

## ASPEK HUKUM CYBERCRIME TERHADAP MODUS SCAM PINJAMAN ONLINE BERBASIS ARTIFICIAL INTELLIGENCE

**Rohmatul Karimah**

Fakultas Hukum Pasca Sarjana Universitas Lampung  
[rohmatulkarimah8@gmail.com](mailto:rohmatulkarimah8@gmail.com)

**Ahmad Irzal Fardiansyah**

Fakultas Hukum Pasca Sarjana Universitas Lampung  
[ahmad.irzal@fh.unila.ac.id](mailto:ahmad.irzal@fh.unila.ac.id)

**Fristia Berdian Tamza**

Fakultas Hukum Pasca Sarjana Universitas Lampung  
[fristia.berdian@fh.unila.ac.id](mailto:fristia.berdian@fh.unila.ac.id)

### ABSTRAK

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) telah membawa dampak signifikan terhadap sektor keuangan digital di Indonesia. Di satu sisi, teknologi ini mempercepat layanan pinjaman online (*fintech lending*) yang efisien, namun di sisi lain memunculkan modus kejahatan baru berupa *financial scam* yang semakin kompleks. Modus penipuan pinjaman online berbasis AI melibatkan rekayasa digital melalui *deepfake*, *chatbot phishing*, serta manipulasi data pribadi yang digunakan untuk memperoleh keuntungan ilegal. Penelitian ini bertujuan untuk menganalisis aspek hukum *cybercrime* dalam praktik *scam* pinjaman online berbasis AI dengan menggunakan pendekatan yuridis normatif melalui telaah terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Hasil penelitian menunjukkan bahwa modus kejahatan pinjaman online berbasis AI merupakan bentuk kejahatan siber terorganisir yang menuntut penegakan hukum berbasis teknologi. Diperlukan pembaruan hukum pidana siber serta kolaborasi antara Otoritas Jasa Keuangan (OJK), Kepolisian, dan Kementerian Kominfo dalam mengembangkan sistem *Regulatory Technology (RegTech)* untuk mendeteksi dan mencegah *AI-driven scam*.

**Kata kunci:** Cybercrime, Artificial Intelligence, Pinjaman Online, Scam Keuangan, Hukum Digital

### ABSTRACT

The development of Artificial Intelligence (AI) has significantly impacted Indonesia's digital finance sector. While AI enhances efficiency in online lending (*fintech lending*) services, it also introduces sophisticated financial scams. AI-driven online loan scams involve digital manipulation through *deepfakes*, *chatbot phishing*, and personal data misuse for illegal profit. This study aims to analyze the legal aspects of cybercrime in AI-based financial scams using a normative juridical approach, focusing on Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 4 of 2023 on Financial Sector Development and Reinforcement, and Law No. 27 of 2022 on Personal Data Protection. The findings indicate that AI-driven loan scams represent a form of organized cybercrime that requires technology-based law enforcement. Legal reform and institutional collaboration between the Financial Services Authority (OJK), the Police, and the Ministry of Communication and Information are essential to implement Regulatory Technology (RegTech) as a preventive and control mechanism for AI-related scams.

**Keywords:** Cybercrime, Artificial Intelligence, Online Lending, Financial Scam, Digital Law.

## PENDAHULUAN

Perkembangan teknologi digital dalam dekade terakhir telah membawa perubahan fundamental terhadap tata kehidupan masyarakat, termasuk dalam bidang ekonomi dan hukum. Revolusi industri 4.0 yang ditandai dengan munculnya *Artificial Intelligence (AI)*, *machine learning*, dan *big data analytics* telah mendorong munculnya berbagai inovasi di sektor keuangan digital. Salah satu bentuknya adalah layanan *financial technology* (fintech) yang menawarkan kemudahan akses pinjaman secara daring (*online lending*) tanpa prosedur administratif yang rumit sebagaimana sistem perbankan konvensional. Namun, di balik kemudahan dan efisiensi tersebut, muncul pula fenomena negatif berupa penyalahgunaan teknologi kecerdasan buatan untuk melakukan kejahatan finansial (*financial scam*), khususnya dalam bentuk *pinjaman online ilegal* yang semakin kompleks dan sulit dilacak.

Fenomena *AI-driven financial scam* atau penipuan keuangan berbasis kecerdasan buatan merupakan perkembangan baru dalam lanskap kejahatan siber (*cybercrime*). Modus ini menggunakan algoritma cerdas, *chatbot*, *deepfake*, dan sistem otomatis yang meniru komunikasi manusia untuk menipu korban, mencuri data pribadi, dan mengajukan pinjaman fiktif atas nama pihak lain. Berbeda dengan modus penipuan konvensional, pelaku kejahatan digital kini mampu memanfaatkan teknologi *natural language processing* dan *deep learning* untuk menyesuaikan pola percakapan dengan karakteristik korban, sehingga tingkat keberhasilan penipuan meningkat secara signifikan.

