Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 3, 2026
DOI: https://doi.org/10.61104/alz.v4i3.6438

Perlindungan Hukum Nasabah Terhadap Deepfake Fraud Pada Perbankan Digital Di Indonesia

Totok Handono[1], Hasnah Aziz[2], Muhammad Rizki Azhari[3], Agus Alqodri[4]
Universitas Islam Syekh-Yusuf Tangerang, Indonesia[1-4]
Email Korespondensi: ttkhandono@gmail.com, haziz@unis.ac.id, muhammadrizkiazhari06@gmail.com, qhorexido@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Maret 2026, Article published: 01 Juni 2026

ABSTRACT
The development of artificial intelligence (AI) has created a new form of cybercrime known as deepfake fraud, which threatens the security of digital banking transactions and customer legal protection. This study aims to analyze the legal protection of customers who become victims of deepfake fraud in digital banking transactions in Indonesia and to identify weaknesses in national regulations compared to international standards. This research employs a normative legal method using statutory, conceptual, and comparative approaches. The study finds that Indonesian regulations, including the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), have not specifically regulated AI-based deepfake threats. As a result, legal protection for banking customers remains partial and insufficiently adaptive to technological developments. In addition, weak digital security literacy and limited cybersecurity mitigation systems in banking institutions increase the risk of deepfake fraud. Compared to Indonesia, the European Union through the Artificial Intelligence Act and the General Data Protection Regulation (GDPR) has adopted a more preventive and progressive approach in regulating AI and personal data protection. This study recommends establishing specific regulations concerning deepfake and AI fraud, strengthening digital security systems, and improving public cybersecurity literacy to enhance customer protection in the digital banking sector.
Keywords: *Deepfake fraud, legal protection, digital banking, artificial intelligence, cybersecurity.*

ABSTRAK
Perkembangan artificial intelligence (AI) telah memunculkan bentuk baru kejahatan siber berupa deepfake fraud yang mengancam keamanan transaksi perbankan digital dan perlindungan hukum nasabah. Penelitian ini bertujuan menganalisis perlindungan hukum terhadap nasabah korban deepfake fraud dalam transaksi perbankan digital di Indonesia serta mengidentifikasi kelemahan regulasi nasional dibandingkan dengan standar internasional. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif. Hasil penelitian menunjukkan bahwa regulasi di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP), belum secara spesifik mengatur ancaman deepfake berbasis AI sehingga perlindungan hukum terhadap nasabah masih bersifat parsial dan belum adaptif terhadap perkembangan teknologi digital. Selain itu, rendahnya literasi keamanan digital masyarakat dan belum optimalnya sistem mitigasi keamanan siber pada institusi perbankan turut meningkatkan risiko deepfake fraud.

Dibandingkan dengan Indonesia, Uni Eropa melalui Artificial Intelligence Act dan General Data Protection Regulation (GDPR) memiliki pendekatan regulasi yang lebih preventif dan progresif dalam mengatur penggunaan AI dan perlindungan data pribadi. Penelitian ini merekomendasikan pembentukan regulasi khusus terkait deepfake dan AI fraud, penguatan sistem keamanan digital, serta peningkatan literasi keamanan siber masyarakat untuk memperkuat perlindungan nasabah dalam sektor perbankan digital.
Kata Kunci: *Deepfake fraud, perlindungan hukum, perbankan digital, artificial intelligence, keamanan siber.*

PENDAHULUAN

Transformasi digital pada sektor perbankan telah mengubah pola transaksi masyarakat menuju sistem keuangan berbasis teknologi elektronik. Perkembangan layanan *mobile banking*, *internet banking*, dan *financial technology* mendorong terciptanya sistem transaksi yang lebih cepat, efisien, dan terintegrasi dengan *artificial intelligence* (AI). Namun, perkembangan tersebut juga memunculkan bentuk baru kejahatan siber yang semakin kompleks, salah satunya *deepfake fraud*. Teknologi *deepfake* memungkinkan manipulasi wajah, suara, dan identitas digital seseorang secara realistis menggunakan AI sehingga sulit dibedakan dari identitas asli. Dalam sektor perbankan digital, teknologi tersebut berpotensi digunakan untuk melakukan impersonasi, pencurian identitas, dan pembobolan sistem autentikasi biometrik.

