JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v6i1.6272
https://creativecommons.org/licenses/by/4.0/
Received: 8 Agustus 2025 | **Revised:** 12 Oktober 2025 | **Accepted:** 23 Oktober 2025

Kejahatan Ekonomi Berbasis Digital: Strategi Harmonisasi Regulasi Internasional dalam Menanggulangi Tindak Pidana Keuangan Global

Gitra Moraza[1], Ani Purwati[2], Saiful Anam[3]
[1]Magister Ilmu Hukum, Universitas Pascasarjana Sahid, Jakarta, Indonesia, gitramorazaa@gmail.com
[2]Magister Ilmu Hukum, Universitas Pascasarjana Sahid, Jakarta, Indonesia, dr.anipurwati.pal.ind@gmail.com
[3]Magister Ilmu Hukum, Universitas Pascasarjana Sahid, Jakarta, Indonesia, saiful_anam@usahid.ac.id

Corresponding Author: gitramorazaa@gmail.com

Abstract: *The digital era has fundamentally changed the global economic landscape, including the dimensions of financial crime, which now utilizes digital technology as a primary tool. Digital-based economic crime is characterized by the anonymity of perpetrators, the speed of transactions, and the cross-jurisdictional nature that hampers the effectiveness of national law enforcement. This study uses a normative juridical method with legislative, comparative, and conceptual approaches to analyze strategies for international regulatory harmonization in addressing global financial crime. International legal instruments such as the United Nations Convention against Transnational Organized Crime (UNTOC), the United Nations Convention against Corruption (UNCAC), and the recommendations of the Financial Action Task Force (FATF) are evaluated for their effectiveness in addressing the challenges of digital financial crime. The results show that despite the existence of a global legal framework, regulatory disparities, technical capacity gaps, and weak political commitment remain major obstacles. This study recommends an international regulatory model that integrates legal harmonization, real-time technical cooperation mechanisms, and continuous regulatory adaptation to strengthen the integrity of the global financial system.*

Keywords: *Digital Economic Crime, Regulatory Harmonization, International Law, FATF, UNTOC, UNCAC.*

Abstrak: Era digital telah mengubah secara fundamental lanskap ekonomi global, termasuk dimensi kejahatan keuangan yang kini memanfaatkan teknologi digital sebagai sarana utama. Kejahatan ekonomi berbasis digital ditandai oleh anonimitas pelaku, kecepatan transaksi, dan sifat lintas yurisdiksi yang menghambat efektivitas penegakan hukum nasional. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, perbandingan, dan konseptual untuk menganalisis strategi harmonisasi regulasi internasional dalam menanggulangi tindak pidana keuangan global. Instrumen hukum internasional seperti *United Nations Convention against Transnational Organized Crime* (UNTOC), *United*

Nations Convention against Corruption (UNCAC), dan rekomendasi *Financial Action Task Force* (FATF) dievaluasi efektivitasnya dalam menghadapi tantangan kejahatan ekonomi digital. Hasil penelitian menunjukkan bahwa meskipun telah ada kerangka hukum global, disparitas regulasi, kesenjangan kapasitas teknis, dan lemahnya komitmen politik masih menjadi kendala utama. Penelitian ini merekomendasikan model pengaturan internasional yang mengintegrasikan harmonisasi hukum, mekanisme kerja sama teknis *real-time*, dan adaptasi regulasi yang berkelanjutan untuk memperkuat integritas sistem keuangan global.

Kata Kunci: Kejahatan Ekonomi Digital, Harmonisasi Regulasi, Hukum Internasional, FATF, UNTOC, UNCAC.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah merevolusi tatanan ekonomi global secara fundamental. Transformasi digital mendorong lahirnya ekosistem keuangan yang bersifat tanpa batas, menghubungkan pasar dan aktor ekonomi lintas yurisdiksi secara instan. Inovasi seperti *blockchain*, *cryptocurrency*, *digital banking*, dan sistem pembayaran berbasis *fintech* telah memperluas akses, mempercepat transaksi, dan menciptakan efisiensi ekonomi (Handoko dkk, 2024). Namun, kemajuan ini juga membawa konsekuensi serius dalam bentuk kerentanan terhadap kejahatan ekonomi yang semakin canggih, terdesentralisasi, dan sulit dideteksi oleh mekanisme pengawasan tradisional.

