JIIC: JURNAL INTELEK INSAN CENDIKIA
https://jicnusantara.com/index.php/jiic
Vol : 03 No: 06, Juni 2026
E-ISSN : 3047-7824

Perlindungan Data Nasabah dalam System Anti-Fraud Perbankan Berasis Artificial Intelligence

Customer Data Protection in an Artificial Intelligence-Based Banking Anti-Fraud System

Sahara Fatril Futur[1*], Syhlina Rizka Febrianty[2], Tyara Koes Marchellita Assalami[3], Shaina Nur Tifara[4], Ikhsan Mahendra[5], Baidhowi[6]
Universitas Negeri Semarang
Email: saharaf2016@students.unnes.ac.id[1], syhlinarizka1813@students.unnes.ac.id[2], chelintyara@students.unnes.ac.id[3], shainafrr@students.unnes.ac.id[4], ikhsanmahendra@students.unnes.ac.id[5], baidhowi@mail.unnes.ac.id

Article Info

Article history:
Received : 27-05-2026
Revised : 29-05-2026
Accepted : 31-05-2026
Pulished : 02-06-2026

Abstract

The advancement of artificial intelligence (AI) in banking drives the adoption of machine learning-based anti-fraud systems to automatically detect suspicious transactions. While enhancing financial security, this raises legal challenges in personal data protection, particularly data minimization under Indonesia's Personal Data Protection Law. AI's data-intensive nature conflicts with data processing limits, and false positives can cause customer losses, prompting questions of legal liability. This normative legal research employs statutory and conceptual approaches, drawing on relevant data protection and banking laws plus legal literature. Findings show AI anti-fraud is justifiable based on security and legitimate interests, but gaps persist in big data processing limits. Banks bear legal responsibility for algorithmic bias and automated decision errors, necessitating stronger regulations and accountable AI governance in banking.

Keywords* : *Artificial Intelligence, personal data protection, banking.

Abstrak

Kemajuan kecerdasan buatan (AI) di sektor perbankan mendorong adopsi sistem anti-penipuan berbasis pembelajaran mesin untuk mendeteksi transaksi mencurigakan secara otomatis. Meskipun meningkatkan keamanan finansial, hal ini menimbulkan tantangan hukum dalam perlindungan data pribadi, khususnya minimalisasi data berdasarkan Undang-Undang Perlindungan Data Pribadi Indonesia. Sifat AI yang intensif data bertentangan dengan batasan pemrosesan data, dan positif palsu dapat menyebabkan kerugian pelanggan, sehingga memunculkan pertanyaan tentang tanggung jawab hukum. Penelitian hukum normatif ini menggunakan pendekatan hukum dan konseptual, dengan mengacu pada undang-undang perlindungan data dan perbankan yang relevan serta literatur hukum. Temuan menunjukkan bahwa anti-penipuan berbasis AI dapat dibenarkan berdasarkan keamanan dan kepentingan yang sah, tetapi masih terdapat kesenjangan dalam batasan pemrosesan data besar. Bank memikul tanggung jawab hukum atas bias algoritmik dan kesalahan pengambilan keputusan otomatis, sehingga memerlukan regulasi yang lebih kuat dan tata kelola AI yang akuntabel di sektor perbankan.

Kata Kunci: Kecerdasan Buatan, perlindungan data pribadi, perbankan.

PENDAHULUAN

Digitalisasi layanan mendorong bank mengembangkan sistem berbasis teknologi guna meningkatkan efisiensi, keamanan, dan kualitas pelayanan. Salah satu inovasi yang banyak digunakan adalah penerapan Artificial Intelligence (AI) dalam sistem deteksi dan pencegahan

kecurangan (anti-fraud system). Teknologi ini memungkinkan analisis pola transaksi secara cepat serta deteksi aktivitas mencurigakan secara otomatis. Namun, kemajuan ini juga memunculkan persoalan hukum terkait perlindungan data pribadi nasabah, karena sistem AI mengumpulkan dan menganalisis data dalam jumlah besar, termasuk identitas, riwayat transaksi, dan pola perilaku keuangan. Hal ini menimbulkan risiko penyalahgunaan maupun kebocoran data apabila tidak diatur secara memadai.(Awosika et al., 2024) Oleh karena itu, perkembangan teknologi harus diimbangi dengan kerangka hukum yang menjamin perlindungan data pribadi secara efektif sebagai bagian dari hak privasi.

Dalam perbankan modern, data nasabah merupakan aset penting sekaligus sensitif. Bank berkewajiban menjaga kerahasiaan data sebagai bagian dari prinsip kepercayaan. Penerapan sistem anti-fraud berbasis AI memerlukan akses terhadap data dalam jumlah besar untuk mengidentifikasi transaksi tidak wajar, seperti pencucian uang, penipuan kartu kredit, dan peretasan akun.(Putro et al., 2025) Teknologi AI dengan machine learning mampu meningkatkan akurasi deteksi fraud secara berkelanjutan. Namun, penggunaannya menimbulkan tantangan hukum terkait batasan penggunaan data, mekanisme pengawasan, serta tanggung jawab jika terjadi kebocoran. Di Indonesia, hal ini semakin relevan sejak berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur hak pemilik data dan kewajiban pengendali data, serta prinsip kerahasiaan dalam regulasi perbankan.(Ramadhani & Trimuliani, 2024)

Sejumlah penelitian menunjukkan bahwa penggunaan AI dalam keamanan perbankan mampu menekan kejahatan finansial secara signifikan melalui analisis transaksi secara real-time. Meski demikian, risiko terhadap privasi dan keamanan data tetap menjadi perhatian, terutama jika tidak disertai mekanisme perlindungan yang kuat. Dalam konteks Indonesia, perlindungan data nasabah masih menghadapi tantangan regulasi, pengawasan, dan implementasi. Objek penelitian ini adalah penerapan sistem anti-fraud perbankan berbasis AI dalam mendeteksi dan mencegah kejahatan finansial.

