ASPEK HUKUM TINDAK PIDANA SIBER PADA PERUSAHAAN PEMBIAYAAN DALAM PENGGUNAAN LEGAL COMPLIANCE DAN SMART CONTRACT

Errisa Oktavianti[1], Tatok Sudjiarto[2], Richard Marolop Nainggolan[3]
2302190060@ms.uki.ac.id[1], tatok.sudjiarto@uki.ac.id[2], richard.nainggolan@uki.ac.id[3]
Universitas Kristen Indonesia

Abstrak: Perkembangan teknologi finansial mendorong perusahaan pembiayaan untuk memanfaatkan smart contract dan kredit skoring digital guna meningkatkan efisiensi dan kecepatan layanan. Meskipun demikian, penggunaan teknologi tersebut juga menimbulkan risiko hukum, khususnya terkait perlindungan data pribadi dan pertanggungjawaban pidana korporasi. Penelitian ini bertujuan untuk menganalisis peranan prinsip legal compliance dalam pencegahan, mitigasi, dan respons terhadap potensi pelanggaran hukum pada perusahaan pembiayaan berbasis smart contract. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, pendekatan kasus, dan pendekatan komparatif. Hasil penelitian menunjukkan bahwa penerapan prinsip legal compliance secara konsisten berperan penting dalam meminimalisir risiko pidana, memperjelas pertanggungjawaban hukum korporasi, serta meningkatkan perlindungan hukum bagi konsumen. Penelitian ini menegaskan bahwa legal compliance bukan sekadar kewajiban administratif, melainkan instrumen strategis dalam penegakan hukum di sektor pembiayaan digital.
Kata Kunci: Legal Compliance, Smart Contract, Pembiayaan Digital, Hukum Pidana, Perlindungan Data.

PENDAHULUAN

Revolusi digital telah mengubah wajah industri keuangan secara mendasar. Di Indonesia, perusahaan pembiayaan kini mengandalkan teknologi seperti scoring kredit digital dan verifikasi nasabah secara elektronik (E-KYC) untuk mempercepat proses dan memperluas jangkauan layanan. Sayangnya, transformasi ini bukannya tanpa masalah. Di balik efisiensi yang ditawarkan, ternyata tersembunyi kerentanan yang dimanfaatkan pihak-pihak tidak bertanggung jawab untuk melakukan kejahatan.

Berdasarkan catatan Otoritas Jasa Keuangan (OJK), selama periode 2022 hingga 2024 terjadi peningkatan yang mengkhawatirkan pada kasus kebocoran data dan penipuan digital di sektor pembiayaan. Modus kejahatan semakin beragam, mulai dari pemalsuan identitas, pembuatan profil nasabah fiktif, hingga rekayasa data untuk memanipulasi nilai kredit. Ironisnya, tidak sedikit pelaku yang justru berasal dari dalam perusahaan itu sendiri, memanfaatkan akses istimewa mereka untuk menggerogoti sistem.

Di tengah situasi ini, muncul wacana untuk menggunakan smart contract atau kontrak pintar berbasis blockchain sebagai solusi. Kontrak digital yang berjalan otomatis ini dianggap mampu mengurangi intervensi manusia yang rentan penyimpangan. Namun, jalan menuju penerapannya tidak mulus. Hukum Indonesia belum sepenuhnya mengakui keabsahan smart contract, sehingga status hukumnya masih abu-abu. Selain itu, sebagaimana perangkat lunak pada umumnya, smart contract juga tidak luput dari kemungkinan terdapat celah keamanan yang dapat dieksploitasi.

Permasalahan yang kompleks ini menuntut pendekatan hukum yang komprehensif. Di satu sisi, teknologi harus terus didorong untuk meningkatkan inklusi keuangan. Di sisi lain, perlindungan terhadap nasabah dan keamanan sistem tidak boleh diabaikan. Berangkat dari ketegangan ini, penelitian ini berupaya menjawab dua pertanyaan mendasar yaitu untuk melihat seperti apa sebenarnya wajah kejahatan siber di industri pembiayaan saat ini, khususnya yang terkait dengan penyalahgunaan sistem verifikasi dan penilaian kredit. Lalu sejauh mana prinsip kepatuhan hukum dan penerapan smart contract dapat berperan sebagai tameng untuk mencegah dan menangani kejahatan tersebut?