Globalisasi ekonomi digital telah menghasilkan peluang besar bagi pertumbuhan ekonomi, tetapi pada saat yang sama memunculkan ruang kriminalitas lintas negara yang sulit diantisipasi. Kejahatan ekonomi berbasis teknologi—termasuk pencucian uang digital, penipuan berbasis kripto, *cyber laundering*, dan pendanaan terorisme melalui aset virtual—memanfaatkan celah hukum dan disparitas regulasi antarnegara. Fenomena ini menempatkan hukum internasional dalam posisi strategis namun penuh tantangan, karena sifat kejahatan tersebut yang lintas yurisdiksi dan memanfaatkan infrastruktur digital global yang tidak mengenal batas teritorial.

Perubahan modus operandi pelaku kejahatan ekonomi global di era digital menunjukkan adanya *shift* dari pendekatan konvensional menuju strategi yang memanfaatkan anonimitas, kecepatan, dan kompleksitas teknologi. Penggunaan *privacy coins*, transaksi lintas *peer-to-peer*, serta platform *decentralized finance* (DeFi) memungkinkan perpindahan nilai dalam jumlah besar tanpa memerlukan perantara keuangan formal. Karakteristik ini secara signifikan mengurangi jejak digital yang dapat ditelusuri oleh otoritas penegak hukum, sehingga memperlemah efektivitas kerangka pengawasan nasional.

Secara yuridis, kejahatan ekonomi berbasis teknologi menantang prinsip-prinsip klasik yurisdiksi negara yang umumnya bersifat teritorial. Hukum pidana ekonomi nasional sering kali tidak memiliki jangkauan yang memadai untuk menindak pelaku yang beroperasi di luar negeri atau memanfaatkan server dan infrastruktur yang tersebar di berbagai negara. Di sisi lain, perjanjian internasional yang ada—seperti *United Nations Convention against Transnational Organized Crime* (UNTOC) dan *United Nations Convention against Corruption* (UNCAC)—belum sepenuhnya dirancang untuk menghadapi kompleksitas instrumen keuangan digital yang terus berevolusi (Haider, 2024).

Ketiadaan harmonisasi regulasi internasional juga menjadi faktor yang memperburuk situasi. Banyak negara mengadopsi kebijakan domestik yang tidak selaras dalam mendefinisikan, mengkriminalisasi, dan mengatur instrumen keuangan digital (Setiawan, 2024). Ketidaksamaan ini menciptakan *regulatory arbitrage*, yaitu praktik di mana pelaku kejahatan memindahkan aktivitasnya ke yurisdiksi dengan regulasi lemah atau pengawasan

longgar. Akibatnya, penegakan hukum menjadi terfragmentasi, dan upaya pemberantasan kejahatan ekonomi global tidak mencapai efektivitas secara optimal.

Dalam konteks ini, urgensi pengaturan internasional terhadap kejahatan ekonomi berbasis teknologi menjadi semakin nyata. Standar internasional yang dikembangkan oleh lembaga seperti *Financial Action Task Force* (FATF) telah menjadi rujukan penting, namun implementasinya di tingkat nasional sering kali menghadapi kendala politik, teknis, dan sumber daya (Nanyun & Nasiri, 2021). Tanpa kerangka kerja global yang mengikat dan terintegrasi, celah hukum akan terus dimanfaatkan oleh aktor kriminal untuk menghindari deteksi dan penuntutan.

Dampak kejahatan ekonomi berbasis teknologi tidak hanya bersifat ekonomi, tetapi juga merambah pada dimensi keamanan dan stabilitas global (Munajat & Yusuf, 2024). Aliran dana ilegal dapat membiayai aktivitas terorisme, mendestabilisasi sistem perbankan, serta menggerus kepercayaan publik terhadap institusi keuangan dan pemerintahan. Dalam jangka panjang, fenomena ini dapat mengancam integritas sistem keuangan internasional, menghambat pertumbuhan ekonomi berkelanjutan, dan merusak legitimasi tata kelola global.

Oleh karena itu, kajian ini memandang bahwa pengaturan internasional yang komprehensif, adaptif terhadap teknologi, dan selaras dengan prinsip *good governance* merupakan kebutuhan mendesak dalam menghadapi realitas kejahatan ekonomi di era digital. Sinergi antara instrumen hukum internasional, mekanisme kerja sama lintas negara, dan inovasi teknologi pengawasan harus dibangun untuk memastikan bahwa kemajuan teknologi tidak menjadi pedang bermata dua yang menguntungkan pelaku kejahatan sekaligus merugikan masyarakat global.