Ancaman *deepfake fraud* menjadi persoalan serius terhadap keamanan transaksi elektronik dan perlindungan data pribadi nasabah. Berbagai penelitian menunjukkan bahwa pelaku kejahatan siber mulai memanfaatkan *voice cloning*, face swapping, dan *synthetic identity* untuk memperoleh akses ilegal terhadap akun perbankan digital dan sistem pembayaran elektronik digital (Ke et al., 2025). Selain itu, perkembangan AI-*driven fraud* berlangsung lebih cepat dibandingkan kemampuan regulasi dan sistem keamanan digital dalam melakukan mitigasi risiko (George et al., 2025). Kondisi tersebut menunjukkan bahwa perkembangan AI tidak hanya membawa manfaat dalam sektor keuangan digital, tetapi juga meningkatkan risiko kejahatan siber berbasis manipulasi identitas digital (Popa et al., 2025).

Di Indonesia, ancaman *deepfake fraud* semakin relevan seiring meningkatnya penggunaan layanan perbankan digital dan masih rendahnya literasi keamanan siber masyarakat. Penelitian Gunawan dan Janisriwati (2023) menjelaskan bahwa transformasi digital perbankan Indonesia membuka peluang penyalahgunaan teknologi *deepfake* dalam bentuk pemalsuan identitas nasabah dan manipulasi biometrik digital. Ancaman tersebut diperparah oleh praktik social engineering yang memanfaatkan rekayasa psikologis dan teknologi AI untuk memperoleh akses terhadap data dan akun nasabah. Akibatnya, *deepfake fraud* tidak hanya menimbulkan kerugian ekonomi, tetapi juga mengancam kepercayaan publik terhadap sistem perbankan digital.

Permasalahan *deepfake fraud* menjadi penting untuk dikaji karena berkaitan dengan efektivitas perlindungan hukum terhadap nasabah sebagai konsumen jasa keuangan digital. Regulasi di Indonesia seperti Undang-Undang Informasi dan

Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP) pada dasarnya telah mengatur keamanan transaksi elektronik dan perlindungan data pribadi. Namun, kedua regulasi tersebut belum secara spesifik mengatur manipulasi identitas digital berbasis *artificial intelligence* seperti *deepfake*. Akibatnya, masih terdapat kekosongan norma terkait pembuktian digital, pertanggungjawaban pelaku, dan mekanisme perlindungan korban *deepfake fraud* dalam sektor perbankan digital.

Penelitian mengenai *deepfake* selama ini lebih banyak berfokus pada aspek teknis deteksi AI, keamanan siber, dan penyebaran disinformasi digital. Sementara itu, kajian yang secara khusus membahas perlindungan hukum nasabah terhadap *deepfake fraud* dalam transaksi perbankan digital di Indonesia masih relatif terbatas. Oleh karena itu, penelitian ini penting dilakukan untuk menganalisis efektivitas perlindungan hukum terhadap nasabah korban *deepfake fraud* serta mengkaji kelemahan regulasi nasional dibandingkan dengan pendekatan regulasi internasional.

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan komparatif. Fokus penelitian diarahkan pada analisis regulasi perlindungan hukum nasabah terhadap *deepfake fraud* dalam sektor perbankan digital di Indonesia serta perbandingannya dengan *Artificial Intelligence Act* dan *General Data Protection Regulation* (GDPR) di Uni Eropa.

Kebaruan penelitian ini terletak pada analisis perlindungan hukum nasabah terhadap *deepfake fraud* dalam transaksi perbankan digital melalui pendekatan hukum normatif dan komparatif dengan regulasi Uni Eropa. Penelitian ini juga menekankan urgensi pembentukan regulasi khusus terkait *artificial intelligence* berbasis *synthetic* media dalam sektor jasa keuangan digital di Indonesia.