Laporan Otoritas Jasa Keuangan (OJK) tahun 2024 menunjukkan bahwa kasus pinjaman online ilegal meningkat hingga 38% dibandingkan tahun 2023, dengan pola penipuan yang sebagian besar melibatkan sistem otomatis berbasis kecerdasan buatan. Sementara itu, Kementerian Komunikasi dan Informatika (Kominfo) dalam laporan resminya per Oktober 2024 menyebutkan bahwa lebih dari 9.000 situs dan aplikasi pinjaman online ilegal telah diblokir selama dua tahun terakhir, namun sebagian di antaranya muncul kembali dengan identitas digital baru yang lebih canggih dan anonim. Hal ini menunjukkan bahwa perlawanan hukum terhadap kejahatan siber memerlukan mekanisme yang adaptif dan berbasis teknologi.<sup>1</sup>

Secara normatif, pengaturan hukum terhadap tindak pidana siber di Indonesia telah diatur dalam beberapa instrumen hukum, di antaranya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kedua regulasi tersebut menjadi pilar utama dalam melindungi masyarakat dari penyalahgunaan data dan informasi elektronik. Pasal 30 sampai dengan Pasal 33 UU ITE menegaskan larangan akses ilegal terhadap sistem elektronik, sementara Pasal 65 UU PDP mengatur sanksi pidana bagi pihak yang dengan sengaja menggunakan data pribadi untuk memperoleh keuntungan secara melawan hukum.

Dalam konteks sektor keuangan, pengawasan terhadap aktivitas pinjaman online berada di bawah kewenangan Otoritas Jasa Keuangan (OJK) sebagaimana ditegaskan dalam Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK). Pasal 228 ayat (1) UU tersebut mewajibkan seluruh penyelenggara layanan keuangan digital, termasuk platform pinjaman online berbasis AI, untuk terdaftar dan memperoleh izin dari OJK. Pelanggaran terhadap ketentuan ini dikategorikan sebagai kegiatan keuangan ilegal yang dapat dikenakan sanksi administratif maupun pidana. Namun demikian, munculnya praktik kejahatan

---

<sup>1</sup> Otoritas Jasa Keuangan Republik Indonesia. (2024). *Laporan Tahunan OJK: Pengawasan Fintech Lending dan Tantangan AI dalam Sektor Keuangan Digital*. Jakarta: OJK Press.

berbasis AI sering kali melampaui kemampuan regulasi konvensional dalam mendeteksi dan menindak pelaku, terutama karena teknologi AI dapat digunakan untuk *spoofing*, *voice cloning*, dan *identity manipulation* secara masif dan anonim.

Dari perspektif hukum pidana, kejahatan pinjaman online berbasis AI dapat dikualifikasikan sebagai bentuk tindak pidana penipuan elektronik dan akses ilegal terhadap sistem keuangan digital, sebagaimana diatur dalam Pasal 35 dan Pasal 46 UU ITE. Namun, kompleksitas AI menimbulkan persoalan baru dalam aspek *mens rea* (niat jahat) dan *liability attribution* (pertanggungjawaban pidana), terutama ketika tindakan dilakukan oleh sistem otomatis yang dikendalikan algoritma. Hal ini menimbulkan perdebatan di kalangan akademisi hukum terkait dengan *artificial criminal liability*, yakni konsep tanggung jawab hukum terhadap sistem kecerdasan buatan yang beroperasi semi-otonom dan menyebabkan kerugian hukum bagi pihak lain.<sup>2</sup>

Selain aspek pidana, dimensi perlindungan konsumen juga menjadi perhatian utama. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan jaminan hak atas keamanan, kenyamanan, dan keselamatan konsumen dalam mengakses produk dan jasa, termasuk jasa keuangan digital. Dalam konteks pinjaman online berbasis AI, pelanggaran hak konsumen dapat terjadi ketika data pribadi digunakan tanpa persetujuan, atau ketika korban dijejek melalui antarmuka aplikasi palsu yang menyerupai lembaga keuangan resmi. Oleh karena itu, keberadaan AI dalam aktivitas keuangan menuntut mekanisme hukum baru yang menggabungkan aspek keamanan data, transparansi algoritma, dan tanggung jawab platform digital.

Dari sudut pandang kebijakan publik, pemerintah Indonesia telah melakukan berbagai langkah strategis untuk menghadapi kejahatan siber di sektor keuangan. Pembentukan Satuan Tugas Pemberantasan Pinjaman Online Ilegal (Satgas PASTI) pada tahun 2023 menjadi langkah sinergis antara OJK, Bank Indonesia, Kominfo, dan Kepolisian RI. Namun, efektivitas penegakan hukum masih menghadapi tantangan serius, antara lain:

1. Keterbatasan kompetensi aparat penegak hukum dalam memahami algoritma dan bukti digital berbasis AI;
2. Kurangnya regulasi turunan yang mengatur penggunaan teknologi AI di sektor keuangan secara spesifik;
3. Keterlambatan mekanisme pelaporan dan pelacakan lintas negara, karena banyak pelaku menggunakan server di luar yurisdiksi Indonesia; dan
4. Ketidadaan standar hukum tentang transparansi algoritmik, yang membuat masyarakat tidak mengetahui cara AI memproses dan menyebarkan data keuangan mereka.