METODE PENELITIAN

Untuk mengurai permasalahan yang diajukan, penelitian ini ditempuh dengan menggunakan metode penelitian hukum normatif. Pilihan ini diambil karena jantung dari kajian ini terletak pada usaha untuk memahami dan mengkritisi aturan hukum yang sudah ada, prinsip-prinsip dasar hukum, serta bagaimana penerapannya dalam kenyataan, khususnya yang tercermin dari putusan-putusan pengadilan. Secara praktis, penulis menggabungkan tiga lensa pendekatan. Pendekatan kasus digunakan untuk membedah beberapa putusan pengadilan nyata yang menangani kasus penipuan digital dan rekayasa data di dunia pembiayaan, guna melihat pola dan dasar pertimbangan hukum yang diterapkan hakim. Secara bersamaan, pendekatan perundang-undangan dilakukan dengan menelusuri jejak dan menilai keselarasan berbagai regulasi, mulai dari KUHP, UU ITE, UU Perlindungan Data Pribadi, hingga aturan teknis dari OJK. Tidak berhenti di dalam negeri, pendekatan komparatif juga dilakukan dengan melihat sepintas bagaimana negara seperti Singapura dan Amerika Serikat menyikapi dan mengatur pemanfaatan smart contract dalam sektor keuangan mereka, sebagai bahan refleksi dan perbandingan.

Seluruh bahan yang menjadi pijakan analisis dalam penelitian ini bersumber dari data sekunder, yang dihimpun melalui penelaahan mendalam terhadap berbagai kepustakaan. Bahan-bahan tersebut mencakup peraturan perundang-undangan sebagai bahan hukum primer; buku, jurnal ilmiah, dan hasil penelitian sebelumnya yang membahas topik seputar kejahatan siber, fintech, dan blockchain sebagai bahan hukum sekunder; serta kamus dan ensiklopedia hukum sebagai bahan hukum tersier untuk memastikan keakuratan pemahaman atas istilah-istilah teknis. Setelah semua data terkumpul,

analisis dilakukan secara kualitatif. Tahap ini tidak sekadar mendeskripsikan pasal-pasal yang ada, tetapi lebih pada upaya untuk menafsirkan makna di baliknya dan menilai sejauh mana aturan-aturan itu sanggup menjawab tantangan kejahatan siber yang nyata terjadi di lapangan.

HASIL DAN PEMBAHASAN

Kejahatan di Dunia Pembiayaan Digital

Digitalisasi sektor pembiayaan ternyata tidak hanya membawa angin efisiensi, tetapi juga menghadirkan ancaman kejahatan siber yang semakin canggih dan sulit dilacak (Ozili, 2022). Riset ini menemukan bahwa proses masuknya nasabah baru (onboarding) menjadi gerbang utama yang paling sering diserang oleh para pelaku kejahatan. Mereka memanfaatkan kelemahan dalam sistem verifikasi elektronik (E-KYC) dengan dua modus operandi yang dominan. Modus pertama adalah pencurian identitas murni, di mana data diri orang lain yang didapat dari kebocoran data massal digunakan untuk membuat akun fiktif.

Modus kedua, yang lebih kompleks, adalah penipuan identitas sintetis (synthetic identity fraud). Dalam skema ini, pelaku merakit sebuah identitas baru yang tampak sah dengan cara menggabungkan potongan data pribadi yang valid dari beberapa korban berbeda, seperti mengambil nama dari satu orang dan nomor KTP dari orang lain (Berg et al., 2020). Karena setiap elemen data tersebut berasal dari sumber yang nyata, sistem otomatis seringkali terkecoh dan menganggapnya sebagai calon nasabah yang legitimate. Kerumitan teknik ini menunjukkan bahwa pelaku bukanlah amatir, melainkan jaringan terorganisir dengan pemahaman teknologi yang mendalam.

