulation, implementation of digital watermarking and provenance metadata, and continuous post-registration monitoring. The proposed framework may strengthen consumer protection, financial-system integrity, and legal certainty while preserving a proportionate pathway for technological innovation. It also clarifies the evidentiary value of authenticated digital content by connecting technical provenance, chain of custody, expert examination, and judicial assessment.

Keywords: *regulatory sandbox, deepfake, electronic evidence, digital verification, artificial intelligence*

PENDAHULUAN

Kecerdasan buatan generatif telah memperluas kemampuan produksi dan manipulasi konten digital, termasuk wajah, suara, dan video manusia. Dalam sektor perbankan, perkembangan tersebut relevan karena proses pembukaan rekening, autentikasi transaksi, dan electronic know-your-customer (e-KYC) semakin mengandalkan verifikasi biometrik jarak jauh. Ketergantungan pada satu atau beberapa faktor biometrik dapat meningkatkan risiko apabila sistem tidak dilengkapi dengan pengujian liveness, pemeriksaan anomali, serta mekanisme verifikasi silang yang memadai (Otoritas Jasa Keuangan, 2024; International AI Safety Report, 2025).

Urgensi persoalan tersebut terlihat dari laporan mengenai peningkatan penipuan digital dan kerugian sektor keuangan Indonesia. Indonesia Anti-Scam Centre dan Otoritas Jasa Keuangan mencatat tingginya jumlah laporan penipuan serta nilai kerugian yang mencapai triliunan rupiah dalam periode 2024–2025 (Otoritas Jasa Keuangan dan Indonesia Anti-Scam Centre, 2026; SWA.co.id, 2026). Data mengenai kerugian lebih dari Rp700 miliar pada sektor keuangan dan peningkatan penipuan berbasis kecerdasan buatan juga diberitakan oleh sumber industri dan media (detikInet, 2025; Asatu News, 2026). Data tersebut digunakan secara hati-hati karena cakupan laporan tidak selalu memisahkan kasus deepfake dari seluruh jenis penipuan digital.

Masalah hukum yang muncul tidak hanya berkaitan dengan kemampuan mendeteksi konten palsu, tetapi juga dengan status konten tersebut sebagai alat bukti. Bukti elektronik yang berupa rekaman suara, gambar, video, pesan elektronik, atau data biometrik harus dapat dikaitkan dengan sumber, waktu pembuatan, proses penyimpanan, serta pihak yang menguasai dan memeriksanya. Tanpa autentikasi yang memadai, bukti elektronik berpotensi kehilangan nilai pembuktian karena pihak lawan dapat menyangkal asal-usul, integritas, atau konteks pembuatannya (Undang-Undang Nomor 1 Tahun 2024).

Kerangka hukum Indonesia telah mengakui informasi dan dokumen elektronik sebagai alat bukti hukum yang sah, terutama melalui Undang-Undang Informasi dan Transaksi Elektronik. Pengaturan tersebut diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan berbagai regulasi sektoral mengenai keamanan informasi serta perlindungan konsumen. Meskipun demikian, pengakuan terhadap bukti elektronik belum sepenuhnya disertai standar operasional yang seragam mengenai autentikasi konten sintetis, pemeriksaan metadata, validasi tanda tangan digital, pengujian hash value, dan pembuktian kesinambungan penguasaan barang bukti (Undang-Undang Nomor 27 Tahun 2022).

Penelitian terdahulu telah membahas regulatory sandbox, tata kelola kecerdasan buatan, dan penggunaan bukti elektronik. Kajian Center for Indonesian Policy Studies berfokus pada desain regulatory sandbox bagi industri teknologi finansial dan menekankan pentingnya kepastian tata kelola serta koordinasi antarlembaga (CIPS, 2023). Penelitian mengenai regulatory sandbox pada sektor kesehatan menunjukkan bahwa ruang uji coba dapat dirancang melalui kerja sama antara regulator umum dan kementerian teknis (Andrianto, 2024; National Center for Biotechnology Information, 2024). Penelitian mengenai bukti digital berbasis deepfake menyoroti pentingnya metadata, nilai hash, pemeriksaan perangkat, validasi ahli, dan pencatatan akses

terhadap barang bukti (AI-Based Deepfake Verification Protocols for Legal Evidence, 2026).

