



POTENSI FINTECH UNTUK FINANCIAL CRIME

Deden Setiadin Putra¹, Abdul Malik², Zuhrah³

Program Studi Magister Hukum

Universitas Muhammadiyah Bima

Email: Dedensetyadin@gmail.com¹, abdulmalik040279@gmail.com², zhoemachy@gmail.com³

Abstract

The development of financial technology (fintech) has brought significant transformations to the modern financial system through efficiency, transaction speed, and wider accessibility. However, this progress has also opened up new opportunities for increasingly complex financial crimes, such as money laundering, terrorism financing, digital fraud, and misuse of personal data. This study aims to analyze the relationship between fintech innovation and its potential misuse for financial crimes, by examining the regulatory framework, legal loopholes, and oversight challenges in Indonesia. The research method used is a normative approach with an analysis of laws and regulations, academic literature, and international practices. The results show that fintech characteristics – speed, anonymity, and a borderless system – are the main factors in increasing the risk of financial crime. This study emphasizes the importance of strengthening risk-based regulations, increasing collaboration between regulators and industry players, and developing a technology-based suspicious transaction detection system.

Keywords: Fintech Potential, Financial, Crime, Digital Regulation.

Abstrak

Perkembangan teknologi finansial (fintech) menghadirkan transformasi signifikan dalam sistem keuangan modern melalui efisiensi, kecepatan transaksi, dan aksesibilitas yang lebih luas. Namun, kemajuan ini juga membuka ruang baru bagi financial crime yang semakin kompleks, seperti pencucian uang, pendanaan terorisme, penipuan digital, dan penyalahgunaan data pribadi. Penelitian ini bertujuan menganalisis hubungan antara inovasi fintech dan potensi penyalahgunaannya untuk kejahatan keuangan, dengan menelaah kerangka regulasi, celah hukum, serta tantangan pengawasan di Indonesia. Metode penelitian yang digunakan adalah pendekatan normatif dengan analisis peraturan perundang-undangan, literatur akademik, serta praktik internasional. Hasil kajian menunjukkan bahwa karakteristik fintech kecepatan, anonimitas, dan borderless system menjadi faktor utama meningkatnya risiko financial crime. Penelitian ini menegaskan pentingnya penguatan regulasi berbasis risiko, peningkatan kolaborasi antara regulator dan pelaku industri, serta pembangunan sistem deteksi transaksi mencurigakan berbasis teknologi.

Kata Kunci: Potensi Fintech, Financial, Crime, Regulasi Digital.

A. PENDAHULUAN

Perkembangan teknologi informasi dalam satu dekade terakhir telah mendorong transformasi signifikan dalam sektor keuangan global. Fenomena digitalisasi ini melahirkan berbagai inovasi layanan keuangan berbasis teknologi, atau yang dikenal

sebagai financial technology (fintech). Kepraktisan, kecepatan, dan efisiensi yang ditawarkan fintech menjadikannya solusi unggulan bagi masyarakat dan pelaku usaha, terutama dalam hal transaksi digital, sistem pembayaran, pembiayaan daring, hingga pengelolaan investasi (Rahmah et al., 2024). Di berbagai negara, termasuk Indonesia, fintech mengalami pertumbuhan eksponensial seiring meningkatnya penetrasi internet dan penggunaan perangkat seluler. Kondisi tersebut menunjukkan potensi besarnya dalam memperluas inklusi keuangan dan mendorong pertumbuhan ekonomi (Purba et al., 2025).

Namun, di balik pesatnya perkembangan tersebut, muncul pula konsekuensi baru yang menuntut perhatian serius, yaitu meningkatnya eksposur terhadap praktik kejahatan keuangan (financial crime). Kejahatan ini tidak hanya mencakup penipuan digital, tetapi juga pencucian uang, pendanaan terorisme, penyalahgunaan data pribadi, hingga manipulasi transaksi. Sifat fintech yang serba cepat, erat dengan otomatisasi, serta sering melibatkan pihak ketiga, membuka peluang terjadinya celah keamanan. Ketergantungan pada sistem daring mengakibatkan pelaku dapat mengeksploitasi kerentanan teknologi untuk menyamarkan identitas, melakukan pemalsuan dokumen, serta mengalihkan dana secara lintas batas dalam hitungan detik. Oleh karena itu, penguatan tata kelola dan manajemen risiko menjadi isu penting dalam ekosistem fintech modern (Munajat & Yusuf, 2024).