Rumusan Masalah

1) Bagaimana karakteristik dan perkembangan kejahatan ekonomi global berbasis teknologi di era digital?
2) Sejauh mana efektivitas pengaturan hukum internasional dalam menanggulangi kejahatan ekonomi digital lintas negara?
3) Model pengaturan internasional seperti apa yang ideal untuk menghadapi kejahatan ekonomi berbasis teknologi secara efektif dan adaptif?

Tujuan Penelitian

1) Menganalisis karakteristik dan perkembangan kejahatan ekonomi global berbasis teknologi di era digital.
2) Mengevaluasi efektivitas pengaturan hukum internasional dalam menanggulangi kejahatan ekonomi digital lintas negara.
3) Merumuskan model pengaturan internasional yang ideal, efektif, dan adaptif terhadap dinamika teknologi untuk menghadapi kejahatan ekonomi berbasis teknologi.

Signifikansi dan Kebaruan Penelitian

Penelitian ini memiliki signifikansi akademik dan praktis karena mengisi kekosongan kajian yang mengintegrasikan analisis hukum internasional dengan perkembangan teknologi finansial digital dalam konteks kejahatan ekonomi global. Pertama, penelitian ini memberikan kontribusi konseptual dengan mengkaji keterbatasan instrumen hukum internasional yang ada dalam menghadapi modus kejahatan berbasis teknologi yang terus berevolusi. Kedua, secara praktis, hasil penelitian ini diharapkan menjadi rujukan bagi pembuat kebijakan dalam merumuskan strategi harmonisasi regulasi internasional yang efektif dan adaptif terhadap inovasi teknologi. Ketiga, kebaruan penelitian ini terletak pada pendekatan interdisipliner yang menggabungkan perspektif hukum, teknologi, dan tata kelola global untuk merumuskan model

pengaturan internasional yang komprehensif dalam menanggulangi kejahatan ekonomi digital lintas negara.

Teori Hukum Pidana Internasional

Teori hukum pidana internasional memegang peranan fundamental dalam membentuk kerangka konseptual yang mengatur penegakan hukum terhadap kejahatan lintas negara, termasuk kejahatan ekonomi berbasis teknologi. Landasan ini menegaskan bahwa yurisdiksi negara tidak hanya terbatas pada batas-batas teritorial, tetapi dapat diperluas melalui prinsip-prinsip seperti *universal jurisdiction*, *extraterritoriality*, dan *mutual legal assistance*. Penerapan prinsip-prinsip tersebut memungkinkan negara untuk menindak pelaku meskipun kejahatan dilakukan di luar wilayahnya, selama perbuatan tersebut berdampak signifikan pada kepentingan nasional atau keamanan internasional. Dalam kerangka kejahatan digital, fleksibilitas ini menjadi krusial karena ruang siber secara inheren meniadakan batas geografis.

Menurut Mufty (2025), efektivitas hukum pidana internasional dalam menanggulangi kejahatan transnasional sangat bergantung pada sejauh mana negara-negara bersedia menginternalisasi norma internasional ke dalam sistem hukum nasionalnya. Proses ini tidak sekadar menyangkut adopsi regulasi formal, tetapi juga meliputi pembangunan kapasitas institusional, koordinasi lintas lembaga, dan penerapan mekanisme kerja sama internasional yang efektif. Dalam konteks kejahatan ekonomi berbasis teknologi, integrasi ini menghadapi hambatan yang signifikan, seperti disparitas definisi hukum, perbedaan standar pembuktian, dan kesenjangan kemampuan teknis antara negara maju dan berkembang.

Tantangan penerapan teori hukum pidana internasional dalam menghadapi kejahatan berbasis teknologi terletak pada sifat teknologi yang dinamis, terdesentralisasi, dan sering kali melampaui prediksi pembentuk undang-undang. Perubahan cepat dalam modus operandi pelaku, seperti pemanfaatan *blockchain*, *privacy coins*, dan *decentralized finance*, menuntut penyesuaian cepat pada kerangka hukum yang berlaku. Hal ini memerlukan pembaruan norma secara berkala, peningkatan kolaborasi antarnegara, dan penguatan mekanisme investigasi lintas yurisdiksi yang memanfaatkan *digital forensics* canggih. Tanpa respons adaptif yang terkoordinasi secara global, teori hukum pidana internasional berisiko kehilangan relevansi dalam menghadapi tantangan kejahatan ekonomi di era digital.