METODE

Penelitian ini merupakan penelitian hukum normatif yang berfokus pada analisis norma hukum terkait perlindungan hukum nasabah terhadap *deepfake fraud* dalam transaksi perbankan digital. Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan komparatif (*comparative approach*). Pendekatan perundang-undangan dilakukan melalui analisis terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, serta regulasi Otoritas Jasa Keuangan dan Bank Indonesia terkait layanan perbankan digital. Pendekatan konseptual digunakan untuk menganalisis konsep perlindungan hukum, *cybercrime*, digital trust, keamanan data pribadi, dan tanggung jawab hukum institusi perbankan terhadap kerugian nasabah akibat *deepfake fraud*. Sementara itu, pendekatan komparatif dilakukan dengan membandingkan regulasi Indonesia dengan *Artificial Intelligence Act* dan *General Data Protection Regulation* (GDPR) di

Uni Eropa. Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan dan dokumen kebijakan, serta bahan hukum sekunder berupa buku, jurnal ilmiah, dan artikel akademik yang relevan dengan penelitian. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*). Selanjutnya, bahan hukum dianalisis secara kualitatif dengan metode deskriptif analitis guna mengkaji efektivitas regulasi perlindungan hukum nasabah terhadap ancaman *deepfake fraud* pada sistem perbankan digital di Indonesia.

HASIL DAN PEMBAHASAN

Perkembangan Deepfake Fraud dalam Transaksi Perbankan Digital

Hasil penelitian menunjukkan bahwa perkembangan *artificial intelligence* (AI) telah menciptakan bentuk baru kejahatan siber dalam sektor perbankan digital melalui penggunaan teknologi *deepfake*. *Deepfake fraud* merupakan tindakan manipulasi identitas digital berupa wajah, suara, maupun video menggunakan AI untuk memperoleh akses ilegal terhadap sistem transaksi elektronik dan data keuangan nasabah. Dalam praktiknya, pelaku memanfaatkan teknologi voice cloning, face swapping, dan synthetic identity untuk meniru identitas nasabah maupun pejabat bank sehingga mampu mengelabui sistem autentikasi digital. Fenomena ini berkembang seiring meningkatnya penggunaan mobile banking, *internet banking*, dan layanan financial technology di Indonesia pascapandemi COVID-19.

Berdasarkan hasil analisis berbagai laporan keamanan siber dan literatur akademik, ditemukan bahwa ancaman *deepfake* dalam sektor perbankan digital tidak lagi bersifat hipotetis, melainkan telah menjadi ancaman nyata terhadap keamanan sistem keuangan digital. Kejahatan ini berkembang karena sistem autentikasi biometrik yang digunakan perbankan digital masih memiliki kerentanan terhadap manipulasi visual dan audio berbasis AI (Ke et al., 2025).

Selain itu, rendahnya literasi keamanan digital masyarakat menyebabkan nasabah mudah terpengaruh oleh manipulasi identitas digital yang tampak autentik. Dalam konteks sosial, perkembangan *deepfake* menunjukkan adanya perubahan pola kejahatan siber dari metode konvensional menuju kejahatan berbasis synthetic media yang lebih kompleks dan sulit dideteksi.

Penelitian ini menemukan bahwa meningkatnya penggunaan *deepfake fraud* turut memengaruhi tingkat kepercayaan publik terhadap layanan perbankan digital. Nasabah cenderung merasa khawatir terhadap keamanan data pribadi dan risiko penyalahgunaan identitas digital dalam transaksi elektronik. Kondisi tersebut menunjukkan bahwa *deepfake* tidak hanya berdampak pada kerugian ekonomi, tetapi juga memengaruhi aspek psikologis dan rasa aman masyarakat dalam menggunakan layanan perbankan digital. Temuan ini sejalan dengan penelitian (Davey & Sauerwein, 2023) yang menyatakan bahwa *deepfake* telah berkembang menjadi instrumen cyber fraud yang mengancam digital trust dalam sistem ekonomi modern.

Kelemahan Regulasi Perlindungan Hukum di Indonesia terhadap Deepfake Fraud

Sistem perlindungan hukum di Indonesia belum secara khusus mengatur ancaman *deepfake fraud* dalam sektor perbankan digital. Regulasi yang berlaku saat ini, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), dan Undang-Undang Perbankan, pada dasarnya telah mengatur keamanan transaksi elektronik dan perlindungan data pribadi. Namun, regulasi tersebut belum secara eksplisit mengatur karakteristik kejahatan berbasis AI seperti *deepfake*.

Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik memberikan perlindungan terhadap penggunaan data pribadi melalui media elektronik. Namun, ketentuan tersebut belum secara spesifik mengatur penyalahgunaan identitas biometrik berbasis artificial intelligence seperti deepfake. Akibatnya, terdapat kekosongan norma terkait pertanggungjawaban hukum terhadap manipulasi identitas digital menggunakan teknologi *synthetic* media.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada prinsipnya juga telah mengatur perlindungan data biometrik sebagai bagian dari data pribadi spesifik. Akan tetapi, regulasi tersebut belum mengatur secara rinci penggunaan teknologi *artificial intelligence* dalam manipulasi data biometrik melalui *voice cloning*, *face swapping*, maupun *synthetic identity*.

Kekosongan norma tersebut menyebabkan munculnya berbagai persoalan hukum. Persoalan tersebut berkaitan dengan pembuktian digital, pertanggungjawaban pelaku, dan tanggung jawab institusi perbankan terhadap kerugian nasabah akibat *deepfake fraud*. Selain kekosongan norma terkait *deepfake*, regulasi nasional juga belum mengatur standar pembuktian digital terhadap manipulasi identitas berbasis *artificial intelligence*. Akibatnya, proses penegakan hukum terhadap pelaku *deepfake fraud* berpotensi mengalami hambatan dalam pembuktian unsur pidana maupun pertanggungjawaban perdata. Dalam praktiknya, pembuktian terhadap manipulasi digital berbasis AI masih sulit dilakukan karena *deepfake* memiliki tingkat kemiripan yang sangat tinggi dengan identitas asli. Selain itu, belum terdapat standar hukum nasional mengenai penggunaan AI dalam autentikasi biometrik dan mitigasi synthetic identity fraud pada layanan perbankan digital.

Perlindungan hukum terhadap nasabah masih bersifat reaktif dan belum mengedepankan pendekatan preventif. Sebagian besar kebijakan keamanan perbankan hanya berfokus pada penguatan sistem autentikasi dan monitoring transaksi mencurigakan tanpa disertai mekanisme perlindungan korban secara komprehensif. Kondisi tersebut memperlihatkan adanya ketidaksiapan regulasi nasional dalam menghadapi perkembangan AI-*driven cybercrime*. Temuan ini sejalan dengan penelitian (Syaputra, 2024) yang menegaskan bahwa hukum pidana Indonesia belum memiliki pengaturan khusus terkait *deepfake* sehingga perlindungan korban masih lemah secara normatif.

Perbandingan Regulasi Indonesia dengan Uni Eropa melalui Artificial Intelligence Act dan GDPR

Keberhasilan penelitian ini menemukan bahwa regulasi Uni Eropa memiliki sistem perlindungan hukum yang lebih progresif dalam menghadapi ancaman *deepfake* dibandingkan Indonesia. Uni Eropa melalui *Artificial Intelligence Act* mengategorikan penggunaan AI berdasarkan tingkat risiko, termasuk penggunaan AI yang berpotensi menimbulkan manipulasi identitas dan pelanggaran hak individu. Regulasi tersebut mengatur kewajiban transparansi bagi pengembang AI, pengawasan terhadap penggunaan teknologi berisiko tinggi, serta kewajiban pelabelan terhadap konten sintetis seperti *deepfake*.

General Data Protection Regulation (GDPR) memberikan perlindungan yang kuat terhadap data pribadi dan hak privasi individu dalam lingkungan digital. GDPR mengatur prinsip data *minimization*, *informed consent*, *accountability*, serta hak subjek data untuk memperoleh perlindungan terhadap penyalahgunaan identitas digital. Dalam konteks *deepfake fraud,* GDPR memungkinkan individu untuk menuntut pihak yang menyalahgunakan data biometrik atau identitas digital mereka tanpa persetujuan.