Kemunculan fintech sebagai inovasi berbasis teknologi telah menjadi katalis yang mendorong berbagai proses keuangan semakin efisien, cepat, dan mudah diakses. Berbagai layanan seperti pembayaran digital, pinjaman berbasis aplikasi, investasi daring, crowdfunding, dan asuransi digital berkembang pesat di berbagai belahan dunia, termasuk di Indonesia. Fenomena ini tidak hanya mempengaruhi perilaku konsumen, tetapi juga mendorong transformasi struktural pada industri keuangan, di mana layanan konvensional mulai tergeser oleh teknologi yang lebih adaptif terhadap kebutuhan masyarakat modern (Budi Raharjo, 2021). Kepraktisan inilah yang menjadikan fintech sebagai pilar penting dalam mendorong inklusi keuangan, terutama bagi masyarakat yang sebelumnya sulit dijangkau oleh layanan keuangan tradisional.

Namun, ekspansi fintech yang begitu cepat juga memunculkan tantangan baru yang tidak bisa diabaikan, khususnya dalam konteks keamanan dan stabilitas sistem keuangan. Kompleksitas teknologi, tingginya volume transaksi, serta kemudahan membuka dan mengakses layanan keuangan secara daring menciptakan peluang bagi pelaku kejahatan untuk mengeksploitasi celah keamanan. Banyak kasus menunjukkan bahwa modus financial crime semakin canggih, baik berupa penipuan digital, penyalahgunaan identitas, pencucian uang, transaksi fiktif, hingga pendanaan aktivitas ilegal melalui platform fintech. Pelaku kejahatan memanfaatkan karakteristik fintech yang serba otomatis, terdesentralisasi, dan kerap melibatkan banyak aktor, sehingga proses pelacakan, pengawasan, dan penegakan hukum menjadi lebih sulit. Kondisi ini menimbulkan urgensi untuk memperkuat sistem keamanan, tata kelola, dan deteksi dini pada seluruh ekosistem fintech (Despotović et al., 2023).

Dalam beberapa tahun terakhir, berbagai penelitian telah mencoba menyoroti keterkaitan antara perkembangan fintech dan risiko kejahatan keuangan. Sejumlah studi mengkaji kerentanan pada sektor pembayaran digital yang sering menjadi sasaran fraud dan phishing (Passas, 2025). Penelitian lain menemukan bahwa platform pinjaman digital berpotensi dimanfaatkan untuk layering dan placement dalam tindak pencucian uang. Ada pula penelitian yang menyoroti lemahnya verifikasi identitas pada beberapa platform fintech, sehingga membuka peluang penggunaan identitas palsu (de Koker & Goldbarsht, 2022). Sementara itu, sejumlah penelitian berfokus pada isu regulasi dan pengawasan, terutama mengenai efektivitas aturan Know Your Customer (KYC), Anti-Money Laundering (AML), serta mekanisme pengawasan dari regulator. Walaupun penelitian-penelitian tersebut memberikan pemahaman awal, masih banyak aspek yang membutuhkan pendalaman lebih lanjut (Adnan & Kumar, 2024).

Berbagai penelitian sebelumnya telah mencoba menelaah hubungan antara perkembangan fintech dan risiko kejahatan keuangan. Sejumlah studi menyoroti bagaimana layanan peer-to-peer lending rentan dimanfaatkan untuk aktivitas pencucian uang, sementara penelitian lain mengungkap peningkatan kasus penipuan digital yang memanfaatkan platform pembayaran elektronik. Selain itu, beberapa karya ilmiah berfokus pada aspek regulasi, terutama efektivitas kebijakan pemerintah dan

otoritas keuangan dalam mengawasi penyelenggara fintech. Temuan-temuan ini memberikan gambaran bahwa fintech, meskipun berpotensi besar bagi perekonomian, tetap menghadirkan risiko yang tidak dapat diabaikan (Wiwoho et al., 2022).

Dari telaah penelitian terdahulu, tampak adanya beberapa research gap yang perlu ditangani. Pertama, sebagian besar penelitian masih berfokus pada satu jenis layanan fintech dan belum melihat ekosistem secara keseluruhan, padahal setiap layanan saling terhubung dan dapat menciptakan risiko berlapis. Kedua, penelitian sebelumnya cenderung berhenti pada pemetaan risiko tanpa mengevaluasi potensi teknologi fintech untuk menjadi alat pencegahan kejahatan keuangan. Ketiga, masih terbatas analisis yang mengaitkan inovasi teknologi seperti artificial intelligence, biometric authentication, blockchain analytics, ataupun big data dengan upaya mitigasi financial crime di fintech. Keempat, terdapat sedikit penelitian yang membahas secara mendalam mengenai bagaimana sinergi antara pemerintah, regulator, dan industri fintech dapat menciptakan sistem pengawasan yang adaptif terhadap modus kejahatan yang terus berkembang. Kekosongan pemahaman pada aspek-aspek tersebut menunjukkan bahwa isu potensi fintech terhadap financial crime perlu dikaji lebih komprehensif dengan pendekatan multidisipliner.