Berdasarkan latar belakang tersebut, penelitian ini merumuskan dua permasalahan utama. Pertama, bagaimana pengaturan hukum perlindungan data pribadi nasabah dalam penerapan sistem anti-fraud berbasis AI. Kedua, bagaimana tanggung jawab hukum bank terhadap penyalahgunaan atau kebocoran data nasabah akibat penggunaan sistem tersebut. Tujuan penelitian ini adalah menganalisis kerangka hukum perlindungan data nasabah serta mengkaji bentuk tanggung jawab bank, sehingga dapat memberikan kontribusi akademik dan rekomendasi bagi penguatan regulasi perlindungan data di era digital.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kualitatif jenis yuridis normatif melalui studi pustaka yang bersifat deskriptif-analitis, dengan fokus pada pengumpulan dan analisis data sekunder dari sumber primer hukum seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) 2022, Peraturan Otoritas Jasa Keuangan (POJK) tentang Implementasi Teknologi Anti-Fraud Berbasis Artificial Intelligence, serta regulasi perbankan terkait privasi data nasabah, dilengkapi literatur sekunder berupa jurnal akademik, laporan Otoritas Jasa Keuangan (OJK).(Dr. Muhaimin, S.H., 2020) Teknik pengumpulan data dilakukan secara sistematis melalui penelusuran, klasifikasi, dan pengutipan referensi dari sumber pustaka yang relevan, diikuti analisis isi (content analysis) untuk mengidentifikasi kesenjangan normatif antara ketentuan perlindungan data dan risiko algoritma AI

dalam sistem anti-fraud, seperti potensi bias prediktif atau pelanggaran prinsip transparansi. Analisis data penyajian dalam matriks perbandingan regulasi, dan verifikasi melalui triangulasi sumber pustaka guna menghasilkan interpretasi holistik serta rekomendasi yuridis terhadap harmonisasi regulasi.

HASIL DAN PEMBAHASAN

1. Pengaturan Hukum Mengenai Perlindungan Data Pribadi Nasabah dalam Penerapan Sistem Anti-Fraud Perbankan Berbasis Artificial Intelligence

Kerangka perlindungan data nasabah di sektor perbankan Indonesia kini bersandar pada UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai regulasi payung. Undang-undang ini memberikan definisi yang tegas mengenai data pribadi serta menetapkan protokol ketat dalam pemrosesannya, yang mencakup prinsip transparansi, akurasi, hingga keamanan yang terjamin. Dalam operasionalnya, perbankan modern mengintegrasikan sistem anti-fraud berbasis kecerdasan buatan (AI) yang secara inheren membutuhkan akses luas terhadap data sensitif seperti pola perilaku transaksi, identitas digital, hingga titik koordinat geolokasi nasabah. Oleh karena itu, UU PDP mewajibkan institusi perbankan untuk memperoleh dasar hukum yang kuat, seperti persetujuan eksplisit, sebelum melakukan pemrosesan tersebut. (Ayunda & Rusdianto, 2021) Kekuatan hukum ini semakin diperkuat oleh UU Nomor 10 Tahun 1998 tentang Perbankan, yang mengamanatkan prinsip kerahasiaan bank. Sinergi antara kedua undang-undang ini memastikan bahwa pengungkapan data nasabah tetap bersifat restriktif dan hanya diperbolehkan melalui mekanisme hukum yang sah, guna menyeimbangkan efisiensi sistem keamanan perbankan dengan hak privasi individu.

Dalam ekosistem perbankan digital, Peraturan Otoritas Jasa Keuangan (POJK) Nomor 21 Tahun 2023 memegang peranan vital sebagai kerangka teknis yang mewajibkan bank umum untuk menjamin keamanan data pribadi, terutama pada layanan yang mengintegrasikan kecerdasan buatan (AI anti-fraud). Bank diinstruksikan untuk membangun infrastruktur teknologi informasi yang kokoh guna menangkal segala bentuk kebocoran maupun penyalahgunaan data. Sejalan dengan itu, Peraturan Bank Indonesia mempertegas bahwa perlindungan data merupakan komponen fundamental dari hak konsumen atas kenyamanan dan keamanan layanan keuangan.

Meskipun demikian, berbagai studi literatur menyoroti adanya tantangan regulasi, dimana aturan yang ada dianggap belum sepenuhnya mampu memitigasi risiko spesifik dari penggunaan data berskala besar oleh AI, seperti potensi munculnya bias algoritma atau pengambilan keputusan otomatis yang merugikan nasabah secara sepihak.

Pada titik ini, muncul persoalan fundamental yang menjadi inti perdebatan dalam perlindungan data, yaitu benturan antara prinsip minimisasi data dalam UU PDP dengan karakteristik teknologi AI yang bersifat data-hungry. UU PDP secara normatif mengharuskan bahwa data yang dikumpulkan harus terbatas pada yang relevan, spesifik, dan sesuai dengan tujuan pemrosesan. Sebaliknya, sistem machine learning dalam anti-fraud justru bekerja secara optimal ketika memiliki akses terhadap data dalam jumlah besar, bahkan termasuk data yang pada awalnya tidak tampak relevan, karena pola kecurangan sering kali baru dapat terdeteksi

melalui analisis korelatif dari data yang luas dan beragam. Kondisi ini menciptakan paradoks antara kebutuhan efisiensi sistem keamanan dengan perlindungan hak privasi nasabah.

Dalam menyikapi konflik tersebut, UU PDP tidak memberikan larangan absolut terhadap penggunaan big data, melainkan mengaturnya melalui pendekatan berbasis prinsip. Pengumpulan data dalam skala besar tetap dimungkinkan sepanjang memiliki dasar pemrosesan yang sah, seperti persetujuan atau kepentingan yang sah dalam pencegahan kejahatan keuangan. Namun, penggunaan dasar ini harus melalui uji kebutuhan (necessity test) dan proporsionalitas, di mana bank wajib membuktikan bahwa data yang dikumpulkan benar-benar relevan dan tidak berlebihan. Dengan demikian, prinsip minimisasi data tidak diartikan secara kaku, tetapi secara kontekstual sesuai tujuan pemrosesan.