Dalam kerangka teori hukum, fenomena *AI-driven financial scam* menunjukkan pergeseran paradigma hukum dari *rule-based regulation* menuju *risk-based regulation*, di mana hukum tidak hanya mengatur perilaku, tetapi juga mengantisipasi risiko yang ditimbulkan oleh perkembangan teknologi. Sebagaimana dikemukakan oleh Satjipto Rahardjo dalam teori *hukum progresif*, hukum harus bersifat dinamis dan adaptif terhadap perubahan sosial. Pendekatan hukum progresif menuntut negara untuk tidak hanya menjadi pengendali (*law as control*), tetapi juga fasilitator bagi pembentukan hukum baru yang responsif terhadap perkembangan digital.<sup>3</sup>

Lebih jauh lagi, konsep Regulatory Technology (*RegTech*) mulai diperkenalkan sebagai instrumen pengawasan digital berbasis hukum, di mana pemerintah dapat menggunakan sistem analitik dan AI untuk memantau aktivitas keuangan daring, termasuk mendeteksi *pattern recognition*

---

<sup>2</sup> Hamzah, Andi. (2008). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.

<sup>3</sup> Rahardjo, Satjipto. (2011). *Hukum Progresif: Urgensi dan Kritik*. Jakarta: Epistema & HuMa.

atas transaksi mencurigakan. Penerapan *RegTech* menjadi bagian dari upaya transformasi hukum agar lebih mampu menghadapi tantangan era keuangan digital berbasis kecerdasan buatan.

Kajian ini menjadi penting karena perkembangan teknologi kecerdasan buatan tidak dapat dibendung, sementara hukum positif Indonesia masih berorientasi pada sistem *reactive regulation* yang cenderung tertinggal dari dinamika teknologi. Oleh karena itu, dibutuhkan rekonstruksi hukum siber dan kebijakan perlindungan konsumen digital yang mampu menjawab realitas kejahatan keuangan berbasis AI, dengan mengedepankan asas kepastian hukum, kemanfaatan, dan keadilan sebagaimana menjadi pilar utama dalam sistem hukum nasional.

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yakni penelitian hukum yang berfokus pada analisis norma, asas, dan sistem hukum yang berlaku dengan menitikberatkan pada bahan pustaka (*library research*) dan peraturan perundang-undangan yang relevan. Pendekatan ini dipilih karena permasalahan yang dikaji berkaitan langsung dengan pengaturan hukum positif Indonesia terhadap fenomena *scam pinjaman online berbasis Artificial Intelligence (AI)* sebagai bentuk baru dari kejahatan siber (*cybercrime*) di sektor keuangan digital.

Menurut Soerjono Soekanto, penelitian hukum normatif dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai dasar utama dalam menganalisis kaidah hukum yang berlaku. Dalam konteks ini, fokus penelitian diarahkan untuk memahami bagaimana hukum positif Indonesia mengatur, melindungi, dan menanggulangi praktik kejahatan finansial berbasis AI yang semakin kompleks.<sup>4</sup>

Penelitian ini menggunakan beberapa pendekatan, antara lain:<sup>5</sup>

Pendekatan ini digunakan untuk mengkaji peraturan perundang-undangan yang menjadi dasar hukum terhadap kejahatan siber dan penyelenggaraan layanan pinjaman online berbasis teknologi di Indonesia. Analisis dilakukan terhadap konsistensi dan efektivitas peraturan yang berlaku dalam melindungi masyarakat dari *AI-driven scam*. Beberapa peraturan yang menjadi fokus analisis antara lain:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) jo. Undang-Undang Nomor 19 Tahun 2016, yang mengatur perbuatan melawan hukum dalam sistem elektronik, termasuk akses ilegal, manipulasi data, dan penipuan digital;
2. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengatur kewajiban pelaku usaha untuk melindungi data pribadi pengguna dari penyalahgunaan teknologi AI;
3. Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK), yang menegaskan bahwa seluruh penyelenggara *financial technology* wajib terdaftar dan diawasi oleh OJK;
4. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, khususnya Pasal 4 dan Pasal 8 yang melarang pelaku usaha memperdagangkan produk atau jasa yang dapat menimbulkan kerugian konsumen;
5. Peraturan Otoritas Jasa Keuangan (POJK) Nomor 10 Tahun 2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi, yang mengatur prinsip kehati-hatian

---

<sup>4</sup> Soekanto, Soerjono. 1986. *Pengantar Penelitian Hukum*. Jakarta: UI Press.