Sementara ancaman mengintai di pintu depan, titik rawan kedua justru berada di jantung proses bisnis, yaitu pada tahap penilaian kelayakan kredit (credit scoring). Di sini, pelaku beralih dari memalsukan identitas menjadi memanipulasi perilaku. Mereka melakukan rekayasa terhadap data yang menjadi pakan algoritma penilaian kredit, sebuah praktik yang dikenal sebagai data poisoning(Berg et al., 2020). Dengan sengaja menciptakan riwayat transaksi digital, aktivitas belanja online, atau bahkan interaksi media sosial yang palsu, pelaku berusaha membangun citra digital sebagai individu yang kreditworthy. Upaya sistematis untuk menipu algoritma ini berhasil dibongkar dalam Putusan Pengadilan Negeri Jakarta Selatan No. 786/Pid.B/2022/PN Jkt.Sel, yang mengungkap kasus manipulasi data otentik untuk pengajuan pinjaman (Hartono dkk., 2024).

Yang paling mengkhawatirkan, temuan penelitian mengindikasikan bahwa ancaman tidak hanya datang dari luar, tetapi juga dari dalam organisasi. Fenomena insider threat atau ancaman dari karyawan sendiri menjadi faktor pemercepat dan pendalam kerugian. Oknum internal dengan akses istimewa menyalahgunakan wewenangnya untuk mengubah data, menyetujui pengajuan fiktif, atau membocorkan database nasabah kepada pihak ketiga (AlBenJasim et al., 2023). Kolusi antara insider dengan jaringan eksternal ini memperlihatkan betapa rapuhnya pertahanan suatu sistem ketika pengawasan internal dan budaya integritas lemah, sebagaimana dijelaskan dalam Putusan Pengadilan Negeri Jakarta Pusat No. 442/Pid.Sus/2024/PN Jkt.Pst.

Legal Compliance sebagai Strategi Pertahan

Dalam gelombang ancaman siber yang semakin kompleks, prinsip legal compliance atau kepatuhan hukum justru muncul sebagai senjata pencegahan yang paling strategis. Pada hakikatnya, kepatuhan ini tidak boleh lagi dipandang sebagai sekumpulan beban administratif belaka, melainkan sebagai kerangka kerja proaktif untuk membangun ketahanan digital sebuah perusahaan (Short, 2021). Dengan mengintegrasikan prinsip ini ke dalam DNA operasional, perusahaan secara tidak langsung merancang sistem pertahanan berlapis. Pendekatan reaktif yang hanya menunggu insiden harus ditinggalkan, digantikan oleh budaya pencegahan yang berlandaskan aturan.

Paradigma ini terwujud nyata dalam ketaatan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP). Regulasi ini secara tegas memaksa perusahaan untuk memperlakukan data nasabah dengan penuh kehati-hatian dan akuntabilitas (UU No. 27 Tahun 2022). Konsekuensinya,

perusahaan dituntut untuk memiliki sistem pengamanan data yang memadai, transparan dalam menyatakan tujuan pengumpulannya, dan siap mempertanggungjawabkan setiap langkah pemrosesan. Implementasi yang tulus dari UU PDP pada akhirnya akan membentuk infrastruktur perlindungan data yang kokoh, yang menjadi garis pertahanan pertama terhadap upaya pencurian atau kebocoran informasi.

Lapisan pertahanan berikutnya dibangun melalui kepatuhan terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta serangkaian peraturan Otoritas Jasa Keuangan (OJK). Regulasi-regulasi ini menetapkan standar baku untuk keamanan sistem elektronik dan tata kelola teknologi informasi yang sehat (UU No. 1 Tahun 2024). Dengan memenuhi standar-standar teknis ini, perusahaan pada dasarnya sedang melakukan hardening atau pengerasan sistem teknologi mereka terhadap serangan eksternal. Proses audit dan sertifikasi yang sering menjadi bagian dari compliance berfungsi sebagai pemeriksaan kesehatan sistem yang berkelanjutan.