Kendati demikian, penelitian terdahulu masih menyisakan sejumlah kelemahan yang menimbulkan adanya research gap. Sebagian besar kajian masih menitikberatkan pada analisis risiko secara parsial, misalnya hanya membahas satu jenis layanan fintech atau satu bentuk kejahatan keuangan tertentu. Selain itu, penelitian sebelumnya cenderung memfokuskan pada aspek regulatif tanpa mengintegrasikan perkembangan teknologi mutakhir seperti machine learning, big data analytics, dan artificial intelligence yang kini digunakan dalam deteksi financial crime. Masih terbatas pula kajian yang mengupas secara menyeluruh mengenai bagaimana potensi inovasi fintech dapat sekaligus menjadi alat pencegahan, bukan hanya objek yang membawa risiko.

Dengan adanya kesenjangan tersebut, penelitian ini menawarkan novelty berupa pendekatan analitis yang memandang fintech bukan hanya sebagai objek yang rentan terhadap kejahatan keuangan, tetapi juga sebagai instrumen potensial dalam pencegahan, deteksi, dan penanggulangan financial crime. Penelitian ini

mengintegrasikan pemahaman mengenai risiko inheren pada layanan fintech dengan pemanfaatan teknologi cerdas yang menjadi bagian dari inovasi fintech itu sendiri. Pendekatan seperti ini masih jarang ditemukan dalam penelitian terdahulu, padahal teknologi seperti machine learning, data mining, dan network analysis sebenarnya memiliki peluang besar untuk memperkuat keamanan sistem fintech. Selain itu, penelitian ini juga menekankan pentingnya tata kelola kolaboratif antara pelaku industri, regulator, dan otoritas penegak hukum dalam menciptakan mekanisme pengawasan yang lebih responsif.

Berdasarkan latar belakang tersebut, tujuan penelitian ini adalah untuk menganalisis secara mendalam potensi fintech dalam konteks kejahatan keuangan, baik dari sisi risiko maupun peluang mitigasinya. Penelitian ini berupaya mengevaluasi bagaimana teknologi fintech dapat menjadi sumber kerentanan sekaligus alat strategis dalam memperkuat pencegahan financial crime. Selain itu, penelitian ini bertujuan untuk merumuskan model konseptual atau rekomendasi kebijakan yang dapat mendukung terciptanya ekosistem fintech yang aman, terkontrol, dan berdaya saing. Melalui analisis yang komprehensif, penelitian ini diharapkan dapat memberikan kontribusi teoritis bagi pengembangan literatur fintech dan financial crime, serta kontribusi praktis bagi regulator, lembaga keuangan, dan perusahaan fintech dalam mengembangkan strategi mitigasi risiko yang lebih efektif dan berkelanjutan.

B. METODE PENELITIAN

Tulisan ini menggunakan metode penelitian hukum normatif karena fokus kajian berangkat dari kekaburan norma terkait regulasi teknologi finansial dalam membendung tindak pidana keuangan. Pendekatan yang digunakan dalam penelitian ini mencakup pendekatan perundang-undangan (*statute approach*) untuk menelaah regulasi eksis, pendekatan konseptual (*conceptual approach*) guna membangun kerangka pemikiran mengenai potensi penyalahgunaan teknologi, serta pendekatan analitis (*analytical approach*) untuk membedah sinkronisasi aturan dengan realita kejahatan finansial. Sumber bahan hukum yang digunakan meliputi bahan hukum primer berupa peraturan perundang-undangan dan bahan hukum sekunder seperti literatur serta

jurnal ilmiah. Teknik pengumpulan bahan hukum dan data dilakukan melalui studi dokumen (studi pustaka) yang sistematis terhadap berbagai literatur terkait. Terakhir, seluruh bahan hukum yang terkumpul diolah menggunakan metode analisis kualitatif untuk menghasilkan kesimpulan yang deskriptif preskriptif mengenai penguatan regulasi fintech di masa depan

C. HASIL DAN PEMBAHASAN

Sektor Teknologi Finansial (FinTech) telah merevolusi cara layanan keuangan diberikan, menawarkan efisiensi, aksesibilitas, dan inovasi yang belum pernah ada sebelumnya. Namun, laju inovasi yang cepat dan sifat digital dari FinTech juga secara inheren menciptakan tantangan baru dan peningkatan potensi untuk dieksploitasi oleh pelaku kejahatan finansial. Potensi risiko ini muncul dari tiga pilar utama: anonimitas dan kecepatan transaksi, kompleksitas regulasi, dan celah keamanan pada teknologi baru (Nandy & Al Mamun, 2024).