<sup>5</sup> Zainuddin, Ali. (2014). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

dan tanggung jawab platform pinjaman online dalam menjaga keamanan data dan transaksi;

6. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Privat, yang menjadi dasar pengawasan terhadap sistem digital berbasis AI yang beroperasi di Indonesia;
7. Konvensi Budapest 2001 tentang Cybercrime dan ASEAN Cybersecurity Cooperation Strategy 2021–2025, yang menjadi acuan internasional bagi kerja sama lintas negara dalam penanggulangan kejahatan siber.

Pendekatan ini bertujuan untuk menilai sejauh mana peraturan-peraturan tersebut mampu menjawab tantangan kejahatan finansial yang memanfaatkan teknologi kecerdasan buatan dalam ruang siber Indonesia.

Pendekatan ini digunakan untuk memahami dan menelaah konsep-konsep hukum yang relevan dengan permasalahan penelitian. Beberapa konsep hukum yang menjadi fokus antara lain:

1. Konsep Kejahatan Siber (Cybercrime), yaitu kejahatan yang dilakukan melalui sistem komputer atau jaringan elektronik untuk memperoleh keuntungan secara melawan hukum;
2. Konsep Tanggung Jawab Hukum terhadap AI (Algorithmic Liability), yaitu teori hukum yang menjelaskan pertanggungjawaban atas tindakan atau hasil keputusan sistem kecerdasan buatan yang menimbulkan kerugian hukum;
3. Konsep Perlindungan Data Pribadi, yaitu hak fundamental warga negara untuk mengontrol informasi pribadinya dari pengumpulan dan pemrosesan data secara ilegal;
4. Konsep Hukum Ekonomi Digital, yang menekankan keseimbangan antara inovasi teknologi dengan perlindungan kepentingan publik;
5. Konsep Hukum Progresif (Progressive Law), sebagaimana dikemukakan oleh Satjipto Rahardjo, yang menempatkan hukum sebagai sarana rekayasa sosial untuk menyesuaikan diri terhadap perubahan perilaku dan struktur sosial di era digital.

Pendekatan konseptual ini penting karena kejahatan finansial berbasis AI bukan hanya persoalan teknis, melainkan juga problem etika hukum dan tanggung jawab sosial penyedia teknologi. Dengan memahami konsep-konsep dasar tersebut, penelitian ini dapat memberikan kerangka teoritis dalam merumuskan arah pembaruan hukum ke depan.

Pendekatan ini digunakan untuk menganalisis praktik penegakan hukum dan putusan pengadilan yang berkaitan dengan kejahatan siber di sektor keuangan. Beberapa kasus yang relevan antara lain:

1. Kasus Pinjol Ilegal “AdaKami” (2023), di mana terjadi dugaan pelanggaran privasi dan intimidasi terhadap pengguna yang datanya disalahgunakan oleh sistem otomatis berbasis AI;
2. Kasus Penipuan Deepfake Bank Digital (2024) yang diungkap oleh Direktorat Siber Bareskrim Polri, di mana pelaku menggunakan *voice cloning* untuk meniru pejabat bank dalam meyakinkan korban untuk mentransfer dana;
3. Kasus Penyalahgunaan Data Pribadi di Platform Fintech Peer-to-Peer Lending (2022) yang mengakibatkan ribuan pengguna mengalami kerugian finansial akibat algoritma rekomendasi palsu.

Melalui pendekatan ini, penelitian berupaya menilai sejauh mana norma hukum diterapkan dalam praktik serta efektivitas sistem peradilan dalam menangani kejahatan digital berbasis AI.

Sumber dan Jenis data yang digunakan adalah data sekunder, yang meliputi:

1. Bahan hukum primer, yaitu peraturan perundang-undangan nasional, konvensi internasional, dan putusan pengadilan yang relevan;
2. Bahan hukum sekunder, yaitu buku, artikel ilmiah, hasil penelitian, laporan OJK dan Kominfo, serta pendapat ahli hukum yang berkaitan dengan kejahatan siber dan hukum teknologi;
3. Bahan hukum tersier, seperti kamus hukum, ensiklopedia hukum digital, serta dokumen resmi lembaga internasional (OECD, ASEAN, dan World Bank) mengenai *AI ethics and digital regulation*.

Data dikumpulkan melalui penelitian kepustakaan (*library research*) dengan cara menelusuri peraturan perundang-undangan, jurnal akademik, serta laporan resmi pemerintah yang relevan dengan isu *cyber financial crime*.