Regulasi Uni Eropa menunjukkan pendekatan yang lebih preventif dan adaptif terhadap perkembangan teknologi AI. Indonesia melalui UU PDP memang telah mengatur perlindungan data pribadi, namun implementasinya masih terbatas pada aspek administratif dan belum secara spesifik mengakomodasi risiko *deepfake* berbasis AI. Selain itu, Indonesia belum memiliki regulasi khusus mengenai tata kelola AI dan kewajiban transparansi penggunaan *synthetic* media. Hal ini menyebabkan perlindungan hukum terhadap nasabah perbankan digital masih memiliki celah yang dapat dimanfaatkan oleh pelaku *cyber fraud*. Temuan ini menunjukkan bahwa Indonesia perlu mengembangkan regulasi AI yang lebih komprehensif untuk memperkuat perlindungan hukum terhadap ancaman *deepfake* dalam sektor jasa keuangan digital.

Implikasi Hukum dan Perlindungan Nasabah terhadap Deepfake Fraud

Deepfake fraud menimbulkan implikasi hukum yang kompleks dalam sistem perbankan digital. Dari perspektif perlindungan konsumen, nasabah sebagai pengguna layanan digital berada pada posisi rentan karena tidak memiliki kemampuan teknis yang memadai untuk membedakan identitas asli dan manipulasi AI. Kondisi tersebut menyebabkan nasabah sering menjadi korban *social engineering* berbasis *deepfake* yang memanfaatkan kepercayaan psikologis terhadap representasi visual dan audio digital.

Dalam perspektif hukum perbankan, institusi bank memiliki *duty of care* untuk menjamin keamanan sistem elektronik dan perlindungan data pribadi nasabah. Kegagalan sistem keamanan digital dalam mencegah *deepfake fraud* dapat menimbulkan tanggung jawab hukum perdata maupun administratif apabila terbukti terdapat kelalaian dalam mitigasi risiko keamanan siber. Namun, penelitian menemukan bahwa sebagian besar mekanisme perlindungan nasabah masih berorientasi pada pendekatan teknis keamanan siber tanpa diimbangi

kebijakan mitigasi risiko *deepfake* secara spesifik. Akibatnya, ketika terjadi *fraud* berbasis AI, proses penyelesaian sengketa dan pembuktian kerugian menjadi sulit dilakukan.

Perlindungan hukum terhadap korban *deepfake fraud* seharusnya tidak hanya berorientasi pada penghukuman pelaku, tetapi juga mencakup pemulihan hak korban, perlindungan data pribadi, serta pemulihan kepercayaan publik terhadap sistem perbankan digital. Dalam konteks ini, negara perlu memperkuat kolaborasi antara regulator, lembaga perbankan, dan pengembang teknologi AI untuk menciptakan sistem keamanan digital yang lebih adaptif terhadap perkembangan kejahatan siber modern. Selain itu, diperlukan peningkatan literasi keamanan digital masyarakat agar nasabah mampu mengenali risiko manipulasi identitas berbasis AI dalam transaksi elektronik.

Relevansi Temuan dan Pengembangan Kebijakan Hukum Digital

Perkembangan *deepfake fraud* telah mengubah paradigma perlindungan hukum dalam era digital. Kejahatan siber berbasis AI tidak lagi dapat ditangani hanya melalui pendekatan hukum konvensional yang bersifat represif, melainkan membutuhkan pendekatan multidisipliner yang mengintegrasikan regulasi, keamanan siber, etika AI, dan perlindungan konsumen digital. Temuan penelitian ini memperkuat teori digital trust yang menempatkan keamanan dan kepercayaan sebagai elemen utama dalam keberlangsungan sistem ekonomi digital. Dalam konteks hukum nasional, perkembangan *deepfake fraud* menunjukkan urgensi pembaruan regulasi *cyber law* Indonesia yang lebih adaptif terhadap perkembangan artificial intelligence. Reformasi hukum diperlukan tidak hanya pada aspek pemidanaan pelaku, tetapi juga pada standar keamanan sistem elektronik, perlindungan data biometrik, dan mekanisme pertanggungjawaban institusi perbankan digital.