Pada akhirnya, perusahaan yang konsisten menjalankan legal compliance akan menikmati manfaat yang melampaui sekadar lolos dari pengawasan regulator. Mereka akan memiliki sistem pengendalian internal yang lebih rapi, mekanisme pengawasan yang lebih ketat, dan yang terpenting, budaya kehati-hatian kolektif yang mengakar di setiap tingkat organisasi (Syahir, Hasan, & Umar, 2023). Lingkungan kerja yang dibangun atas dasar integritas dan prosedur ini secara alamiah menciptakan ekosistem yang kurang bersahabat bagi praktik penyalahgunaan, baik yang berasal dari dalam maupun dari luar perusahaan. Dengan demikian, investasi dalam kepatuhan hukum berubah dari biaya menjadi aset pertahanan siber yang paling bernilai.

Tantangan dalam Mengimplementasikan Smart Contract

Di tengah upaya mencari solusi untuk meningkatkan transparansi dan efisiensi, smart contractmuncul sebagai teknologi yang menjanjikan. Kontrak digital berbasis blockchain ini menawarkan eksekusi otomatis yang dapat meminimalisir intervensi manusia yang rentan terhadap bias atau kecurangan (Mohanta, Panda, & Jena, 2018). Dalam praktik pembiayaan, kontrak pintar dapat diprogram untuk secara otomatis mencairkan dana ketika seluruh syarat kredit terpenuhi, atau sebaliknya, membekukan agunan digital jika nasabah melakukan wanprestasi. Mekanisme yang berjalan sendiri dan meninggalkan jejak audit yang permanen di blockchain ini berpotensi besar untuk mengurangi ruang bagi manipulasi administratif.

Namun, di balik potensi efisiensi tersebut, terdapat jurang ketidakpastian hukum yang masih membayangi. Meskipun Undang-Undang ITE telah mengakui keabsahan informasi dan dokumen elektronik, kerangka hukum nasional belum secara eksplisit mengatur posisi dan kekuatan mengikat dari smart contract (Kadly, Rosadi, & Gultom, 2021). Ketidakjelasan ini menjadi sumber risiko utama, karena apabila terjadi kesalahan kode (bug) yang merugikan salah satu pihak atau timbul sengketa interpretasi, landasan hukum untuk penyelesaiannya masih sangat lemah. Situasi ini menciptakan celah berbahaya yang dapat dimanfaatkan oleh pihak yang beritikad buruk atau justru menjerat pengguna yang beritikad baik.

Kerentanan tidak hanya berasal dari aspek hukum, tetapi juga dari sisi teknis smart contract itu sendiri. Sebagai sebuah program komputer, kontrak pintar tetaplah rentan terhadap kesalahan logika pemrograman (logical flaw) dan celah keamanan (vulnerability) yang dapat dieksploitasi (Sayeed, Marco-Gisbert, & Caira, 2020). Sejarah kelam dunia cryptocurrency, seperti peretasan terhadap The DAO yang menyebabkan kerugian puluhan juta dolar, menjadi bukti nyata bahwa satu baris kode yang salah dapat berdampak fatal. Karakter immutable atau tidak dapat diubahnya blockchain justru memperparah konsekuensinya, karena kesalahan yang terlanjur terdeploy sangat sulit untuk dikoreksi.