Konsep Kejahatan Ekonomi Global

Kejahatan ekonomi global pada hakikatnya merupakan bentuk tindak pidana yang memiliki implikasi lintas batas negara, dengan melibatkan aktor-aktor yang beroperasi dalam jaringan transnasional dan berdampak langsung terhadap stabilitas sistem ekonomi internasional. Karakteristiknya mencakup keterkaitan erat antara dimensi ekonomi, hukum, dan politik global, sehingga penanganannya menuntut respons kolektif dari berbagai yurisdiksi. Sebagaimana dikemukakan oleh Grabosky (2016), kejahatan ekonomi global tidak terbatas pada satu bentuk pelanggaran hukum, melainkan mencakup spektrum luas seperti pencucian uang, penipuan lintas negara, penggelapan pajak internasional, dan pendanaan terorisme. Kompleksitas ini menjadikan fenomena tersebut sebagai salah satu ancaman paling signifikan bagi integritas sistem keuangan global.

Dalam era digital, kejahatan ekonomi global mengalami transformasi signifikan melalui adopsi teknologi mutakhir yang mengubah modus operandi pelaku. Pemanfaatan *blockchain*, *cryptocurrency*, dan *decentralized finance* telah memperkenalkan tingkat anonimitas dan kecepatan transaksi yang belum pernah terjadi sebelumnya (Nuryanto & Pramudianto, 2021). Inovasi ini, meskipun memberikan manfaat ekonomi, sekaligus dimanfaatkan oleh aktor kriminal untuk menyamarkan aliran dana ilegal, mempersulit pelacakan, serta mengaburkan jejak transaksi di lintas yurisdiksi. Hal ini menciptakan tantangan besar bagi otoritas penegak hukum yang harus menyesuaikan metode investigasi dengan perkembangan teknologi yang sangat dinamis.

Kompleksitas kejahatan ekonomi global di era digital diperparah oleh adanya disparitas regulasi antarnegara, yang membuka peluang *regulatory arbitrage* bagi pelaku. Ketidaksinkronan hukum ini memungkinkan mereka memindahkan aktivitas ilegal ke yurisdiksi dengan pengawasan lemah atau celah hukum yang longgar. Dalam konteks ini, pendekatan nasional semata menjadi tidak memadai, sehingga dibutuhkan harmonisasi regulasi internasional yang komprehensif. Tanpa upaya kolektif yang terkoordinasi secara global, sistem keuangan internasional akan tetap rentan terhadap eksploitasi oleh jaringan kriminal transnasional yang adaptif dan inovatif dalam memanfaatkan teknologi.

Kejahatan ekonomi Berbasis Teknologi (*Digital Financial Crime*)

Kejahatan ekonomi berbasis teknologi merepresentasikan evolusi dari kejahatan ekonomi yang memanfaatkan secara optimal perkembangan teknologi digital sebagai sarana, infrastruktur, sekaligus modus operandi. Fenomena ini mencakup aktivitas kriminal yang dilakukan melalui perangkat elektronik, jaringan internet, dan platform digital yang saling terhubung secara global. Berdasarkan laporan *United Nations Office on Drugs and Crime* (UNODC, 2022), bentuk-bentuk kejahatan ini meliputi *cyber laundering*, penipuan daring (*online fraud*), serangan terhadap infrastruktur keuangan, serta pemanfaatan aset kripto untuk kegiatan ilegal. Perkembangan ini menunjukkan adanya pergeseran signifikan dari pola konvensional menuju modus berbasis teknologi yang lebih kompleks dan sulit diantisipasi.

Karakteristik utama dari kejahatan ekonomi berbasis teknologi adalah anonimitas pelaku, kecepatan perpindahan nilai, dan minimnya jejak transaksi yang dapat ditelusuri. Pemanfaatan teknologi seperti *blockchain* dan protokol kriptografi memungkinkan pelaku untuk memindahkan dana dalam skala besar tanpa memerlukan perantara keuangan formal (Pangestu, 2023). Hal ini tidak hanya mengurangi visibilitas otoritas terhadap aliran dana, tetapi juga menciptakan hambatan signifikan dalam pengumpulan bukti dan penetapan identitas pelaku. Kecepatan transaksi yang dapat terjadi dalam hitungan detik semakin mempersempit ruang intervensi aparat penegak hukum.