Berbeda dari penelitian terdahulu, penelitian ini menghubungkan tiga isu secara terpadu. Pertama, penelitian ini menganalisis risiko deepfake terhadap verifikasi biometrik perbankan. Kedua, penelitian ini mengkaji konsekuensi hukum kelemahan autentikasi terhadap admissibility dan kekuatan pembuktian bukti elektronik. Ketiga, penelitian ini merumuskan desain Ex-Ante Regulatory Sandbox kolaboratif antara OJK dan Komdigi yang menguji kemampuan produk kecerdasan buatan generatif untuk mencegah penyalahgunaan terhadap sistem keuangan.

Autentikasi merupakan proses untuk menunjukkan bahwa suatu bukti elektronik benar berasal dari sumber yang diklaim, dibuat atau diterima pada waktu tertentu, serta tidak mengalami perubahan material sejak pertama kali diperoleh. Autentikasi tidak sama dengan pembuktian kebenaran materiil seluruh isi bukti. Autentikasi menjawab pertanyaan awal mengenai identitas, asal, proses perolehan, dan keutuhan bukti.

Parameter autentikasi meliputi identitas perangkat atau sistem, identitas pihak yang membuat atau menerima bukti, waktu pembuatan, metadata, kesesuaian antara berkas asli dan salinan, nilai hash, tanda tangan digital, catatan pemindahan, serta keterangan ahli. Untuk konten yang diduga dihasilkan atau dimanipulasi AI, autentikasi harus dilengkapi pengujian forensik karena penilaian visual manusia tidak cukup untuk memastikan keaslian.

Integritas menunjukkan bahwa bukti tidak mengalami perubahan, penghapusan, penyisipan, atau manipulasi sejak diperoleh sampai diajukan di persidangan. Integritas dapat diuji dengan membuat salinan forensik, menghitung nilai hash, membandingkan nilai hash pada beberapa tahap pemeriksaan, dan menggunakan media penyimpanan yang dapat mendeteksi perubahan. Nilai hash tidak membuktikan bahwa isi awal berkas benar atau tidak palsu; nilai tersebut hanya menunjukkan apakah berkas yang diperiksa identik dengan berkas yang sebelumnya dihitung nilai hash-nya.

Chain of custody adalah rangkaian dokumentasi mengenai penguasaan, pemindahan, penyimpanan, pemeriksaan, dan penyajian bukti. Setiap perubahan penguasaan harus mencatat identitas pihak yang menyerahkan dan menerima, waktu pemindahan, tujuan pemindahan, kondisi barang bukti, metode penyimpanan, nilai hash, serta tanda tangan atau autentikasi pihak yang bertanggung jawab. Putusnya chain of custody tidak selalu membuat bukti otomatis tidak dapat diterima, tetapi dapat mengurangi bobot pembuktian.

Keterangan ahli menjembatani kompleksitas teknis dengan penilaian hukum. Ahli forensik digital dapat menerangkan metode ekstraksi, validasi metadata, pemeriksaan hash, analisis artefak perangkat, dan indikasi manipulasi. Ahli AI dapat menjelaskan karakteristik model generatif, teknik face swapping, kloning suara, dan keterbatasan sistem pendeteksi. Ahli tidak menggantikan kewenangan hakim, melainkan memberikan dasar teknis bagi penilaian alat bukti.

METODE

Penelitian ini menggunakan metode hukum sosio-legal dengan analisis normatif dan kebijakanpublik. Pendekatan sosio-legal digunakan untuk menghubungkan norma hukum dengan praktik verifikasi digital, perkembangan teknologi deepfake, dan kebutuhan pengawasan sektor jasa keuangan.

Bahan penelitian diklasifikasikan menjadi tiga kelompok. Pertama, bahan hukum primer meliputi Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, serta POJK Nomor 3 Tahun 2024 tentang Penyelenggaraan Inovasi Teknologi Sektor Keuangan. Kedua, bahan sekunder berupa artikel jurnal, buku akademik, laporan penelitian, dokumen kebijakan, laporan regulator, dan penelitian mengenai autentikasi bukti elektronik, digital forensics, deepfake, dan regulatory sandbox. Ketiga, bahan tersier berupa laman resmi lembaga dan publikasi media yang digunakan secara terbatas untuk konteks empiris.

Pengumpulan bahan dilakukan melalui penelusuran peraturan, dokumen resmi regulator, basis data penelitian, dan publikasi relevan. Bahan diseleksi berdasarkan relevansi, otoritas penerbit, keterbaruan, dan keterlacakan metodologis. Bahan diklasifikasikan ke dalam empat tema: pengaturan bukti elektronik; autentikasi, integritas, dan chain of custody; tata kelola AI dan regulatory sandbox; serta risiko deepfake terhadap sektor keuangan. Analisis dilakukan secara kualitatif dengan teknik deskriptif-analitis dan preskriptif.