Oleh karena itu, penerapan smart contract di industri pembiayaan memerlukan pendekatan yang sangat hati-hati dan tidak terburu-buru. Langkah pertama dan terpenting adalah melakukan audit keamanan kode (smart contract audit) yang komprehensif dan berulang oleh pihak ketiga yang

independen sebelum kontrak dijalankan. Selain itu, perusahaan harus mengembangkan mekanisme contingency plan atau rencana darurat untuk mengantisipasi kegagalan eksekusi. Sinergi antara pengembang teknologi, ahli hukum, dan praktisi keuangan mutlak diperlukan untuk merancang smart contract yang tidak hanya cerdas secara teknis, tetapi juga kokoh secara hukum dan berkeadilan bagi semua pihak yang terikat.

Membangun Sinergi Strategis dalam Penegakan Hukum Siber

Upaya menangkal kejahatan siber di sektor pembiayaan tidak akan efektif jika hanya mengandalkan pendekatan yang terpisah-pisah dan reaktif. Ancaman yang bersifat sistemik dan teknis ini menuntut respons yang terpadu, melibatkan kolaborasi aktif antara regulator, penegak hukum, dan pelaku industri (Zamayya dkk., 2025). Setiap pihak harus bergerak keluar dari sekat-sekat tradisional dan membangun pemahaman bersama tentang peta ancaman digital. Hanya dengan strategi kolektif yang sinergis, ekosistem pembiayaan digital dapat dilindungi secara menyeluruh dari risiko yang terus berevolusi.

Peran regulator, dalam hal ini Otoritas Jasa Keuangan (OJK), perlu bergeser dari sekadar pembuat aturan menjadi fasilitator dan pemandu teknis. Regulasi yang dikeluarkan harus melampaui larangan-larangan umum dan mulai memberikan panduan operasional yang jelas, seperti standar keamanan minimum untuk sistem verifikasi digital (E-KYC) dan algoritma scoring kredit (OJK, 2024). Yang tak kalah penting, OJK perlu merumuskan pedoman tata kelola internal (internal governance) untuk membantu perusahaan mencegah ancaman dari dalam (insider threat). Kepastian hukum bagi inovasi seperti smart contract juga harus segera diwujudkan melalui regulasi yang adaptif dan tidak menghambat kemajuan teknologi.

Di lain pihak, aparat penegak hukum dituntut untuk melakukan lompatan kapasitas yang signifikan. Penyidik, jaksa, dan hakim harus mendapatkan pelatihan berkelanjutan untuk membekali mereka dengan literasi dasar teknologi finansial dan keahlian forensik digital (Suwiknyo, 2021). Tanpa pemahaman ini, proses pembuktian dalam kasus-kasus siber yang rumit akan terhambat. Membangun unit khusus yang beranggotakan personel dengan latar belakang hukum dan teknologi, serta menjalin kemitraan strategis dengan ahli dari perguruan tinggi dan industri, menjadi sebuah keharusan untuk mengungkap modus kejahatan yang semakin canggih.

Sementara itu, tanggung jawab terbesar justru berada di pundak perusahaan pembiayaan sendiri. Perusahaan harus bersikap proaktif dengan memandang keamanan siber dan kepatuhan hukum sebagai investasi strategis, bukan beban biaya. Investasi dalam teknologi pertahanan mutakhir harus diimbangi dengan investasi yang sama besarnya dalam membangun sumber daya manusia dan budaya perusahaan yang berintegritas (Syahir, Hasan, & Umar, 2023). Penerapan teknologi baru, termasuk smart contract, wajib diawali dengan kajian dampak mendalam, uji keamanan berlapis, dan skema percobaan (pilot project) sebelum diimplementasikan secara penuh. Pada akhirnya, ketahanan siber sebuah perusahaan lebih banyak ditentukan oleh manusianya daripada sekadar oleh kecanggihan perangkat lunaknya.