Meskipun secara konseptual pendekatan ini mampu menjembatani kebutuhan teknologi dan perlindungan hukum, dalam praktiknya masih terdapat celah hukum yang cukup signifikan. UU PDP tidak memberikan parameter yang jelas mengenai batasan "data yang relevan" dalam sistem berbasis AI, sehingga membuka ruang interpretasi yang luas bagi institusi perbankan. Dalam kondisi ini, bank berpotensi memperluas pengumpulan data dengan dalih meningkatkan akurasi sistem anti-fraud atau menjaga stabilitas sistem keuangan. Praktik semacam ini berisiko menimbulkan fenomena over-collection of data maupun function creep, yaitu penggunaan data di luar tujuan awal yang telah ditetapkan. Oleh karena itu, meskipun hukum tidak secara eksplisit melegitimasi pengumpulan big data tanpa batas, terdapat ruang abu-abu yang memungkinkan praktik tersebut dilakukan sepanjang dapat dibungkus dalam narasi "kepentingan keamanan sistem keuangan".(Yuniari & I Dewa Ayu Dwi Mayasari, 2022)

Sistem penanggulangan penipuan (anti-fraud) di industri perbankan saat ini mengandalkan algoritma machine learning canggih untuk membedah pola transaksi secara seketika (real-time) guna mengidentifikasi anomali yang mengarah pada tindak pidana pencucian uang, pembobolan akun, maupun penipuan siber lainnya. Operasional sistem ini sangat bergantung pada akses terhadap beragam data pribadi nasabah yang bersifat sensitif, mulai dari informasi identitas resmi (KTP), rincian nomor rekening, riwayat transaksi, hingga jejak perilaku digital dan pola akses aplikasi.(Wiriani et al., 2025)

Analisis pada tahun 2024 menunjukkan bahwa integrasi kecerdasan buatan mampu mendongkrak akurasi deteksi kecurangan hingga mencapai angka 90%. Namun, lonjakan performa ini berbanding lurus dengan meningkatnya risiko pelanggaran privasi, terutama jika data tersebut tidak diproteksi melalui teknik enkripsi mutakhir dan mekanisme kontrol akses yang berlapis.(Annafa et al., 2024) Dalam implementasinya, institusi perbankan memikul tanggung jawab hukum untuk menjamin bahwa model AI yang digunakan tidak memproses data pribadi yang bersifat diskriminatif seperti informasi etnis, keyakinan agama, atau riwayat kesehatan, kecuali jika hal tersebut dilakukan demi tujuan yang sah, terukur, dan tetap mengedepankan prinsip proporsionalitas sesuai regulasi yang berlaku.

Dalam praktik perbankan di Indonesia, institusi besar seperti BCA dan BRI telah mengintegrasikan sistem anti-fraud berbasis kecerdasan buatan (AI) guna memitigasi kerugian masif akibat kejahatan digital yang nilainya mencapai triliunan rupiah setiap tahunnya. Walaupun efektivitasnya terbukti tinggi, para ahli memperingatkan adanya risiko ketergantungan pada teknologi ini, yang dapat memicu keputusan diskriminatif jika model AI

dilatih menggunakan data yang bias, sehingga berpotensi merugikan kelompok nasabah tertentu secara tidak adil.

Menanggapi tantangan tersebut, Regulasi OJK tahun 2025 mewajibkan bank untuk mendokumentasikan setiap tahapan proses pengambilan keputusan otomatis oleh AI. Langkah ini bertujuan untuk menjamin hak nasabah dalam meminta penjelasan serta mengajukan keberatan atas keputusan yang merugikan mereka. Selain itu, terkait dengan aspek teknis, setiap aktivitas transfer data kepada vendor AI di luar negeri harus tunduk sepenuhnya pada ketentuan transfer lintas batas dalam UU PDP. Hal ini merupakan instrumen hukum yang krusial untuk memastikan kedaulatan data dan mencegah eksploitasi informasi sensitif nasabah oleh pihak luar yang tidak bertanggung jawab.

Merujuk pada UU PDP, asas transparansi mewajibkan institusi perbankan untuk memberikan informasi yang jelas dan komprehensif kepada nasabah mengenai mekanisme pemrosesan data mereka dalam sistem AI anti-fraud. Hal ini mencakup rincian mengenai klasifikasi data yang diambil, periode retensi penyimpanan, hingga potensi keterlibatan pihak ketiga dalam pengolahan informasi tersebut. Keberadaan asas ini sangat vital karena nasabah memiliki hak untuk memahami logika sistem yang dapat berdampak langsung pada layanan keuangan mereka.(Pratama et al., 2025)

Di sisi lain, asas minimisasi data menekankan bahwa pengumpulan informasi harus dibatasi hanya pada data yang benar-benar esensial dan relevan dengan tujuan deteksi kecurangan. Namun dalam praktiknya, ketentuan ini masih menyisakan celah hukum karena tidak adanya parameter yang jelas mengenai batas “data yang relevan” dalam sistem berbasis AI. Hal ini membuka ruang bagi perbankan untuk melakukan pengumpulan data secara lebih luas dengan dalih meningkatkan akurasi sistem anti-fraud atau menjaga keamanan sistem keuangan. Praktik tersebut berpotensi menimbulkan over-collection of data dan function creep, yaitu penggunaan data yang melampaui tujuan awal pemrosesan.

Dengan demikian, bank secara hukum dilarang mengakumulasi data geolokasi maupun rekam jejak perilaku digital yang tidak memiliki urgensi langsung dalam mitigasi risiko fraud.(Syarifah et al., 2024) Namun dalam konteks AI, prinsip minimisasi tidak dapat dipahami secara sempit sebagai pembatasan kuantitas data, melainkan sebagai pembatasan berbasis justifikasi dan tujuan. Artinya, pengumpulan data dalam jumlah besar masih dimungkinkan sepanjang dapat dibuktikan relevansi dan kebutuhannya secara proporsional.