Salah satu daya tarik terbesar FinTech, yaitu kecepatan dan kemudahan transaksi, juga menjadi kerentanan utamanya dalam konteks kejahatan finansial. Platform pembayaran digital, remittance lintas batas yang instan, dan terutama aset kripto, memungkinkan transfer dana dalam volume besar secara cepat dan seringkali pseudo-anonim. Kecepatan ini mempersulit lembaga keuangan dan regulator untuk menerapkan kontrol Know Your Customer (KYC) dan Anti-Money Laundering (AML) secara efektif. Misalnya, aset kripto menawarkan tingkat anonimitas yang signifikan, menjadikannya alat yang ideal untuk pencucian uang (money laundering) dan pendanaan terorisme. Dana dapat dipecah menjadi transaksi kecil (smurfing) dan dipindahkan ke berbagai dompet digital di seluruh dunia dalam hitungan menit, jauh melampaui kemampuan sistem perbankan tradisional untuk melacak atau membekukan dana secara real-time. Kecepatan ini secara signifikan mempersingkat "jendela" waktu yang tersedia bagi lembaga untuk mendeteksi aktivitas mencurigakan dan mengambil tindakan korektif (Passas, 2025).

Sifat global dan inovatif dari FinTech sering kali mendahului kerangka regulasi yang ada, menciptakan wilayah abu-abu dan peluang untuk regulatory arbitrage.

Banyak entitas FinTech beroperasi di bawah lisensi yang berbeda dari bank tradisional, atau bahkan di yurisdiksi yang memiliki pengawasan AML/KYC yang lemah. Misalnya, layanan cross-border payment dan platform peer-to-peer lending mungkin memiliki rezim kepatuhan yang tidak sekuat lembaga perbankan yang diatur secara ketat. Selain itu, definisi financial crime yang jelas dan konsisten di seluruh yurisdiksi yang berbeda menjadi sulit diterapkan, terutama pada teknologi baru seperti Decentralized Finance (DeFi). Dalam ekosistem DeFi, tidak adanya otoritas pusat menghilangkan titik kontrol tradisional, membuat pelacakan pelaku dan penegakan hukum menjadi sangat menantang. Pelaku kejahatan dapat mengeksploitasi perbedaan-perbedaan ini dengan memindahkan aktivitas mereka ke yurisdiksi dengan regulasi paling ringan, yang dikenal sebagai "berburu yurisdiksi yang lunak (Torano & Rahman, 2025)."

Adopsi teknologi baru seperti Kecerdasan Buatan (AI), Machine Learning (ML), dan blockchain memang membawa manfaat, tetapi juga membuka vektor serangan baru. Ancaman siber seperti peretasan exchange kripto, penipuan phishing yang menargetkan dompet digital, dan pencurian data pribadi untuk penipuan identitas (identity fraud) menjadi risiko yang meningkat. Data sensitif pelanggan yang disimpan oleh perusahaan FinTech menjadi target bernilai tinggi bagi peretas, yang kemudian dapat menggunakan informasi tersebut untuk mengambil alih akun atau membuat identitas sintetis untuk kejahatan lebih lanjut. Risiko teknologi baru juga mencakup kerentanan pada kode pintar (*smart contract*) dalam ekosistem blockchain yang dapat dieksploitasi untuk mencuri dana dalam jumlah besar, seperti yang sering terjadi pada kasus rug pull atau eksploitasi pada protokol DeFi. Selain itu, penggunaan AI untuk meningkatkan efisiensi juga dapat dibalik oleh pelaku kejahatan yang menggunakan AI generatif untuk membuat *deepfake* atau pesan *phishing* yang sangat meyakinkan, meningkatkan kompleksitas penipuan rekayasa sosial (*social engineering fraud*) (Deryl Leeland and Richard C. Adam, 2025).