Data yang telah dikumpulkan kemudian diolah melalui proses:

1. Inventarisasi terhadap seluruh norma hukum yang berkaitan dengan kejahatan digital dan penggunaan AI di sektor keuangan;
2. Klasifikasi berdasarkan tingkat hierarki dan relevansi norma hukum (nasional, internasional, dan sektoral);
3. Interpretasi hukum melalui penafsiran sistematis terhadap pasal-pasal dalam UU ITE, UU PDP, dan UU P2SK;
4. Analisis komparatif antara kebijakan hukum Indonesia dengan praktik internasional (terutama Singapura, Korea Selatan, dan Uni Eropa) dalam menangani *AI-driven cybercrime*; dan
5. Penarikan kesimpulan hukum melalui metode analisis yuridis kualitatif untuk menghasilkan rekomendasi pembaruan regulasi.

Analisis yuridis kualitatif digunakan untuk menafsirkan norma hukum dan menilai efektivitasnya dalam konteks sosial digital. Dengan demikian, penelitian ini tidak hanya bersifat deskriptif, tetapi juga analitis dan preskriptif, yakni memberikan rekomendasi hukum yang relevan bagi pembuat kebijakan dan lembaga penegak hukum di Indonesia.

## HASIL DAN PEMBAHASAN

Perkembangan teknologi kecerdasan buatan telah mengubah lanskap kejahatan siber secara signifikan. Dalam konteks layanan keuangan digital, AI dimanfaatkan tidak hanya oleh lembaga resmi untuk meningkatkan efisiensi dan *risk management*, tetapi juga oleh pelaku kejahatan untuk meluncurkan berbagai modus penipuan finansial (*financial scam*). Modus penipuan pinjaman online berbasis AI (*AI-driven scam*) merupakan bentuk lanjutan dari praktik *cyber fraud* yang memadukan kemampuan analisis data masif (*big data analytics*) dengan sistem otomatis untuk meniru perilaku manusia secara meyakinkan.

Secara umum, terdapat beberapa pola *modus operandi* yang ditemukan dalam kasus *AI-based scam*, antara lain:

1. Deepfake Communication, yaitu penggunaan algoritma AI untuk meniru wajah, suara, atau gestur seseorang guna meyakinkan korban bahwa ia berinteraksi dengan pihak resmi seperti petugas bank atau lembaga keuangan.
2. Chatbot Phishing, yakni sistem percakapan otomatis yang dirancang untuk memancing informasi pribadi pengguna (Nomor Induk Kependudukan, nomor rekening, OTP, dan sebagainya).

3. Synthetic Identity Fraud, yaitu penciptaan identitas digital baru hasil gabungan beberapa data pribadi korban, yang kemudian digunakan untuk mengajukan pinjaman fiktif atau memanipulasi transaksi.
4. Algorithmic Loan Manipulation, di mana AI dimanfaatkan untuk mengubah atau meniru hasil evaluasi kredit digital agar permohonan pinjaman ilegal terlihat valid di sistem.
5. Voice Cloning dan Impersonation Fraud, yaitu pemanfaatan teknologi *text-to-speech AI* untuk meniru suara pejabat atau pihak terpercaya yang meminta transfer dana atau verifikasi data.

Fenomena tersebut menunjukkan bahwa kecerdasan buatan kini menjadi instrumen baru dalam kejahatan finansial digital. Hal ini menimbulkan tantangan serius bagi sistem hukum, sebab kejahatan dilakukan bukan lagi oleh individu manusia semata, tetapi juga oleh sistem algoritmik yang dapat berjalan secara otonom.

Laporan Direktorat Tindak Pidana Siber Bareskrim Polri tahun 2024 mencatat bahwa lebih dari 2.000 kasus penipuan digital menggunakan sistem AI telah ditangani dalam dua tahun terakhir, dengan kerugian masyarakat mencapai Rp1,4 triliun. Jumlah ini menunjukkan peningkatan signifikan dibandingkan tahun sebelumnya, yang hanya sekitar 800 kasus. Kasus-kasus tersebut umumnya melibatkan penggunaan data pribadi dari korban yang diperoleh melalui pelanggaran privasi atau kebocoran data (*data breach*).<sup>6</sup>

Dalam perspektif hukum positif, tindak pidana penipuan berbasis AI dapat dikualifikasikan sebagai bagian dari *cybercrime* yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Pasal 28 ayat (1) UU ITE menyatakan bahwa:

“Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Ketentuan ini relevan terhadap modus penipuan digital yang dilakukan dengan *deepfake communication* dan *chatbot phishing*, di mana pelaku menggunakan sistem elektronik untuk menyebarkan informasi palsu yang menimbulkan kerugian finansial bagi masyarakat.

Selain itu, Pasal 35 UU ITE menegaskan bahwa:

“Setiap orang dengan sengaja dan tanpa hak memanipulasi, menciptakan, mengubah, menghapus, merusak, atau membuat tidak berfungsinya suatu informasi elektronik atau dokumen elektronik dengan tujuan agar seolah-olah data tersebut otentik, dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).”