Dalam kerangka hukum perlindungan data, asas keamanan menetapkan standar teknis yang ketat bagi institusi perbankan, mulai dari penerapan enkripsi dan teknik pseudonimisasi data, hingga pemeliharaan audit log serta pelaksanaan pengujian penetrasi (penetration testing) secara sistematis untuk memitigasi risiko serangan siber. Beriringan dengan itu, asas akuntabilitas menegaskan bahwa beban pembuktian sepenuhnya berada di pihak perbankan institusi wajib mendemonstrasikan kepatuhan regulasi secara konkret apabila terjadi insiden keamanan atau kegagalan perlindungan data.

Lebih lanjut, asas proporsionalitas menginstruksikan agar upaya mitigasi risiko kecurangan (fraud) dilakukan secara seimbang tanpa melanggar privasi nasabah secara berlebihan. Oleh karena itu, sistem kecerdasan buatan (AI) wajib mengintegrasikan mekanisme

pengawasan manusia (human oversight) dalam setiap proses pengambilan keputusan yang bersifat krusial.(Legowo et al., 2024) Prinsip-prinsip ini pada dasarnya mencerminkan standar global yang selaras dengan General Data Protection Regulation (GDPR) Uni Eropa, yang sebagian ketentuannya telah diadopsi ke dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) guna memastikan ekosistem perbankan Indonesia memiliki ketahanan hukum yang setara dengan standar internasional.

Berdasarkan mandat Pasal 13 hingga 18 UU Nomor 27 Tahun 2022 (UU PDP), nasabah selaku subjek data pribadi dibekali dengan hak-hak fundamental yang mencakup hak akses, koreksi, penghapusan, hingga portabilitas data. Dalam operasional perbankan berbasis teknologi, instrumen hukum ini memungkinkan nasabah untuk memperoleh salinan data yang diolah oleh sistem kecerdasan buatan (AI anti-fraud), melakukan perbaikan atas informasi yang tidak akurat, hingga mengajukan permohonan penghapusan data secara permanen setelah masa retensi yang ditetapkan peraturan perundang-undangan berakhir.

Selain itu, hak nasabah untuk melakukan penarikan persetujuan pemrosesan data memunculkan dinamika tersendiri dalam praktik perbankan digital. Di satu sisi, sistem AI memerlukan asupan data yang kontinu untuk menjaga reliabilitas deteksi kecurangan namun di sisi lain, UU PDP secara tegas memprioritaskan perlindungan privasi individu dengan memberikan wewenang kepada nasabah untuk membatasi atau menghentikan pemrosesan data mereka. Konsekuensinya, institusi perbankan dituntut untuk menyelaraskan kebutuhan teknis keamanan sistem mereka dengan kewajiban hukum untuk memfasilitasi setiap permintaan hak subjek data secara transparan dan akuntabel.

Dalam kerangka hukum Indonesia, hak nasabah untuk tidak menjadi subjek tunggal dari pengambilan keputusan otomatis berlaku secara penuh apabila sistem kecerdasan buatan (AI) menghasilkan keputusan yang berdampak signifikan bagi nasabah. Dalam kondisi tersebut, nasabah memiliki wewenang hukum untuk menuntut adanya intervensi manusia sebagai bentuk validasi atas keputusan mesin. Guna mengimplementasikan hak ini secara efektif, institusi perbankan diwajibkan untuk menyediakan infrastruktur penunjang, seperti portal hak data pribadi yang terintegrasi di dalam aplikasi perbankan digital, sehingga nasabah dapat dengan mudah mengelola preferensi data mereka.

Kegagalan bank dalam memfasilitasi hak-hak subjek data tersebut tidak hanya berisiko pada sanksi administratif sesuai regulasi perlindungan data, tetapi juga dapat menjadi landasan yuridis yang kuat bagi nasabah untuk mengajukan tuntutan perdata. Dengan merujuk pada Undang-Undang Perlindungan Konsumen, setiap kerugian yang timbul akibat pengabaian hak data pribadi dapat diklasifikasikan sebagai pelanggaran kewajiban pelaku usaha, yang memberikan hak bagi nasabah untuk menuntut kompensasi atau ganti rugi atas dampak negatif yang dialami akibat operasional sistem AI yang tidak transparan.

Sebagai pengendali data pribadi, bank memikul tanggung jawab penuh atas seluruh siklus pemrosesan informasi dalam sistem AI anti-fraud, yang mencakup kewajiban menunjuk pejabat pelindung data (Data Protection Officer) serta melakukan penilaian dampak perlindungan data (DPIA) secara mendalam. Berdasarkan Peraturan OJK 2025, bank juga diwajibkan untuk melaksanakan audit periodik terhadap vendor penyedia teknologi AI guna menjamin kepatuhan yang konsisten terhadap standar keamanan. Meskipun demikian, data menunjukkan bahwa

sekitar 60% perbankan di Indonesia masih memiliki kelemahan dalam penyusunan DPIA yang komprehensif bagi sistem AI mereka, yang berpotensi menimbulkan risiko hukum di masa depan.

Pasal 46 UU PDP memberikan mandat yang tegas mengenai kewajiban notifikasi dalam kurun waktu 72 jam kepada OJK dan nasabah apabila terjadi kegagalan perlindungan data pengabaian terhadap kewajiban ini dapat berimplikasi pada sanksi administratif hingga sanksi pidana. Dalam hubungan dengan pihak ketiga, para prosesor data seperti vendor AI diwajibkan untuk menandatangani perjanjian pemrosesan data (Data Processing Agreement) yang membatasi penggunaan data hanya untuk tujuan yang disepakati. Sebagai langkah perlindungan tambahan, bank perlu memperkuat aspek kontraktual melalui pencantuman klausul indemnitas yang tegas, guna memastikan bahwa tanggung jawab hukum dan kerugian yang timbul akibat kelalaian vendor tetap teralokasi secara adil dan melindungi kepentingan institusi perbankan.