Jika tidak diatasi, potensi FinTech untuk memfasilitasi kejahatan finansial dapat merusak kepercayaan publik terhadap inovasi digital dan menyebabkan kerugian ekonomi yang signifikan, baik bagi konsumen maupun pasar keuangan global. Untuk

memitigasi risiko ini, diperlukan kolaborasi yang erat antara regulator, lembaga penegak hukum, dan perusahaan FinTech. Pendekatan yang efektif melibatkan peningkatan pengawasan regulasi yang adaptif, investasi dalam teknologi RegTech (*Regulatory Technology*) untuk otomatisasi kepatuhan AML/KYC, dan pengembangan alat analitik canggih yang mampu melacak transaksi di berbagai blockchain. Perusahaan FinTech harus memprioritaskan keamanan siber dan memastikan bahwa protokol KYC/AML mereka dapat diskalakan dan sebanding dengan risiko yang ditimbulkan oleh produk atau layanan yang mereka tawarkan.

Singkatnya, sementara FinTech adalah pendorong pertumbuhan ekonomi, inovasinya juga telah menciptakan jalur baru dan lebih efisien bagi kejahatan finansial. Mengatasi tantangan ini menuntut keseimbangan yang hati-hati antara mendukung inovasi dan memastikan integritas serta keamanan sistem keuangan global.

A. Kerentanan Teknologi Fintech terhadap Modus Kejahatan Finansial Baru

Pertumbuhan fintech yang sangat cepat menghadirkan inovasi dalam sistem pembayaran, pinjaman daring, dompet digital, investasi berbasis aplikasi, hingga kripto-aset. Namun, perkembangan ini juga memperluas permukaan serangan (*attack surface*) yang dapat dimanfaatkan pelaku kejahatan finansial. Arsitektur fintech yang mengutamakan kecepatan, otomatisasi, dan kemudahan onboarding sering membuka celah jika tidak dibarengi dengan penguatan pengawasan dan verifikasi identitas. Misalnya, proses KYC (*Know Your Customer*) yang sepenuhnya digital dapat dimanipulasi dengan identitas palsu, hasil rekayasa gambar, atau pencurian data pribadi. Ketika proses verifikasi dapat dilakukan tanpa tatap muka, risiko impersonasi, *synthetic identity fraud*, serta pembukaan akun untuk aktivitas ilegal meningkat drastis (Latifah et al., 2022).

Selain itu, integrasi API (*Application Programming Interface*) yang menjadi fondasi ekosistem fintech juga dapat menciptakan kerentanan baru. API memungkinkan data pengguna berpindah antar platform dengan cepat, tetapi jika tidak ada standar keamanan yang kuat, titik ini dapat dimanfaatkan untuk mengakses informasi sensitif atau menyusupkan transaksi abnormal ke dalam sistem. Beberapa kasus menunjukkan bahwa celah dalam API dapat memungkinkan serangan seperti *account takeover*,

pencurian dana, hingga penyusupan malware ke dalam perangkat pengguna. Dengan semakin banyaknya layanan fintech yang saling terhubung, satu titik kebocoran data dapat menimbulkan konsekuensi sistemik yang mengancam seluruh jaringan finansial digital.

Lebih jauh lagi, penggunaan teknologi blockchain dan aset kripto membawa dimensi baru dalam kejahatan finansial. Walaupun bersifat transparan, sifat pseudonim transaksi kripto membuat pelaku kejahatan dapat menyembunyikan identitas melalui teknik seperti mixing services, chain hopping, dan penggunaan DeFi (Decentralized Finance) tanpa KYC. Teknologi ini sering dimanfaatkan dalam aktivitas seperti pencucian uang lintas negara, pendanaan terlarang, dan penipuan investasi. Kombinasi antara teknologi yang kompleks dan rendahnya literasi pengguna membuat masyarakat semakin rentan terhadap skema penipuan berbasis kripto, seperti ponzi, rug pull, atau phishing yang menyamar sebagai aplikasi investasi resmi. Dalam konteks digital onboarding, proses verifikasi berbasis foto KTP, selfie, atau video singkat sering kali tidak mampu membedakan antara identitas asli dan identitas sintetis. Dengan dukungan teknologi rekayasa wajah (deepfake), pelaku dapat memalsukan identitas dengan kualitas yang sangat mirip sehingga lolos pemeriksaan otomatis. Kondisi ini memunculkan ancaman baru seperti synthetic identity fraud yang semakin sulit diberantas oleh teknologi konvensional (Khudsiyah, dkk 2025)

Tidak hanya pada sisi identitas, arsitektur terbuka fintech yang menggunakan API untuk menghubungkan platform keuangan, merchant, maupun aplikasi pihak ketiga juga memberikan celah keamanan. API yang tidak dienkripsi atau tidak memiliki kontrol otorisasi kuat dapat menyebabkan kebocoran data, account takeover, atau manipulasi transaksi. Para pelaku sering memanfaatkan celah API untuk menyisipkan perintah transaksi otomatis tanpa ketahuan, terutama dalam sistem yang memproses jutaan transaksi harian. Dalam lingkungan yang saling terhubung, satu kelemahan kecil pada API sebuah perusahaan rintisan dapat berdampak domino ke seluruh ekosistem pembayaran digital (Azizah et al., 2024).