HASIL DAN PEMBAHASAN

Deepfake mengubah profil risiko verifikasi digital karena memungkinkan pelaku memproduksi representasi wajah, suara, atau video yang tampak konsisten dengan identitas korban. Risiko tersebut berada pada sisi nasabah, desain e-KYC, penyedia teknologi, pengelolaan data biometrik, dan prosedur respons insiden. Serangan yang

berhasil menembus satu sistem berpotensi direplikasi terhadap lembaga lain yang menggunakan arsitektur verifikasi serupa.

Data kuantitatif mengenai kerugian dan peningkatan insiden harus selalu ditempatkan bersama sumbernya. Laporan mengenai kerugian lebih dari Rp700 miliar digunakan untuk menunjukkan urgensi risiko sektor keuangan, sedangkan laporan mengenai 274.000 laporan penipuan dan kerugian lebih dari Rp6 triliun harus dibaca sebagai data pelaporan penipuan secara luas dan tidak otomatis seluruhnya dikategorikan sebagai deepfake (detikInet, 2025; SWA.co.id, 2026).

Kelemahan autentikasi dapat menimbulkan tiga konsekuensi hukum. Pertama, bukti dapat dipersoalkan dari aspek admissibility apabila tidak memenuhi persyaratan mengenai cara perolehan, keaslian, integritas, atau keterkaitan dengan perkara. Kedua, bukti dapat diterima secara formal tetapi memiliki kekuatan pembuktian rendah karena asal-usul atau proses penyimpanannya tidak dapat dijelaskan. Ketiga, kelemahan autentikasi dapat memengaruhi alat bukti lain apabila bukti elektronik menjadi dasar utama rangkaian peristiwa.

Dalam perkara yang melibatkan video atau suara deepfake, hakim perlu membedakan apakah berkas berasal dari perangkat atau akun yang diklaim, apakah berkas berubah setelah diperoleh, dan apakah isi berkas menggambarkan peristiwa yang benar atau merupakan hasil manipulasi. Pertanyaan pertama berkaitan dengan autentikasi, pertanyaan kedua dengan integritas, dan pertanyaan ketiga dengan kebenaran materiil serta penilaian keseluruhan alat bukti.

Tabel 1. Standar autentikasi berlapis

Tahap	Parameter	Tujuan
Identifikasi sumber	Perangkat, akun, sistem, dan pemilik data	Memastikan asal bukti
Akuisisi forensik	Salinan forensik dan dokumentasi ekstraksi	Mencegah perubahan saat pengambilan
Pemeriksaan integritas	Hash, tanda tangan digital, media aman	Menunjukkan tidak ada perubahan
Pemeriksaan metadata	Waktu, lokasi, perangkat, format, riwayat	Menguji konsistensi teknis
Analisis manipulasi	Artefak, ketidaksesuaian suara-gambar, pola kompresi	Mengidentifikasi indikasi deepfake
Provenans konten	Metadata tertanda tangan dan Content Credentials	Menelusuri riwayat pembuatan

Tahap	Parameter	Tujuan
Keterangan ahli	Metode, keterbatasan, dan tingkat probabilitas	Membantu hakim memahami hasil
Koreborasi	Log transaksi, saksi, perangkat, dan bukti lain	Menguji kebenaran materiil

Standar tersebut diterapkan secara proporsional. Bukti yang menjadi dasar utama penetapan tersangka atau putusan harus menjalani pemeriksaan lebih ketat daripada bukti pendukung. C2PA dapat digunakan sebagai salah satu standar teknis provenans karena menyediakan standar terbuka untuk mencatat asal dan perubahan konten secara kriptografis, tetapi manifest provenans tidak boleh diperlakukan sebagai jaminan mutlak (C2PA, 2025).

POJK Nomor 3 Tahun 2024 menyediakan kerangka regulatory sandbox untuk menguji dan mengembangkan inovasi teknologi sektor keuangan, termasuk permohonan, rencana pengujian, evaluasi, dan kebijakan keluar. Penelitian ini mengadaptasi arsitektur tersebut dan mengusulkan perluasan khusus untuk AI generatif yang berpotensi menyerang sistem verifikasi keuangan (Otoritas Jasa Keuangan, 2024).