Otoritas Jasa Keuangan (OJK), melalui POJK Nomor 12/POJK.03/2021 tentang Bank Umum Digital, telah menetapkan standar ketat bagi pengamanan data dalam layanan keuangan digital yang mengintegrasikan teknologi kecerdasan buatan (AI). Regulasi ini kemudian diperkuat secara spesifik melalui Pedoman Tata Kelola AI Perbankan 2025, yang mengamanatkan penerapan prinsip etika, transparansi, serta inklusivitas sebagai pilar utama dalam pemanfaatan sistem AI anti-fraud. Hal ini bertujuan agar penggunaan teknologi tersebut tidak hanya efektif secara teknis, tetapi juga adil dan tidak diskriminatif terhadap kelompok nasabah mana pun.

Sejalan dengan otoritas sektor keuangan, Bank Indonesia melalui peta jalan (roadmap) pengembangan fintech nasional, secara konsisten mengintegrasikan aspek perlindungan data pribadi ke dalam sistem pengawasan pembayaran digital. Langkah strategis ini diambil untuk memastikan bahwa setiap inovasi dalam ekosistem keuangan tetap mengedepankan hak privasi konsumen sebagai bagian integral dari stabilitas sistem pembayaran digital di Indonesia. Sinergi regulasi ini menciptakan kerangka kerja yang komprehensif bagi perbankan untuk berinovasi melalui AI dengan tetap berada dalam koridor hukum yang akuntabel.

2. Tanggung Jawab Hukum Bank terhadap Penyalahgunaan atau Kebocoran Data Nasabah yang Timbul Dari Penggunaan Sistem Anti-Fraud Berbasis Artificial Intelligence

Walaupun sistem anti-fraud berbasis AI dapat dikembangkan bersama vendor teknologi atau pihak ketiga lainnya, bank tetap merupakan pihak yang memiliki hubungan hukum langsung dengan nasabah sehingga tanggung jawab hukum bank tetap menjadi hal yang utama. Banklah yang menentukan tujuan penggunaan teknologi, jenis data yang dikumpulkan, serta bagaimana data tersebut diproses dalam kegiatan operasional. Oleh karena itu, apabila terjadi penyalahgunaan atau kebocoran data nasabah, bank tidak dapat melepaskan tanggung jawab dengan alasan bahwa kesalahan berasal dari sistem otomatis atau dari penyedia teknologi. Penelitian mengenai tantangan adopsi AI di sektor perbankan menunjukkan bahwa permasalahan utama bukan hanya soal kemampuan teknis AI, tetapi juga menyangkut keamanan siber, kepatuhan terhadap regulasi, dan kesiapan tata kelola lembaga yang menggunakannya.(Simbolon et al., 2025) Artinya, penggunaan AI justru memperbesar kewajiban bank untuk menerapkan perlindungan hukum yang lebih kuat terhadap data nasabah.

Tanggung jawab hukum bank tidak hanya muncul ketika terjadi kebocoran data, tetapi juga sejak tahap perancangan dan penerapan sistem teknologi tersebut. Artinya, bank memiliki kewajiban untuk mencegah terjadinya risiko pelanggaran data sejak awal penggunaan sistem AI. Tanggung jawab ini sering dipahami sebagai tanggung jawab preventif, yaitu kewajiban untuk menerapkan berbagai langkah pengamanan sebelum terjadi pelanggaran. Bentuk tanggung jawab preventif dapat berupa penerapan sistem keamanan teknologi yang memadai, pembatasan akses terhadap data, pengujian terhadap model AI yang digunakan, serta pengawasan terhadap pihak ketiga yang terlibat dalam pengelolaan sistem tersebut.

Selain itu, penggunaan AI dalam sektor perbankan juga menuntut adanya tata kelola teknologi yang baik. Tata kelola ini mencakup transparansi penggunaan data, pengawasan terhadap algoritma yang digunakan, serta adanya keterlibatan manusia dalam proses pengambilan keputusan yang penting. Tanpa adanya pengawasan yang memadai, sistem AI dapat menghasilkan keputusan yang keliru atau tidak adil bagi nasabah. Misalnya, sistem dapat menandai transaksi yang sebenarnya sah sebagai transaksi mencurigakan sehingga menyebabkan pembatasan akses terhadap layanan perbankan. Situasi seperti ini dapat menimbulkan kerugian bagi nasabah serta memengaruhi kepercayaan masyarakat terhadap lembaga perbankan.

Salah satu risiko hukum yang paling konkret dari penggunaan sistem AI anti-fraud dalam perbankan adalah terjadinya false positive, yaitu kondisi di mana sistem secara keliru mengidentifikasi transaksi nasabah yang sah sebagai aktivitas mencurigakan atau fraudulent. Akibatnya, sistem secara otomatis memblokir rekening atau menolak transaksi tersebut tanpa ada intervensi manusia sebelumnya. Risiko ini bukan sekadar gangguan teknis dalam kondisi tertentu, false positive dapat menimbulkan kerugian nyata yang serius bagi nasabah.(Wiriani et al., 2025)

Sebagai ilustrasi, apabila seorang nasabah bermaksud melakukan transfer darurat untuk membayar tagihan rumah sakit, dan sistem AI memblokir transaksi tersebut secara otomatis karena dianggap tidak sesuai dengan pola perilaku historis nasabah, maka nasabah berpotensi mengalami kerugian materiil maupun immateriil secara bersamaan. Kerugian materiil berupa gagal bayar tagihan dan konsekuensi finansial yang mengikutinya, sementara kerugian immateriil berupa tekanan psikologis, hilangnya kepercayaan, dan gangguan atas hak mendapatkan layanan perbankan secara adil. Dalam konteks hukum perlindungan konsumen, kondisi ini dapat dikategorikan sebagai kegagalan pelaku usaha dalam memberikan layanan yang layak sebagaimana diamanatkan Pasal 4 huruf (a) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Studi terbaru menunjukkan bahwa tingkat false positive pada sistem AI anti-fraud masih menjadi tantangan yang belum sepenuhnya terselesaikan. Meskipun akurasi deteksi telah meningkat signifikan, kekeliruan sistem tetap berpeluang merugikan segmen nasabah tertentu, terutama nasabah dengan pola transaksi yang tidak umum atau tidak linear.(Pratama et al., 2025) Kondisi ini mempertegas urgensi pengaturan tanggung jawab hukum yang jelas bagi bank sebagai pihak yang memilih, mengoperasikan, dan mengawasi sistem tersebut.