Dalam konteks *AI-based financial scam*, perbuatan ini mencakup pembuatan identitas palsu melalui *synthetic data generation* untuk mengajukan pinjaman fiktif. Oleh karena itu, sistem hukum nasional telah memiliki dasar normatif untuk menindak pelaku kejahatan AI-driven scam meskipun teknologi yang digunakan semakin kompleks.

---

<sup>6</sup> Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Laporan Nasional Penanganan Pinjaman Online Ilegal dan Kejahatan Siber*. Jakarta: Kominfo.

Namun, yang menjadi persoalan adalah aspek pembuktian digital (*digital forensic evidence*). Dalam banyak kasus, pelaku menggunakan *server* luar negeri dan sistem *proxy AI* yang menyulitkan pelacakan. Selain itu, pertanggungjawaban pidana menjadi kabur ketika tindakan dilakukan melalui sistem otomatis yang tidak memiliki unsur kehendak (*mens rea*) manusia. Kondisi ini menunjukkan keterbatasan UU ITE yang masih berorientasi pada subjek hukum manusia, belum menyentuh entitas hukum digital seperti *autonomous systems* atau *AI agents*.

Kejahatan pinjaman online berbasis AI hampir selalu berawal dari kebocoran data pribadi. Penggunaan AI untuk menganalisis perilaku digital, merekam biometrik wajah, atau memproses data tanpa izin melanggar prinsip dasar Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Pasal 46 ayat (1) UU PDP mengatur bahwa:

“Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau pihak lain yang dapat mengakibatkan kerugian bagi subjek data pribadi.”

Pelanggaran terhadap pasal ini diancam pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp5.000.000.000,00. Ketentuan ini dapat diterapkan terhadap pelaku *data harvesting* yang menggunakan AI untuk mengumpulkan dan mengolah data tanpa izin pengguna. Selain itu, UU PDP mengatur tanggung jawab penyelenggara sistem elektronik untuk menerapkan prinsip keamanan siber adaptif (*adaptive cybersecurity*) dalam melindungi data pribadi pengguna. Namun, dalam praktiknya banyak platform pinjaman online ilegal yang tidak menerapkan sistem keamanan berbasis *encryption* dan *multi-factor authentication*, sehingga memudahkan pelaku kejahatan memanipulasi data nasabah.

Dengan demikian, pelanggaran terhadap UU PDP bukan hanya bersifat administratif, tetapi juga memiliki dimensi pidana yang signifikan ketika digunakan untuk tujuan penipuan finansial berbasis AI.

Regulasi terkait aktivitas pinjaman online secara eksplisit diatur dalam Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) serta Peraturan Otoritas Jasa Keuangan (POJK) Nomor 10 Tahun 2022. Pasal 228 ayat (1) UU P2SK mewajibkan penyelenggara *financial technology* untuk terdaftar dan memperoleh izin dari OJK. Platform yang beroperasi tanpa izin dianggap sebagai lembaga keuangan ilegal. Selain itu, POJK 10/2022 Pasal 26 ayat (2) mengharuskan setiap penyelenggara fintech menerapkan sistem perlindungan data dan keamanan transaksi yang memenuhi standar teknologi informasi, termasuk penggunaan *AI ethics framework* dalam pengambilan keputusan algoritmik.<sup>7</sup>

Namun dalam realitasnya, ribuan platform pinjaman online ilegal masih beroperasi di luar pengawasan OJK. Penggunaan AI justru memperumit penelusuran karena sistem tersebut mampu menyembunyikan *source code*, menyamarkan lokasi server, dan meniru identitas perusahaan legal. Oleh karena itu, pengawasan hukum berbasis manusia perlu ditransformasikan ke arah *Regulatory Technology (RegTech)*, di mana OJK dan Kominfo menggunakan algoritma pengawasan otomatis untuk mendeteksi aktivitas keuangan ilegal secara real time.

Penerapan *RegTech* ini sejalan dengan prinsip hukum progresif yang dikemukakan oleh Satjipto Rahardjo, bahwa hukum tidak boleh tertinggal dari perubahan sosial. Dalam konteks digital, hukum harus bertransformasi menjadi “*smart regulation*” sistem hukum yang mampu

---

<sup>7</sup> Sari, L. D. (2023). “Analisis Yuridis terhadap Penyalahgunaan Data Pribadi dalam Layanan Pinjaman Online.” *Jurnal Hukum dan Transformasi Digital*, Vol. 4 No. 1.



mengawasi dan menegakkan norma melalui teknologi yang sama dengan yang digunakan pelaku kejahatan.