Tantangan dalam menanggulangi kejahatan ekonomi berbasis teknologi semakin kompleks karena sifatnya yang lintas yurisdiksi dan terdesentralisasi. Sistem keuangan digital memungkinkan pelaku beroperasi dari berbagai negara sekaligus, memanfaatkan perbedaan regulasi dan kelemahan koordinasi antarotoritas. Di sisi lain, instrumen hukum internasional yang ada sering kali belum dirancang secara spesifik untuk menghadapi kompleksitas teknologi ini, sehingga diperlukan pembaruan regulasi yang adaptif dan mekanisme kerja sama internasional yang lebih intensif. Tanpa pembaruan tersebut, kejahatan ekonomi berbasis teknologi berpotensi berkembang menjadi ancaman sistemik terhadap stabilitas keuangan global.

Instrumen Hukum Internasional yang Relevan

Instrumen hukum internasional memainkan peran penting dalam membentuk kerangka regulasi global untuk menanggulangi kejahatan ekonomi berbasis teknologi. Beberapa konvensi utama seperti *United Nations Convention against Transnational Organized Crime* (UNTOC) dan *United Nations Convention against Corruption* (UNCAC) memberikan landasan normatif bagi kerja sama antarnegara dalam pencegahan, penegakan hukum, dan ekstradisi pelaku kejahatan ekonomi lintas batas (Rose, 2020). Kedua instrumen ini memuat ketentuan yang dapat diadaptasi untuk mengatur kejahatan digital, meskipun awalnya tidak dirancang secara khusus untuk menghadapi teknologi finansial modern. Selain itu, lembaga internasional seperti *Financial Action Task Force* (FATF) berperan menetapkan standar global terkait pencegahan pencucian uang (*anti-money laundering/AML*) dan pendanaan terorisme (*counter-terrorism financing/CTF*), yang kini juga mencakup pengaturan aset virtual.

Meskipun kerangka internasional tersebut telah menyediakan dasar yang komprehensif, efektivitasnya sangat bergantung pada kesediaan dan kemampuan negara-negara anggota untuk mengadopsi dan mengimplementasikan ketentuan yang disepakati. Dalam praktiknya,

terdapat kesenjangan signifikan antara standar internasional dan legislasi nasional, terutama di negara berkembang yang menghadapi keterbatasan sumber daya teknis dan institusional. Hal ini sering kali mengakibatkan pelaksanaan ketentuan internasional menjadi parsial, sehingga menciptakan celah hukum yang dapat dieksploitasi oleh pelaku kejahatan ekonomi digital.

Di tengah perkembangan teknologi yang sangat cepat, instrumen hukum internasional yang ada perlu diperkuat melalui amandemen, protokol tambahan, atau pembentukan perjanjian baru yang secara eksplisit mengatur teknologi finansial digital. Pembaruan ini harus mencakup definisi yang jelas, mekanisme *real-time information sharing*, serta prosedur *digital evidence gathering* yang diakui lintas yurisdiksi. Selain itu, diperlukan mekanisme *compliance review* yang ketat untuk memastikan bahwa negara-negara tidak hanya mengadopsi regulasi secara formal, tetapi juga menerapkannya secara efektif. Tanpa langkah-langkah ini, efektivitas instrumen hukum internasional dalam menghadapi kejahatan ekonomi berbasis teknologi akan terus tertinggal dari inovasi yang dimanfaatkan oleh pelaku kriminal.

Tantangan Harmonisasi Regulasi Internasional

Harmonisasi regulasi internasional merupakan prasyarat krusial dalam penanggulangan kejahatan ekonomi berbasis teknologi, mengingat sifatnya yang lintas batas dan sangat bergantung pada koordinasi antarnegara. Namun, proses harmonisasi ini menghadapi berbagai tantangan struktural maupun substantif. Perbedaan sistem hukum—baik dalam tradisi *civil law, common law,* maupun hukum campuran—menyebabkan perbedaan dalam pendekatan terhadap definisi kejahatan, alat bukti, dan prosedur hukum. Selain itu, perbedaan tingkat kematangan teknologi, kapasitas kelembagaan, dan kepentingan ekonomi-politik antarnegara memperparah fragmentasi regulatif yang ada.