Menghadapi gugatan nasabah yang dirugikan akibat false positive, bank acapkali berdalih bahwa keputusan pemblokiran dilakukan secara otomatis oleh sistem AI sehingga bank tidak dapat dimintai pertanggungjawaban atas keputusan tersebut. Argumen ini dalam doktrin hukum

dikenal sebagai upaya pelepasan tanggung jawab dengan berdalil pada "kesalahan mesin" (machine error defense). Secara hukum, argumentasi semacam ini tidak dapat diterima dan tidak memiliki pijakan yang kuat dalam sistem hukum Indonesia.

Bank sebagai pengendali data (data controller) adalah pihak yang secara sadar memilih untuk mengimplementasikan sistem AI, menentukan parameter deteksi fraud, mengintegrasikan sistem tersebut ke dalam operasional layanan, dan yang terpenting menyerahkan kewenangan pengambilan keputusan kepada algoritma tersebut. Dengan demikian, keputusan sistem AI secara hukum merupakan perpanjangan dari kehendak dan kebijakan bank itu sendiri.(Rahmawati et al., 2023) Apabila bank memilih untuk mendelegasikan keputusan yang berdampak langsung terhadap hak nasabah kepada sistem otomatis, maka bank juga harus menanggung seluruh konsekuensi hukum dari keputusan tersebut.

Dalam dimensi tanggung jawab perdata, terdapat doktrin yang sangat relevan untuk diterapkan terhadap bank pengguna AI, yaitu doktrin strict liability atau tanggung jawab mutlak. Berbeda dengan prinsip tanggung jawab berbasis kesalahan (fault-based liability) yang mengharuskan penggugat membuktikan adanya kelalaian atau kesengajaan pihak tergugat, strict liability menempatkan tanggung jawab pada pihak yang melakukan kegiatan berisiko tinggi (ultra-hazardous activity) meskipun tidak ada unsur kelalaian yang terbukti.(Lutfi, 2024) Doktrin ini memiliki relevansi yang kuat dalam konteks sistem AI anti-fraud karena beberapa alasan.

Pertama, sistem AI anti-fraud beroperasi dengan cara yang tidak sepenuhnya transparan bahkan bagi bank itu sendiri fenomena yang dikenal sebagai black box problem. Ketika keputusan diambil oleh model yang tidak sepenuhnya dapat dijelaskan, sangat sulit bagi nasabah yang dirugikan untuk membuktikan secara teknis di mana letak kesalahan atau kelalaian bank. Kedua, penggunaan sistem AI yang berpotensi memblokir rekening atau membatasi akses layanan keuangan secara massal dan otomatis dapat dikategorikan sebagai kegiatan yang mengandung risiko tinggi terhadap hak-hak nasabah. Ketiga, bank memiliki kapasitas teknis, sumber daya, dan akses informasi yang jauh lebih besar dibandingkan nasabah untuk mengelola dan memitigasi risiko tersebut.

Meskipun Kitab Undang-Undang Hukum Perdata Indonesia tidak secara eksplisit mengatur strict liability sebagaimana dikenal dalam tradisi common law, konsepnya dapat dijembatani melalui Pasal 1365 KUHPerdata yang mengatur perbuatan melawan hukum (onrechtmatige daad), serta Pasal 19 ayat (1) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang mewajibkan pelaku usaha memberikan ganti rugi atas kerugian konsumen akibat penggunaan produk atau jasa yang tidak sebagaimana mestinya. Lebih jauh, Pasal 46 ayat (2) UU PDP secara eksplisit menetapkan hak nasabah untuk memperoleh ganti kerugian atas pelanggaran pemrosesan data pribadi, tanpa mensyaratkan pembuktian niat jahat dari pihak bank.(Yuniari & I Dewa Ayu Dwi Mayasari, 2022) Sehingga bank bertanggung jawab atas kerugian yang ditimbulkan oleh sistem AI yang dioperasikannya, terlepas dari apakah kelalaian dapat dibuktikan.

Apabila dibandingkan dengan beberapa penelitian ilmiah terbaru, terlihat bahwa ada pola yang relatif sama dalam pembahasan AI dan fraud detection di sektor keuangan. Pertama, AI terbukti bermanfaat dalam meningkatkan efektivitas deteksi fraud dan mempercepat analisis data keuangan. Kedua, kelebihan tersebut selalu disertai dengan tantangan berupa risiko privasi,

lemahnya transparansi, potensi bias, dan persoalan akuntabilitas kelembagaan. Ketiga, penelitian yang menyoroti sektor perbankan menunjukkan bahwa kepercayaan publik terhadap AI tidak hanya bergantung pada kecanggihan teknologinya, tetapi juga pada kualitas tata kelola lembaga yang menerapkannya.(Pratama et al., 2025) Dari perbandingan tersebut dapat dipahami bahwa tanggung jawab hukum bank harus dilihat secara luas, yaitu mencakup seluruh siklus penggunaan AI, mulai dari perencanaan, pengumpulan data, pemrosesan, analisis, pengambilan keputusan, kerja sama dengan pihak ketiga, sampai penanganan dampak ketika sistem menimbulkan kerugian.