Tabel 2. Tahapan Ex-Ante Regulatory Sandbox untuk Pengawasan Deepfake pada Sektor Perbankan

Tahap	Kegiatan utama	Keluaran
1. Pra-registrasi	Identifikasi pengembang, klasifikasi risiko, pemeriksaan dokumen, analisis awal	Diterima, dilengkapi, atau ditolak
2. Simulasi risiko	Red-teaming e-KYC, uji liveness, kloning suara, face swapping, uji serangan berulang	Lulus, lulus bersyarat, atau tidak lulus
3. Autentikasi konten	Metadata, C2PA, watermark, fingerprint, hash, dan log perubahan	Sertifikat/persyaratan autentikasi
4. Pemantauan	Pelaporan pembaruan model, audit, insiden, pengujian ulang, exit policy	Operasional, mitigasi, uji ulang, atau penghentian

Tahap pertama: pra-registrasi

Pra-registrasi merupakan gerbang masuk untuk mengidentifikasi produk AI yang mampu menghasilkan atau memanipulasi wajah, suara, atau video manusia dan berpotensi digunakan untuk melewati verifikasi biometrik. Pengembang harus menyerahkan identitas badan usaha, deskripsi model, tujuan penggunaan, jenis data pelatihan, mekanisme pencegahan penyalahgunaan, prosedur pelaporan,

desain watermarking, analisis risiko awal, dan rencana pengujian. Komdigi menilai tata kelola AI dan aspek perlindungan data, sedangkan OJK menilai dampak terhadap bank, e-KYC, transaksi, dan konsumen.

Tahap kedua: simulasi risiko

Simulasi meliputi pembukaan rekening dengan face swapping, verifikasi suara melalui kloning, video langsung yang dimanipulasi, serangan terhadap liveness detection, pemalsuan dokumen yang dipadukan dengan biometrik sintetis, dan manipulasi metadata. Indikator pengujian meliputi tingkat deteksi, false acceptance, false rejection, waktu respons, kemampuan menyimpan log, kemampuan eskalasi kepada manusia, dan kemampuan menghentikan transaksi mencurigakan. Hasilnya adalah lulus, lulus bersyarat, atau tidak lulus.

Tahap ketiga: autentikasi konten

Produk yang lulus pengujian wajib menggunakan autentikasi berlapis berupa metadata, manifest provenans bertanda tangan, watermark tidak kasatmata, dan pencatatan fingerprint serta log perubahan. C2PA dapat digunakan untuk mencatat sumber dan perubahan konten secara terbuka dan dapat diverifikasi. Namun, setiap lapisan memiliki keterbatasan sehingga tidak menggantikan pemeriksaan forensik dan penilaian hakim.

Tahap keempat: pemantauan berkelanjutan

Kelulusan sandbox tidak berlaku tanpa batas. Pengembang wajib melaporkan pembaruan model, perubahan data, perubahan infrastruktur, insiden, kegagalan watermarking, jumlah pengguna, dan keluhan konsumen. Pengujian ulang dilakukan apabila ada perubahan material, teknik serangan baru, insiden berulang, perluasan fungsi, atau perubahan infrastruktur. Exit policy mencakup penghentian layanan, penyelesaian kewajiban kepada konsumen, pengembalian atau penghapusan data, serta pelaporan akhir.

Tabel 3. Pembagian kewenangan

Institusi	Peran
OJK	Menilai dampak terhadap stabilitas dan integritas sektor keuangan, menjadi host sandbox, dan menetapkan persyaratan bagi bank/penyelenggara ITSK
Komdigi	Menilai tata kelola AI, transparansi, perlindungan data, dan standar autentikasi konten
Bank/penyelenggara	Menguji sistem, memantau transaksi, dan melaporkan insiden

Institusi	Peran
Ahli forensik digital	Melakukan akuisisi, pemeriksaan integritas, dan analisis manipulasi
Penegak hukum	Menjaga legalitas perolehan, penyimpanan, dan penyajian bukti
Hakim	Menilai relevansi, keaslian, integritas, reliabilitas, dan kekuatan pembuktian

Perbandingan dan pembaharuan

Kajian (CIPS, 2023) menekankan tata kelola dan koordinasi dalam sandbox fintech, sedangkan penelitian mengenai sandbox kesehatan menunjukkan manfaat kolaborasi dengan kementerian teknis. Penelitian mengenai bukti deepfake berfokus pada metode verifikasi dan pembuktian setelah sengketa. Penelitian ini menambahkan dimensi preventif dengan menghubungkan pengujian sebelum pasar, ketahanan e-KYC, autentikasi konten, chain of custody, dan penilaian ahli. Kebaruan penelitian terletak pada integrasi tata kelola produk AI dengan kesiapan pembuktian digital, bukan pada penciptaan alat deteksi baru.