Salah satu bentuk nyata dari ketidakharmonisan ini adalah fenomena *regulatory arbitrage*, yaitu situasi ketika pelaku kejahatan memanfaatkan yurisdiksi yang memiliki regulasi lemah atau tidak jelas untuk menghindari deteksi dan penindakan hukum (Minto dkk, 2021). Hal ini semakin diperparah oleh ketidaksinkronan dalam pengakuan hukum terhadap aset digital seperti kripto, NFT, atau platform DeFi, yang belum diatur secara seragam dalam hukum nasional. Di beberapa negara, aset kripto dikategorikan sebagai komoditas, sementara di negara lain dianggap sebagai mata uang atau sekuritas—perbedaan ini menciptakan celah hukum yang dapat dengan mudah dieksploitasi.

Hambatan lainnya bersumber dari lemahnya mekanisme koordinasi internasional yang belum mengakomodasi kompleksitas kejahatan digital kontemporer. Meskipun terdapat inisiatif multilateral seperti FATF, Interpol, dan Egmont Group, kerja sama lintas negara masih menghadapi kendala administratif, perbedaan bahasa hukum, dan kerahasiaan data finansial. Di tengah urgensi penegakan hukum yang cepat dan terintegrasi, kecepatan respons institusi internasional sering kali tertinggal dari kecepatan inovasi teknologi yang dimanfaatkan oleh pelaku kejahatan. Oleh karena itu, dibutuhkan reformulasi mekanisme harmonisasi regulasi yang tidak hanya bersifat formal, tetapi juga substantif dan operasional, untuk menjawab dinamika kejahatan ekonomi digital secara efektif.

Pendekatan Interdisipliner dalam Pengaturan

Pendekatan interdisipliner dalam pengaturan kejahatan ekonomi berbasis teknologi merupakan kebutuhan strategis yang lahir dari kompleksitas fenomena ini, di mana dimensi hukum, teknologi, ekonomi, dan keamanan saling berkelindan (Romadhonia, 2025). Perspektif hukum diperlukan untuk menetapkan kerangka normatif, sementara pemahaman teknologi berfungsi mengidentifikasi celah dan potensi penyalahgunaan sistem digital. Di sisi lain, analisis ekonomi berkontribusi dalam menilai dampak makro maupun mikro dari aliran dana ilegal, sedangkan dimensi keamanan menekankan mitigasi risiko terhadap stabilitas nasional dan internasional. Integrasi keempat aspek ini membentuk basis kebijakan yang lebih komprehensif dan adaptif.

Dalam praktiknya, pendekatan interdisipliner memerlukan kolaborasi aktif antara otoritas penegak hukum, regulator keuangan, penyedia layanan teknologi, dan lembaga penelitian (Disantara, 2024). Misalnya, *digital forensics* yang dikelola oleh lembaga penegak hukum harus didukung oleh keahlian teknis dari sektor swasta yang menguasai arsitektur sistem dan algoritma keamanan. Kolaborasi semacam ini juga harus dilengkapi dengan protokol pertukaran data lintas negara yang aman, cepat, dan sesuai dengan prinsip perlindungan privasi. Dengan demikian, pengaturan yang dihasilkan tidak hanya berbasis norma hukum, tetapi juga berlandaskan pemahaman teknis yang solid.

Keberhasilan pendekatan interdisipliner sangat bergantung pada mekanisme tata kelola global yang mampu mengkoordinasikan berbagai kepentingan lintas sektor dan lintas yurisdiksi. Untuk itu, diperlukan forum internasional yang secara khusus menangani isu kejahatan ekonomi digital, dengan mandat yang mencakup harmonisasi regulasi, peningkatan kapasitas teknis negara anggota, serta penyusunan protokol bersama untuk penegakan hukum. Pendekatan ini diharapkan mampu menjembatani kesenjangan antara kecepatan inovasi teknologi dengan adaptasi regulasi, sehingga pengaturan yang diterapkan tidak hanya efektif dalam jangka pendek, tetapi juga berkelanjutan dalam menghadapi tantangan masa depan.