Selain itu, teknologi blockchain dan aset kripto menghadirkan risiko baru. Meskipun blockchain bersifat transparan, identitas pengguna tetap tersamar karena

hanya direpresentasikan sebagai alamat wallet. Sifat pseudo-anonymous ini memungkinkan pelaku mencampur dana ilegal melalui mixing services atau berpindah blockchain (chain-hopping) untuk menghilangkan jejak transaksi. Platform DeFi yang tidak memiliki proses KYC juga menjadi sarana ideal untuk pencucian uang, pendanaan kriminal, serta transaksi lintas negara yang sulit dilacak. Kurangnya pemahaman masyarakat mengenai kripto memperbesar peluang terjadinya penipuan berbasis investasi digital, seperti ponzi, rug pull, dan broker palsu yang memanfaatkan ketidaktahuan korban (Menur Kusumaningtyas dan Dhyah Wulansari, 2025).

B. Potensi Fintech sebagai Sarana Pencucian Uang dan Pendanaan Terlarang

Fintech memiliki karakteristik yang secara inheren dapat dimanfaatkan untuk aktivitas pencucian uang (*money laundering*), terutama karena prosesnya yang cepat, volume transaksi tinggi, dan minimnya interaksi fisik. Dalam tahap placement, pelaku dapat memasukkan dana ilegal ke dalam sistem melalui pembukaan akun fintech dengan identitas palsu atau akun yang dibeli secara ilegal di pasar gelap. Setelah dana berada dalam sistem, tahap layering menjadi lebih mudah dilakukan karena fintech mendukung fragmentasi dana, transaksi mikro (*micro-transactions*), serta perpindahan dana secara instan ke berbagai platform, termasuk lintas negara. Upaya pelacakan menjadi jauh lebih rumit karena alur transaksi di fintech sering kali bersifat terdistribusi dan memanfaatkan jaringan pembayaran internasional yang kompleks (Usman et al., 2024).

Pada tahap integration, dana yang telah “diputihkan” melalui berbagai sistem fintech dapat muncul kembali sebagai hasil investasi yang sah, keuntungan perdagangan aset digital, atau pendapatan dari platform peer-to-peer lending. Banyak pelaku yang memanfaatkan fitur withdraw ke rekening bank atau dompet digital dengan nominal kecil berulang untuk menghindari deteksi otomatis oleh sistem anti-money laundering (AML). Selain itu, sejumlah platform fintech yang belum memiliki prosedur AML yang matang cenderung kesulitan mengidentifikasi pola transaksi abnormal, terutama jika pelaku menggunakan otomatisasi atau bot untuk mensimulasikan transaksi pengguna biasa (Annisa, 2007).

Fintech juga berpotensi menjadi sarana pendanaan terlarang karena metode pembayaran digital memiliki jangkauan global yang sulit dibatasi oleh regulasi lokal. Jaringan pendanaan ilegal dapat memanfaatkan dompet digital lintas batas, stablecoin, atau layanan remittance berbasis blockchain untuk memindahkan dana tanpa pengawasan otoritas keuangan. Dalam beberapa kasus internasional, organisasi kriminal memanfaatkan fintech yang berbasis di yurisdiksi dengan regulasi lemah agar dapat menjalankan kegiatan secara bebas. Tantangan makin besar ketika pelaku menggunakan teknologi pengaburan seperti VPN, obfuscation tools, dan wallet anonim untuk menutupi jejak digital. Hal ini menunjukkan bahwa fintech tidak hanya membuka peluang efisiensi, tetapi juga memperluas ruang gerak bagi aktivitas kriminal yang semakin terorganisir dan canggih (Wójcik-Czerniawska, 2024).