KESIMPULAN

Berdasarkan uraian di atas, dapat disimpulkan bahwa kejahatan siber pada perusahaan pembiayaan telah berevolusi menjadi ancaman yang sistematis dan teknis. Modusnya memanfaatkan celah pada sistem verifikasi digital dan algoritma kredit, dengan pelaku yang semakin berani melibatkan oknum internal. Dalam menghadapi hal ini, prinsip kepatuhan hukum (legal compliance) terbukti berperan penting sebagai fondasi pencegahan. Dengan mematuhi seperangkat regulasi yang ada, perusahaan secara tidak langsung telah memperkuat sistem keamanan dan pengawasan internalnya. Smart contract menawarkan mekanisme otomatisasi yang menjanjikan transparansi, namun potensinya masih terbentur pada masalah keabsahan hukum dan kerentanan teknis yang memerlukan pendekatan hati-hati.

Agar ekosistem pembiayaan digital Indonesia dapat tumbuh dengan sehat dan aman, penulis memberikan beberapa rekomendasi:

1. Percepatan Harmonisasi Regulasi. Pemerintah dan DPR perlu segera menyelesaikan RUU tentang Penggunaan Teknologi Dalam Transaksi Keuangan yang dapat mengakomodir keabsahan smart contract dan standar keamanan siber spesifik untuk sektor pembiayaan.
2. Penguatan Kapasitas Pengawasan OJK. Otoritas Jasa Keuangan perlu membentuk unit pengawasan siber yang khusus menangani sektor pembiayaan dan fintech. Unit ini harus dilengkapi dengan tenaga ahli teknologi yang mumpuni untuk melakukan pemeriksaan yang mendalam, tidak hanya administratif.
3. Peningkatan Literasi dan Kolaborasi. Aparat penegak hukum harus mendapatkan pelatihan berkelanjutan tentang digital forensik dan modus kejahatan siber terbaru. Kolaborasi tiga arah antara regulator, penegak hukum, dan asosiasi industri pembiayaan perlu diformalkan untuk berbagi informasi ancaman (threat intelligence).
4. Penerapan Tata Kelola Teknologi yang Responsible oleh Perusahaan. Perusahaan pembiayaan harus menjadikan keamanan siber dan perlindungan data sebagai bagian dari strategi bisnis inti, bukan sekadar kewajiban. Penerapan teknologi baru wajib didahului oleh uji keamanan (penetration test) dan audit kode oleh pihak ketiga yang independen.

Dengan langkah-langkah konkret ini, diharapkan industri pembiayaan digital Indonesia tidak hanya tumbuh pesat, tetapi juga tumbuh dengan kuat, aman, dan mampu menjaga kepercayaan masyarakat.

DAFTAR PUSTAKA

AlBenJasim, S., dkk. (2023). FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study. Journal of Computer Information Systems, 64, 838-850.

Berg, T., Burg, V., Gombović, A., & Puri, M. (2020). On the rise of fintechs: Credit scoring using digital footprints. The Review of Financial Studies, 33(7), 2845-2897.

Efendi, J., & Rijadi, P. (2022). Metode Penelitian Hukum Normatif dan Empiris: Edisi Kedua. Prenada Media.

Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. Computer Law & Security Review, 33(6), 825-835.

Hartono, B., dkk. (2024). Kepastian Hukum Bagi Korban Tindak Pidana Manipulasi Data Otentik Dalam Kasus Kejahatan Cyber Putusan Pengadilan Negeri Jakarta Selatan. Journal of Law and Nation, 3(3), 699-713.

Kadly, E. I., Rosadi, S. D., & Gultom, E. (2021). Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura. Jurnal Sains Sosio Humaniora, 5(1), 199-212.

Kamu, G. J. (2025). Kajian Yuridis Membantu Melakukan Tindak Pidana Manipulasi Informasi Atau Dokumen Elektronik (Putusan PN Jakarta Pusat No. 442/Pid.Sus/2024/PN Jkt.Pst). Lex Privatum, 15(4), 210-225.

Otoritas Jasa Keuangan (OJK). (2024). Laporan Tahunan Otoritas Jasa Keuangan 2023. Jakarta: OJK.

Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart Contract: Attacks and Protections. IEEE Access, 8, 24416-24427.

Suwiknyo, F. B. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. Lex Privatum, 9(4), 1-15.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.