Dengan demikian, ada beberapa ukuran yang dapat digunakan untuk menilai apakah bank telah memenuhi tanggung jawab hukumnya. Pertama, apakah pemrosesan data benar-benar dibatasi untuk tujuan anti-fraud dan tidak meluas tanpa dasar yang jelas. Kedua, apakah bank telah menerapkan langkah teknis dan organisasional yang memadai untuk menjaga keamanan data. Ketiga, apakah sistem AI yang digunakan diawasi, diuji, dan dievaluasi secara berkala. Keempat, apakah ada pengawasan yang jelas terhadap vendor atau pihak ketiga. Kelima, apakah nasabah diberi ruang untuk memperoleh penjelasan, mengajukan keberatan, dan mendapatkan pemulihan apabila dirugikan oleh keputusan sistem. Apabila unsur-unsur tersebut tidak dipenuhi, maka argumentasi bahwa bank telah lalai akan semakin kuat. Sebaliknya, apabila bank dapat menunjukkan bahwa seluruh kewajiban preventif dan korektif telah dijalankan secara patut, maka penilaian tanggung jawab hukumnya dapat dipertimbangkan secara lebih proporsional.

Dalam perspektif hukum perbankan, kegagalan bank dalam menjaga keamanan data nasabah dapat dianggap sebagai pelanggaran terhadap prinsip kehati-hatian yang tertuang jelas pada Pasal 2 UU Perbankan. Prinsip kehati-hatian merupakan salah satu prinsip dasar dalam kegiatan perbankan yang mengharuskan bank menjalankan kegiatan usahanya secara hati-hati dan bertanggung jawab untuk melindungi kepentingan nasabah. Apabila bank menggunakan teknologi AI tanpa sistem pengamanan yang memadai atau tanpa pengawasan yang cukup, maka bank dapat dinilai tidak menjalankan prinsip kehati-hatian secara optimal. Hal ini terutama terjadi apabila penggunaan teknologi tersebut justru menimbulkan risiko baru bagi nasabah, seperti kebocoran data atau penyalahgunaan informasi pribadi.(Lutfi, 2024) Apabila kebocoran data atau penyalahgunaan data nasabah benar-benar terjadi akibat penggunaan sistem anti-fraud berbasis AI, maka bank dapat dimintai pertanggungjawaban hukum. Tanggung jawab tersebut pada umumnya dapat dilihat dari tiga bentuk, yaitu tanggung jawab perdata, tanggung jawab administratif, dan tanggung jawab pidana.

Pertama, Tanggung jawab perdata berkaitan dengan kewajiban bank untuk memberikan ganti rugi kepada nasabah apabila terjadi kerugian akibat kebocoran atau penyalahgunaan data pribadi. Dasar hukum utama yang dapat digunakan oleh nasabah untuk menuntut ganti rugi adalah ketentuan mengenai perbuatan melawan hukum yang telah diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata.

Dalam konteks penggunaan sistem anti-fraud berbasis AI, ketentuan tersebut dapat diterapkan apabila kebocoran data terjadi akibat kelalaian bank dalam mengelola atau mengamankan sistem teknologi yang digunakan termasuk dalam skenario false positive di mana bank dapat dikenai prinsip strict liability tanpa mensyaratkan pembuktian kelalaian secara teknis. Hak nasabah untuk menuntut ganti rugi juga diperkuat oleh Pasal 46 ayat (1) UU PDP yang

menyatakan bahwa setiap subjek data pribadi memiliki hak untuk mengajukan gugatan apabila terjadi pelanggaran terhadap pemrosesan data pribadinya.

Kedua, tanggung jawab administratif dapat timbul apabila bank dinilai melanggar ketentuan yang mengatur tata kelola dan perlindungan data dalam sektor perbankan. Dalam hal ini, otoritas pengawas perbankan yakni OJK atau lembaga pengawas PDP memiliki kewenangan untuk menjatuhkan sanksi kepada bank yang tidak mampu menjaga kerahasiaan data nasabah atau tidak menerapkan sistem pengamanan yang memadai. Sanksi administratif tersebut dapat berupa teguran tertulis, denda administratif, pembatasan kegiatan usaha, hingga pencabutan izin usaha dalam kondisi tertentu.

Ketiga, tanggung jawab pidana dapat muncul apabila kebocoran atau penyalahgunaan data terjadi karena adanya unsur kesengajaan atau kelalaian yang serius dalam pengelolaan sistem teknologi.(Annafa et al., 2024) Walaupun tanggung jawab pidana lebih sering dikenakan kepada individu yang terlibat langsung dalam pelanggaran, pengurus atau pihak yang bertanggung jawab atas pengelolaan sistem juga dapat dimintai pertanggungjawaban apabila terbukti mengabaikan kewajiban untuk menjaga keamanan data. Dalam situasi tertentu, pemrosesan data pribadi secara ilegal atau penyebaran data tanpa izin dapat dikategorikan sebagai pelanggaran hukum yang memiliki konsekuensi pidana.

Tanggung jawab hukum bank terhadap penyalahgunaan atau kebocoran data nasabah yang timbul dari penggunaan sistem anti-fraud berbasis artificial intelligence bersifat utama dan tidak dapat dialihkan begitu saja. Bank tetap menjadi subjek hukum yang paling bertanggung jawab karena bank adalah pihak yang menentukan penggunaan teknologi dan memproses data nasabah dalam rangka pencegahan fraud. Oleh karena itu, ketika terjadi kebocoran data, penyalahgunaan data, atau kerugian akibat keputusan sistem yang keliru termasuk dalam skenario false positive yang mengaktifkan prinsip strict liability bank tetap harus memikul tanggung jawab hukum, baik dalam bentuk pencegahan, pemulihan, maupun pertanggungjawaban atas kerugian yang timbul.(Rahmawati et al., 2023) rahrahsAI dalam sistem anti-fraud perbankan hanya dapat dibenarkan apabila inovasi teknologi berjalan beriringan dengan perlindungan yang nyata terhadap hak-hak nasabah.