Implikasi penelitian

Pembentuk undang-undang perlu menyusun dasar hukum mengenai AI berisiko tinggi, autentikasi konten, pembagian kewenangan, dan konsekuensi bagi pengembang yang tidak melakukan mitigasi. OJK dan Komdigi perlu menyusun peraturan bersama atau pedoman teknis mengenai kriteria risiko, pra-registrasi, simulasi, pelaporan, dan pengujian ulang. Aparat penegak hukum perlu menerapkan prosedur akuisisi dan penyimpanan bukti yang mendokumentasikan perangkat, metode, hash, penguasaan, dan pemeriksaan. Hakim perlu menilai bukti deepfake secara berlapis dan tidak menerima hasil deteksi AI secara otomatis tanpa memeriksa metode serta tingkat kesalahannya. Ahli forensik digital perlu menjelaskan metode, batas probabilitas, dan keterbatasan pemeriksaan secara transparan.

Saran penelitian lanjutan

Penelitian lanjutan perlu menguji praktik autentikasi bukti elektronik pada tingkat penyidikan dan persidangan melalui wawancara dengan penyidik, jaksa, hakim, ahli, bank, dan penyelenggara teknologi. Studi empiris juga diperlukan untuk mengukur tingkat keberhasilan liveness detection terhadap berbagai jenis deepfake. Penelitian komparatif dapat membandingkan C2PA, standar watermarking, mekanisme disclosure AI, serta prosedur penerimaan bukti digital di beberapa yurisdiksi.

KESIMPULAN

Penipuan berbasis deepfake menunjukkan bahwa perlindungan hukum terhadap sistem verifikasi digital tidak dapat hanya mengandalkan penindakan setelah kerugian terjadi. Persoalan utamanya terletak pada belum terhubungnya tata kelola AI, pengawasan sektor keuangan, dan standar autentikasi bukti elektronik pada tahap sebelum teknologi digunakan secara luas.

Penelitian ini mengusulkan Ex-Ante Regulatory Sandbox kolaboratif antara OJK dan Komdigi sebagai instrumen preventif yang menguji risiko, legalitas, transparansi, dan kemampuan autentikasi produk AI sebelum digunakan dalam sistem keuangan. Implikasi teoretisnya adalah autentikasi bukti elektronik perlu dipahami sebagai bagian dari siklus tata kelola teknologi, bukan semata persoalan pembuktian setelah perkara terjadi. Implikasi praktisnya adalah perlunya autentikasi berlapis, dokumentasi chain of custody, penggunaan ahli, dan pemantauan berkelanjutan.

Penelitian lanjutan disarankan untuk menguji kelayakan operasional kerangka ini melalui kajian dampak regulasi dan studi empiris mengenai praktik autentikasi bukti elektronik pada tingkat penyidikan serta persidangan.

REFERENSI

AI-Based Deepfake Verification Protocols for Legal Evidence. 2026. "AI-Based Deepfake Verification Protocols for Legal Evidence." Andrianto, Wahyu. 2024. "Catatan Sederhana untuk Regulatory Sandbox Bidang Kesehatan." Fakultas Hukum Universitas Indonesia. Asatu News. 2026. "Kejahatan Deepfake Fintech Indonesia Melonjak 1.550 Persen." C2PA. 2025. Content Credentials: C2PA Technical Specification. Center for Indonesian Policy Studies. 2023. Membedah Kerangka Regulatory Sandbox Industri Fintech Indonesia. detikInet. 2025. "Sektor Keuangan Indonesia Rugi Rp700 Miliar Lebih Gegara Deepfake." International AI Safety Report. 2025. International AI Safety Report: Technical Safeguards and Risk Management. National Center for Biotechnology Information. 2024. "Introducing a Regulatory Sandbox Into the Indonesian Health System Using e-Malaria as a Use Case: Participatory Action Study." Otoritas Jasa Keuangan. 2024. Peraturan Otoritas Jasa Keuangan Nomor 3 Tahun 2024 tentang Penyelenggaraan Inovasi Teknologi Sektor Keuangan. Otoritas Jasa Keuangan. 2024. Regulatory Sandbox dan Publikasi Inovasi Teknologi Sektor Keuangan. Otoritas Jasa Keuangan dan Indonesia Anti-Scam Centre. 2026. Laporan Penanganan Penipuan Sektor Keuangan. SWA.co.id. 2026. "274 Ribu Kasus, Rp6 Triliun Kerugian: Deepfake Tekan Industri Keuangan RI." Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.