Penegakan hukum terhadap kejahatan finansial berbasis AI di Indonesia masih menghadapi berbagai tantangan struktural dan normatif, antara lain:<sup>8</sup>

1. Ketiadaan regulasi spesifik tentang kecerdasan buatan.

Hingga tahun 2025, Indonesia belum memiliki undang-undang khusus yang mengatur penggunaan AI, termasuk tanggung jawab hukum terhadap algoritma atau sistem otomatis yang menyebabkan kerugian.

2. Keterbatasan kapasitas lembaga penegak hukum.

Banyak aparat belum memiliki kompetensi teknis dalam menganalisis bukti digital yang dihasilkan oleh sistem AI (*AI forensic*), sehingga proses pembuktian sering kali tidak efektif.

3. Tantangan lintas yurisdiksi.

Sebagian besar server yang digunakan oleh pelaku kejahatan digital berbasis AI berada di luar negeri, sehingga penegakan hukum membutuhkan kerja sama internasional yang lebih intensif melalui *Mutual Legal Assistance (MLA)* dan *ASEAN Cybersecurity Framework*.

4. Aspek etika dan transparansi algoritmik.

AI yang digunakan dalam sektor keuangan tidak selalu memiliki transparansi keputusan (*algorithmic transparency*), sehingga sulit menentukan apakah kesalahan sistem merupakan kejahatan atau kegagalan teknis.

Melihat kompleksitas tersebut, arah pembaruan hukum perlu diarahkan pada:

- Penyusunan Rancangan Undang-Undang Kecerdasan Buatan (RUU AI) yang mengatur aspek etika, tanggung jawab hukum, dan perlindungan hak konsumen digital;
- Integrasi sistem pengawasan RegTech dan SupTech (Supervisory Technology) di bawah OJK dan Kominfo;
- Peningkatan kapasitas penegak hukum melalui pelatihan digital forensik dan penegakan hukum lintas batas; serta
- Kolaborasi internasional dengan negara-negara ASEAN untuk membentuk *regional AI regulation framework* sebagai upaya pencegahan kejahatan finansial digital.

Dengan demikian, dapat disimpulkan bahwa hukum positif Indonesia sebenarnya telah memiliki dasar normatif dalam UU ITE, UU PDP, dan UU P2SK untuk menindak *AI-based financial scam*, namun diperlukan pembaruan hukum yang bersifat adaptif, integratif, dan berbasis teknologi agar penegakan hukum mampu menjawab dinamika kejahatan siber modern.<sup>9</sup>

Berdasarkan uraian tersebut dapat dilihat bahwa perkembangan kecerdasan buatan (*Artificial Intelligence/ AI*) di bidang keuangan digital menghadirkan dilema hukum yang kompleks bagi sistem hukum nasional. Di satu sisi, AI berperan penting dalam meningkatkan efisiensi, aksesibilitas, dan inovasi layanan pinjaman online (*fintech lending*). Namun di sisi lain, teknologi ini juga menciptakan bentuk kejahatan finansial baru yang bersifat otonom, sulit dilacak, dan melibatkan jaringan lintas yurisdiksi.

Dari sisi regulasi, Indonesia sebenarnya telah memiliki kerangka hukum yang cukup memadai melalui UU ITE, UU PDP, dan UU P2SK. Namun, ketiga instrumen hukum tersebut

---

<sup>8</sup> Pratama, A. (2023). "Penegakan Hukum terhadap Kejahatan Siber di Sektor Keuangan Digital." *Jurnal Ilmu Hukum Lex Renaissance*, Vol. 8 No. 2.

<sup>9</sup> Susanto, R. & Widjaja, F. (2022). "Artificial Intelligence and Algorithmic Liability: Legal Challenges in Financial Technology Regulation." *Indonesian Journal of Law and Technology*, Vol. 7 No. 3.

belum sepenuhnya mampu menjawab kompleksitas kejahatan berbasis algoritma karena belum mengenal subjek hukum non-manusia (entitas digital) serta belum menetapkan mekanisme pertanggungjawaban pidana terhadap sistem otomatis yang beroperasi secara independen. Akibatnya, penegakan hukum masih bersifat *reactive enforcement* baru bertindak setelah kejahatan terjadi bukan *preventive regulation* yang mampu mengantisipasi risiko melalui teknologi pengawasan yang setara.

Dalam pandangan penulis, tantangan terbesar hukum Indonesia saat ini bukan hanya pada aspek normatif, tetapi pada ketertinggalan paradigma hukum dibandingkan dengan kecepatan inovasi teknologi. Oleh karena itu, hukum nasional harus bertransformasi menuju sistem hukum digital adaptif, yang tidak hanya mengatur perilaku manusia, tetapi juga mengatur interaksi manusia dengan algoritma.

Penulis berpendapat bahwa pembentukan Undang-Undang Kecerdasan Buatan (AI Law) menjadi kebutuhan mendesak untuk memberikan kepastian hukum mengenai batas etika, tanggung jawab, dan transparansi algoritmik (*algorithmic accountability*). Selain itu, perlu dikembangkan sistem *Regulatory Technology* (RegTech) dan *Supervisory Technology* (SupTech) sebagai instrumen pengawasan hukum berbasis data real-time agar hukum tidak hanya menjadi perangkat kontrol sosial, tetapi juga instrumen pengendalian teknologi.