KESIMPULAN

Dapat disimpulkan bahwa Pemanfaatan sistem anti-fraud berbasis Artificial Intelligence (AI) dalam sektor perbankan merupakan bentuk inovasi teknologi yang memiliki peran strategis dalam meningkatkan efektivitas deteksi serta pencegahan kejahatan finansial. Kemampuan AI dalam menganalisis data transaksi secara real time melalui algoritma pembelajaran mesin memungkinkan bank mengidentifikasi pola transaksi mencurigakan secara lebih cepat dan akurat dibandingkan metode konvensional. Namun demikian, penggunaan teknologi ini menimbulkan implikasi hukum yang signifikan, terutama berkaitan dengan pelindungan data pribadi nasabah karena sistem AI memerlukan pemrosesan data dalam jumlah besar yang bersifat sensitif. Dalam kerangka hukum nasional, penggunaan AI dalam sistem anti-fraud pada prinsipnya dapat dibenarkan sepanjang sejalan dengan ketentuan Undang-Undang Pelindungan Data Pribadi dan kewajiban kerahasiaan bank. Meskipun demikian, karakteristik AI yang bersifat data-hungry berpotensi menimbulkan ketegangan dengan prinsip minimisasi data sehingga masih terdapat ruang interpretasi yang memerlukan penguatan tata kelola data dan pengawasan yang lebih ketat. Selain

itu, dalam hal terjadi kesalahan identifikasi transaksi atau kebocoran data, bank sebagai pengendali dan penyelenggara sistem tetap memikul tanggung jawab hukum terhadap nasabah, baik dalam bentuk tanggung jawab perdata, administratif, maupun pidana, sehingga tidak dapat berlindung di balik alasan kesalahan teknologi. Oleh karena itu, penerapan AI dalam sistem anti-fraud perbankan harus disertai penguatan regulasi, tata kelola teknologi yang transparan dan akuntabel, serta penerapan prinsip kehati-hatian guna menjaga keseimbangan antara inovasi teknologi, keamanan sistem keuangan, dan pelindungan hak nasabah

DAFTAR PUSTAKA

Annafa, Syafa Widya, Hanintya Pasha Gabriel Hasa Simanjuntak, and Meira Ananda Ayudia. "Tanggung Jawab Hukum Bank Dalam Kasus Kebocoran Data Nasabah." *Jurnal Multidisiplin Ilmu Akademik* 1, no. 6 (2024): 129–35.

Awosika, Tomisin, Raj Mani Shukla, and Bernardi Pranggono. "Transparency and Privacy : The Role of Explainable AI and Federated Learning in Financial Fraud Detection." *IEEE Access* 12, no. April (2024): 64551–60. https://doi.org/10.1109/ACCESS.2024.3394528.

Ayunda, Rahmi, and Rusdianto. "Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence Dalam Aktifitas Perbankan Di Indonesia." *Jurnal Komunikasi Hukum* 7 (2021): 663–77.

Dr. Muhaimin, S.H., M.Hum. *METODE PENELITIAN HUKUM*, 2020.

Legowo, Mercurius Broto, Fangky Antoneus Sorongan, and Nurani Buaty. "Peran Kecerdasan Buatan Untuk Perlindungan Data Nasabah Dalam Aktivitas Operasional Sektor Perbankan." *LOFIAN: Jurnal Teknologi Informasi Dan Komunikasi* 4, no. 1 (2024). https://doi.org/10.58918/lofian.v4i1.252.

Lutfi, Melinda Putri. "URGENSI PERLINDUNGAN HUKUM TERHADAP DATA PRIVASI NASABAH BANK DI ERA PERKEMBANGAN DIGITAL." *Jurnal Multidisiplin Ilmu Akademik* 1, no. 5 (2024): 210–18.

Pratama, Andistya, Dwi Ratna, Indri Hapsari, and Listiyani Wulandari. "Bridging Regulation and Reality : A Comparative Study of Artificial Intelligence Regulation in the Financial Sectors." *LEGALITY: JURNAL ILMIAH HUKUM* 33, no. 2 (2025): 307–33.

Putro, Rizki Listyono, Titi Rapini, and Umi Farida. "Analisis Penerapan Kecerdasan Buatan (Artificial Intelligence) Untuk Meningkatkan Keamanan Finansial Nasabah Pada Sektor Perbankan Universitas Muhammadiyah Ponorogo , Indonesia," 2025.

Rahmawati, Irma Nurrizki, Nova Rahmadani, Diyah Rosita Heni, Sandro Kevin, and Perlindungan Hukum. "Pertanggung Jawaban Pihak Bank Terhadap Kebocoran Data Diri Nasabah." *Aufklarung : Jurnal Pendidikan , Sosial Dan Humaniora* 3, no. 2 (2023): 208–15.

Ramadhani, Fanny, and Diva Trimuliani. "PEMANFAATAN SISTEM ARTIFICIAL INTELLIGENCE PADA INDUSTRI PERBANKAN : SYSTEMATIC LITERATURE REVIEW" 9, no. 1 (2024): 37–49.

Simbolon, Novi Handayani, Fatma Dwi Jati, and Sondang Beatrix Siahaan. "Overcoming the Challenges of Ai Adoption in Banking Sector : Security , Regulation , and Infrastructure." *International Journal of Applied Finance and Business Studies Journal* 13, no. 1 (2025): 86–95.

Syarifah, Annisa, Alya Ananda, Zaskia Azzahra, and Catur Septiana Rakhmawati. "Implikasi Pasal 20 Dan 21 Undang Undang No . 27 Tahun 2022 Tentang Perlindungan Data Pribadi Terhadap

Bank Dalam Pemrosesan Data Biometrik Nasabah." *Prosiding Nasional Hukum Aktual*, no. 27 (2024): 481–93.

Wiriani, Erni, Jauharil Maknuni, Esti Alemia Puspita, and Masitah Masitah. "Peran Artificial Intelligence Dalam Mitigasi Risiko Transaksi Mobile Banking : Tinjauan Governansi Dan Etika Data." *Journal of Trends Economics and Accounting Research* 6, no. 1 (2025): 103–11. https://doi.org/10.47065/jtear.v6i1.2223.

Yuniari, I Dewa Ayu Wacik, and I Dewa Ayu Dwi Mayasari. "PERLINDUNGAN HUKUM DATA PRIBADI NASABAH APABILA BANK MENGGUNAKAN TEKNOLOGI ARTIFICIAL INTELLIGENCE MENURUT HUKUM POSITIF DI INDONESIA." *Jurnal Kertha Negara* 10, no. 7 (2022): 665–75.