Penelitian ini merekomendasikan pembentukan regulasi khusus terkait *artificial intelligence* dan *deepfake fraud* di Indonesia, khususnya dalam sektor jasa keuangan digital. Pemerintah dan Otoritas Jasa Keuangan (OJK) perlu mengembangkan standar keamanan autentikasi biometrik berbasis AI *detection system* (sistem deteksi berbasis *artificial intelligence*) serta memperkuat mekanisme pengawasan terhadap penggunaan data biometrik nasabah. Selain itu, diperlukan harmonisasi regulasi nasional dengan standar internasional seperti *Artificial Intelligence Act* dan GDPR agar perlindungan hukum terhadap nasabah menjadi lebih efektif dan adaptif terhadap perkembangan teknologi global.

SIMPULAN

Penelitian ini menunjukkan bahwa perkembangan teknologi *artificial intelligence* (AI), khususnya *deepfake*, telah menciptakan bentuk baru kejahatan siber dalam sektor perbankan digital yang berpotensi mengancam keamanan transaksi elektronik dan perlindungan hukum nasabah. *Deepfake fraud* berkembang melalui manipulasi identitas digital berupa wajah, suara, maupun video yang digunakan untuk memperoleh akses ilegal terhadap sistem perbankan digital dan data pribadi

nasabah. Hasil penelitian menunjukkan bahwa regulasi di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pelindungan Data Pribadi (UU PDP), serta regulasi sektor perbankan, belum secara spesifik mengatur ancaman *deepfake* berbasis AI sehingga perlindungan hukum terhadap nasabah masih bersifat parsial dan belum adaptif terhadap perkembangan teknologi digital. Penelitian ini juga menemukan bahwa kelemahan perlindungan hukum tidak hanya disebabkan oleh keterbatasan regulasi, tetapi juga oleh rendahnya literasi keamanan digital masyarakat dan belum optimalnya sistem mitigasi risiko pada institusi perbankan digital. Dalam praktiknya, mekanisme perlindungan nasabah masih lebih berorientasi pada pendekatan teknis keamanan siber dibandingkan perlindungan korban secara komprehensif. Selain menimbulkan kerugian ekonomi, *deepfake fraud* juga berdampak pada aspek psikologis dan menurunkan tingkat kepercayaan publik terhadap sistem transaksi digital. Oleh karena itu, ancaman *deepfake* perlu dipahami tidak hanya sebagai persoalan teknologi, tetapi juga sebagai persoalan hukum, sosial, dan perlindungan konsumen digital.

Dari perspektif komparatif, penelitian ini menunjukkan bahwa regulasi Uni Eropa melalui *Artificial Intelligence Act* dan *General Data Protection Regulation* (GDPR) memiliki pendekatan yang lebih preventif dan progresif dalam mengatur penggunaan AI serta perlindungan data pribadi dibandingkan Indonesia. Regulasi tersebut dapat menjadi rujukan bagi Indonesia dalam membangun sistem hukum yang lebih adaptif terhadap perkembangan teknologi AI dan kejahatan siber berbasis *synthetic* media. Temuan penelitian ini memberikan kontribusi teoretis dalam pengembangan kajian hukum siber dan perlindungan konsumen digital, khususnya terkait relasi antara teknologi AI, *digital trust*, dan perlindungan hukum nasabah dalam sektor perbankan digital. Secara praktis, penelitian ini merekomendasikan perlunya pembentukan regulasi khusus terkait *deepfake* dan AI *fraud* dalam sektor jasa keuangan digital, penguatan sistem autentikasi berbasis AI detection, peningkatan literasi keamanan digital masyarakat, serta penguatan koordinasi antara pemerintah, Otoritas Jasa Keuangan (OJK), institusi perbankan, dan pengembang teknologi. Selain itu, penelitian selanjutnya disarankan untuk mengkaji implementasi teknologi deteksi *deepfake* pada sistem perbankan digital serta efektivitas regulasi perlindungan data pribadi dalam menghadapi perkembangan artificial intelligence pada sektor jasa keuangan digital.