Pada tahap placement, pelaku dapat memasukkan dana hasil kejahatan melalui berbagai platform, seperti dompet digital, aplikasi investasi, hingga platform pinjaman P2P. Identitas palsu atau akun fiktif sering digunakan untuk menyamarkan sumber dana. Sementara itu, transaksi mikro dalam jumlah besar sangat efektif untuk menghindari deteksi sistem perbankan tradisional yang biasanya hanya fokus pada transaksi bernilai besar. Tahap layering menjadi lebih berbahaya karena ekosistem fintech mendukung perpindahan dana secara cepat antar platform, termasuk ke luar negeri. Pelaku dapat membagi dana menjadi ratusan transaksi kecil dan memindahkannya ke aplikasi lain, membeli aset digital, atau menukar dana menjadi stablecoin untuk kemudian dikirim ke wallet asing. Proses ini tidak hanya mempersulit pelacakan tetapi juga memperpanjang rantai transaksi sehingga semakin sulit diurai oleh otoritas (Nikkel, 2020).

Pada tahap integration, dana yang telah “dibersihkan” melalui berbagai proses dapat muncul kembali sebagai hasil investasi yang sah, keuntungan perdagangan kripto, atau pembayaran dari platform P2P lending. Pelaku sering melakukan withdraw dalam nominal kecil berulang kali agar tidak memicu alarm AML. Selain itu lemahnya sistem kontrol pada sebagian fintech ilegal atau tidak berizin membuka kesempatan bagi jaringan kejahatan untuk menjalankan kegiatan pendanaan terlarang. Stabilitas

sistem keuangan digital dapat terganggu jika aktivitas ini terjadi dalam skala besar tanpa pengawasan ketat (Anggun, 2022)

D. PENUTUP

FinTech (Teknologi Finansial) menghadirkan dua mata pisau yang signifikan dalam ekosistem keuangan, di satu sisi ia merevolusi layanan melalui efisiensi, aksesibilitas, dan inovasi seperti pembayaran digital, *peer-to-peer* lending, dan mata uang kripto; namun, di sisi lain, pertumbuhan pesat dan sifatnya yang sering kali tanpa batas geografis menciptakan celah dan tantangan baru yang berpotensi dimanfaatkan oleh pelaku kejahatan finansial. Potensi ini terutama berakar pada Anonimitas yang lebih besar yang ditawarkan oleh beberapa platform (terutama Decentralized Finance atau DeFi dan transaksi kripto), Kecepatan transaksi yang mempersulit pelacakan dan pembekuan dana, serta Kompleksitas teknologi yang melampaui kemampuan regulasi dan kepatuhan tradisional, membuka jalan bagi praktik pencucian uang, pendanaan terorisme, penipuan, dan scam investasi digital. Oleh karena itu, sementara FinTech menjanjikan inklusi keuangan yang lebih besar, diperlukan upaya regulasi yang adaptif dan kolaboratif yang berfokus pada penguatan identitas digital (KYC/AML), analisis transaksi berbasis Artificial Intelligence (AI) untuk mendeteksi pola yang mencurigakan, dan kemitraan publik-swasta untuk memastikan bahwa inovasi digital tidak dijadikan saluran utama baru bagi kejahatan finansial.

DAFTAR PUSTAKA

- Adnan, S. A., & Kumar, P. (2024). Financial Crimes and Fintech in India. In C. M. Gupta & G. Kaur (Eds.), *E-banking, Fintech, {&} Financial Crimes: The Current Economic and Regulatory Landscape* (pp. 97-109). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67853-0_8
- Anggun, L. (2022). Perkembangan Kejahatan Tindak Pidana Pencucian Uang Dan Perkembangan Kejahatan Tindak Pidana Pencucian Uang Dan Tindak Pidana Pendanaan Terorisme (TPPU Dan TPPT) Di Masa Pandemi Covid-19. *Technology and Economics Law Journal*, 1(1). <https://doi.org/10.21143/TELJ.vol1.no1.1004>
- Annisa, F. (2007). Penerapan Program Apu Ppt Untuk Mencegah Pencucian Uang Dan Pendanaan Terorisme Pada Industri Fintech. *Adil: Jurnal Hukum Vol.11*, 11(8), 63.
- Azizah, S., Ula, Z. N., Mutiara, D., Prameswari, M. P., Ekonomi, F., Islam, U.,