Dengan demikian, fenomena *AI-driven financial scam* harus dipahami bukan semata-mata sebagai bentuk kejahatan digital, melainkan sebagai cermin keterlambatan hukum dalam beradaptasi terhadap era kecerdasan buatan. Hukum yang progresif seharusnya tidak berhenti pada teks, melainkan harus mampu hidup, beradaptasi, dan menjangkau dimensi sosial baru yang diciptakan oleh teknologi.

## KESIMPULAN DAN SARAN

### Kesimpulan

Berdasarkan penjelasan diatas maka penulis menyimpulkan sebagai berikut:

Kejahatan *scam* pinjaman online berbasis kecerdasan buatan merupakan bentuk evolusi baru dari *cybercrime* yang menantang sistem hukum positif Indonesia, karena melibatkan penggunaan algoritma otonom, manipulasi data pribadi, serta penyamaran identitas digital yang sulit dijangkau hukum konvensional. Meskipun Indonesia telah memiliki landasan hukum melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Undang-Undang Nomor 4 Tahun 2023 tentang Penguatan dan Pengembangan Sektor Keuangan, namun regulasi tersebut belum sepenuhnya mampu mengatur tanggung jawab hukum terhadap sistem AI dan belum menyediakan instrumen pengawasan yang adaptif terhadap kejahatan digital modern. Oleh karena itu, diperlukan pembaruan paradigma hukum yang lebih progresif melalui pembentukan Undang-Undang Kecerdasan Buatan, penguatan mekanisme pengawasan digital berbasis RegTech dan SupTech, serta peningkatan literasi hukum dan kapasitas penegakan hukum agar sistem hukum nasional dapat melindungi masyarakat secara efektif di era transformasi digital yang semakin kompleks.

### Saran

Sebagai tindak lanjut dari hasil penelitian ini, penulis menyarankan agar pemerintah bersama lembaga terkait seperti Otoritas Jasa Keuangan (OJK), Kementerian Komunikasi dan Informatika (Kominfo), serta aparat penegak hukum segera memperkuat regulasi dan mekanisme pengawasan terhadap penggunaan kecerdasan buatan dalam sektor keuangan digital melalui

penerapan teknologi pengawasan berbasis *Regulatory Technology (RegTech)* dan *Supervisory Technology (SupTech)*. Selain itu, perlu dipertimbangkan pembentukan Undang-Undang Kecerdasan Buatan (*AI Law*) yang mengatur tanggung jawab hukum, etika algoritma, serta perlindungan data pribadi secara komprehensif. Upaya preventif melalui peningkatan literasi digital masyarakat dan pelatihan forensik siber bagi aparat penegak hukum juga menjadi langkah strategis agar hukum tidak hanya berfungsi sebagai alat penindakan, tetapi juga sebagai sarana pencegahan, perlindungan, dan pemberdayaan masyarakat dalam menghadapi kejahatan finansial berbasis AI di masa depan.

## DAFTAR PUSTAKA

### Buku

- Hamzah, Andi. (2008). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
- Rahardjo, Satjipto. (2011). *Hukum Progresif: Urgensi dan Kritik*. Jakarta: Epistema & HuMa.
- Soekanto, Soerjono. (1986). *Pengantar Penelitian Hukum*. Jakarta: UI Press.
- Zainuddin, Ali. (2014). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

### Peraturan Perundang-undangan

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.
- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.
- Peraturan Otoritas Jasa Keuangan Nomor 10 Tahun 2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi.
- Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Privat.

### Artikel / Jurnal

- Otoritas Jasa Keuangan Republik Indonesia. (2024). *Laporan Tahunan OJK: Pengawasan Fintech Lending dan Tantangan AI dalam Sektor Keuangan Digital*. Jakarta: OJK Press.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Laporan Nasional Penanganan Pinjaman Online Ilegal dan Kejahatan Siber*. Jakarta: Kominform.
- Pratama, A. (2023). "Penegakan Hukum terhadap Kejahatan Siber di Sektor Keuangan Digital." *Jurnal Ilmu Hukum Lex Renaissance*, Vol. 8 No. 2.
- Sari, L. D. (2023). "Analisis Yuridis terhadap Penyalahgunaan Data Pribadi dalam Layanan Pinjaman Online." *Jurnal Hukum dan Transformasi Digital*, Vol. 4 No. 1.
- Susanto, R. & Widjaja, F. (2022). "Artificial Intelligence and Algorithmic Liability: Legal Challenges in Financial Technology Regulation." *Indonesian Journal of Law and Technology*, Vol. 7 No. 3.