UCAPAN TERIMAKASIH:

1. Prof. Dr. Mustofa Kamil, Dipl.RSI., M.Pd. selaku Rektor Universitas Islam Syekh-Yusuf (UNIS), atas segala kebijakan dan fasilitas akademik yang diberikan selama penulis menempuh pendidikan di lingkungan UNIS.
2. Dr. Siti Humulhaer, S.H., M.H., selaku Ketua Program Studi Magister Ilmu Hukum Universitas Islam Syekh-Yusuf (UNIS), atas kesabaran, bimbingan ilmiah, dan arahan yang penuh ketelitian dalam artikel Jurnal ini.
3. Dr. Hasnah Aziz, SPd, SH, MPd, MH., selaku pengampu mata kuliah Hukum Perbankan dan Financial Technology.

4. Seluruh Dosen Pengajar Program Pascasarjana Ilmu Hukum Universitas Islam Syekh-Yusuf (UNIS), yang telah memberikan ilmu akademik, wawasan, inspirasi penelitian selama masa perkuliahan.
5. Kepada semua keluarga tercinta dari keseluruhan penulis yang memberikan penyemangat berkarya membuat penelitian dan penulisan jurnal ilmiah.
6. Kepada Al-Zayn: Jurnal Ilmu Sosial & Hukum yang telah memberikan tempat, membantu terlaksananya publikasi

DAFTAR RUJUKAN

Aprillia, N., Khasanah, D. R. A. U., & Pongantung, R. J. (2025). Implikasi hukum tentang penyalahgunaan teknologi deepfake terhadap kejahatan identitas digital. *Dinamika Hukum*, *26*(2). https://doi.org/10.35315/dh.v26i2.10209

Davey, O. M., & Sauerwein, L. (2023). Deepfake in online fraud cases: The haze of artificial intelligence's accountability based on international law. *Sriwijaya Crimen and Legal Studies*, *1*(2). https://doi.org/10.28946/scls.v1i2.2654

George, M. Z. H., Alam, M. K., & Hasan, M. T. (2025). Machine learning for fraud detection in digital banking: A systematic literature review. *ArXiv*. https://doi.org/https://arxiv.org/abs/2510.05167

Gunawan, I. J., & Janisriwati, S. (2023). Legal analysis on the use of deepfake technology: Threats to Indonesian banking institutions. *Law and Justice*, *8*(2). https://doi.org/10.23917/laj.v8i2.2513

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

Hasanudin, T. A. (2025). Perlindungan nasabah dan tanggung jawab bank dalam penanggulangan kejahatan digital berbasis social engineering: Analisis hukum perbankan Indonesia. *Indonesia Journal of Business Law*, *5*(1). https://doi.org/10.47709/ijbl.v5i1.7476

Ke, Z., Zhou, S., Zhou, Y., Chang, C. H., & Zhang, R. (2025). Detection of AI deepfake and fraud in online payments using GAN-based models. *ArXiv*. https://doi.org/https://arxiv.org/abs/2501.07033

Khan, M. A., Khusnah, H., Kusuma, E. A., Ilahiyah, M. E., & Khan, M. Z. (2025). Deepfake-driven financial fraud in Indonesia: A systematic review of economic impacts and regulatory challenges. *International Journal of Advances in Signal and Image Sciences*, *12*(3s), 295–312. https://doi.org/10.29284/87d1j190

Noviantama, D., & Rahman, A. A. (2025). Deepfake: A review from the victimology perspective. *Contemporary Issues in Criminal Law*, *1*(2). https://doi.org/10.20885/CICL.vol1.iss2.art1

Popa, C., Pallath, R., Cunningham, L., Tahiri, H., Kesavarajah, A., & Wu, T. (2025). Deepfake technology unveiled: The commoditization of AI and its impact on digital trust. *ArXiv*. https://doi.org/https://arxiv.org/abs/2506.07363

Syaputra, R. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artficial Inteligence (Ai) Dari Perspektif Hukum Pidana Indonesia. *Jurnal Respubica*, *24*(1), 1–12. https://doi.org/10.55606/khatulistiwa.v3i3.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Lembaran Negara Republik Indonesia Tahun 1992 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 3472.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum.

Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran.

Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.