- Abdurrahman, N. K. H., & Pekalongan, W. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile : Studi literatur mengenai cybercrime dan mitigasinya kehidupan , aplikasi keuangan mobile telah menjadi salah satu inovasi terkemuka yang bisnis dalam mengakses dan mengelola keuangan s. *Akuntansi Dan Teknologi Informasi*, 17(April), 221–237.
- Budi Raharjo. (2021). *FINTECH: TEKNOLOGI FINANSIAL PERBANKAN DIGITAL*.
- de Koker, L., & Goldbarsht, D. (2022). Financial Technologies and Financial Crime: Key Developments and Areas for Future Research. In D. Goldbarsht & L. de Koker (Eds.), *Financial Technology and the Law : Combating Financial Crime* (pp. 303–320). Springer International Publishing. https://doi.org/10.1007/978-3-030-88036-1_13
- Deryl Leeland and Richard C. Adam. (2025). Table Of Content Indonesian Journal of Law and Economics Review. *Indonesian Journal of Law and Economics Review*, 20(4), 1–15.
- Despotović, A., Parmaković, A., & Miljković, M. (2023). *Cybercrime and Cyber Security in Fintech BT - Digital Transformation of the Financial Industry: Approaches and Applications* (S. Benković, A. Labus, & M. Milosavljević (eds.); pp. 255–272). Springer International Publishing. https://doi.org/10.1007/978-3-031-23269-5_15
- Khudsiyah, D. (2025). Penegakan Hukum Terhadap Modus Baru Kejahatan Cyber Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui Internet Banking. *Jurnal Ilmiah Wahana Pendidikan*, Agustus, 11(8), 232–244.
- Latifah, F. N., Mawardi, I., & Wardhana, B. (2022). Threat of Data Theft (Phishing) Amid the Trend of Fintech Users in the Covid- 19 Pandemic (Study of Phishing in Indonesia) Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemi Covid – 19 (Study Phishing Di Indonesia). *Perisai: Islamic Banking and Finance Journal*, 6(1), 74–86. <https://doi.org/10.21070/perisai.v6i1>.
- Menur Kusumaningtyas dan Dhyah Wulansari. (2025). Literasi Digital dan Fintech : Strategi Menghadapi Disinformasi di Indonesia. *Journal of Artificial Intelligence and Digital Business (RIGGS)*, 4(3), 4640–4645.
- Munajat, A. A., & Yusuf, H. (2024). *Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus : Studi Tentang Kejahatan Keuangan Berbasis Digital The Role of Information Technology in the Prevention and Disclosure of Special Economic Crimes : A Study of Digital-Based Financial Crimes*. November, 4853–4865.
- Nandy, D., & Al Mamun, A. (2024). Financial Crimes Through Fintech by Political Leaders: The Experience of Select South Asian States. In C. M. Gupta & G. Kaur (Eds.), *E-banking, Fintech, {&} Financial Crimes: The Current Economic and Regulatory Landscape* (pp. 79–95). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67853-0_7
- Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, 33, 200908. <https://doi.org/https://doi.org/10.1016/j.fsidi.2020.200908>

- Passas, N. (2025). Cryptocurrencies , Blockchain , and Financial Crimes. *International Journal of Criminology and Sociology*, 14, 76–89.
- Purba, D. S., Permatasari, P. D., Tanjung, N., Fitriani, R., Wulandari, S., Islam, U., Sumatera, N., Muslim, U., Al, N., & Ekonomi, P. (2025). *ANALISIS PERKEMBANGAN EKONOMI DIGITAL*. 10(204), 126–139.
- Rahmah, A. T., Fasa, M. I., Islam, U., Raden, N., Lampung, I., & Lampung, K. B. (2024). *Pengaruh Transformasi Digital Dan Pengembangan Financial Technology (Fintech) Terhadap Inovasi Pengaruh Transformasi Digital Dan Pengembangan Financial Technology (Fintech) Terhadap Inovasi*. 2(10).
- Torano, M. T., & Rahman, H. Y. (2025). Claims of Economic Rights of Wives in Divorce Cases According to the Compilation of Islamic Law in the Biak Religious Court Islamic Family Law. *International Journal of Management*, 7(1), 531–542. <https://doi.org/10.56338/ijhess.v7i1.5871>
- Usman, N., Griffiths, M., & Alam, A. (2024). FinTech and money laundering: moderating effect of financial regulations and financial literacy. *Digital Policy, Regulation and Governance*, 27(3), 301–326. <https://doi.org/10.1108/DPRG-04-2024-0068>
- Wiwoho, J., Kharisma, D. B., & Wardhono, D. T. K. (2022). Financial crime in digital payments. *Journal of Central Banking Law and Institutions*, 1(1), 47–70. <https://doi.org/10.21098/jcli.v1i1.7>
- Wójcik-Czerniawska, A. (2024). Voltaic Money Laundering, the Dark Side of Fintech. In M. H. Bilgin, H. Danis, E. Demir, & M. Zipperling (Eds.), *Eurasian Business and Economics Perspectives* (pp. 337–353). Springer Nature Switzerland.