METODE

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan (*statute approach*), perbandingan hukum (*comparative approach*), dan pendekatan konseptual (*conceptual approach*). Bahan hukum primer meliputi instrumen hukum internasional seperti *United Nations Convention against Transnational Organized Crime* (UNTOC), *United Nations Convention against Corruption* (UNCAC), dan rekomendasi *Financial Action Task Force* (FATF), serta peraturan perundang-undangan nasional terkait pencegahan dan pemberantasan kejahatan ekonomi berbasis teknologi. Bahan hukum sekunder diperoleh dari literatur ilmiah, jurnal hukum, laporan lembaga internasional, dan kajian akademis terbaru, sedangkan bahan hukum tersier meliputi kamus hukum dan ensiklopedia hukum. Analisis dilakukan secara kualitatif dengan menelaah kesesuaian, efektivitas, dan kelengkapan pengaturan internasional dalam menghadapi kejahatan ekonomi digital lintas negara, guna merumuskan model pengaturan internasional yang ideal dan adaptif terhadap perkembangan teknologi.

HASIL DAN PEMBAHASAN

Karakteristik dan Perkembangan Kejahatan Ekonomi Global Berbasis Teknologi di Era Digital

Perkembangan teknologi informasi dan komunikasi telah mendorong pergeseran mendasar dalam modus operandi kejahatan ekonomi global (Supanto, 2023). Kejahatan yang sebelumnya mengandalkan mekanisme fisik atau jaringan terstruktur secara konvensional kini beralih memanfaatkan infrastruktur digital yang bersifat lintas batas, terdesentralisasi, dan berkecepatan tinggi. Fenomena ini terlihat pada meningkatnya *cyber laundering*, penipuan daring lintas negara, serangan terhadap sistem perbankan internasional, serta pemanfaatan aset kripto untuk menyamarkan aliran dana ilegal. Perubahan ini mengaburkan batas yurisdiksi tradisional, menantang prinsip teritorialitas hukum pidana, dan memerlukan kerangka hukum internasional yang lebih responsif.

Salah satu karakteristik utama kejahatan ekonomi berbasis teknologi adalah tingkat anonimitas yang tinggi, di mana pelaku dapat menyembunyikan identitas melalui *privacy-enhancing technologies* seperti *mixers*, *tumblers*, atau *privacy coins*. Teknologi *blockchain* yang awalnya dirancang untuk transparansi justru dimanfaatkan untuk menciptakan transaksi yang sulit dilacak, terutama ketika dipadukan dengan jaringan *dark web* yang menyediakan pasar gelap global. Karakteristik lainnya adalah *instantaneity*—yakni kemampuan mentransfer

dana dalam hitungan detik tanpa perantara bank tradisional, sehingga mempersempit peluang otoritas untuk melakukan intervensi atau pembekuan aset secara efektif.

Data empiris menunjukkan tren peningkatan signifikan dalam kasus kejahatan ekonomi berbasis teknologi. Menurut laporan *Chainalysis Crypto Crime Report 2023*, nilai aset kripto yang terlibat dalam aktivitas ilegal pada tahun 2022 mencapai lebih dari USD 20 miliar, meningkat dibandingkan tahun sebelumnya. Angka ini mencerminkan tidak hanya eskalasi frekuensi kejahatan, tetapi juga semakin kompleksnya metode yang digunakan pelaku (Semenoh dkk, 2025). Modus-modus baru seperti *cross-chain bridge exploitation* dan *flash loan attacks* menjadi contoh nyata inovasi kriminal di sektor keuangan digital. Hal ini memperkuat argumentasi bahwa perkembangan teknologi tidak dapat dilepaskan dari risiko penyalahgunaan, sehingga memerlukan mekanisme hukum internasional yang mampu mengantisipasi dinamika tersebut secara berkelanjutan.

Secara konseptual, kejahatan ekonomi digital di era globalisasi bukan hanya sekadar *high-tech crime*, melainkan bagian integral dari kejahatan ekonomi transnasional yang mempengaruhi stabilitas sistem keuangan internasional. Perbedaannya terletak pada kapasitas teknologi untuk memperluas skala, mempercepat waktu, dan meminimalisir risiko deteksi bagi pelaku. Akibatnya, kerangka hukum nasional yang berdiri sendiri menjadi tidak memadai karena keterbatasan yurisdiksi dan kemampuan teknis. Situasi ini menuntut kehadiran pengaturan internasional yang tidak hanya mengharmonisasikan norma hukum, tetapi juga mengintegrasikan mekanisme teknis seperti *real-time information sharing*, kerja sama *digital forensics*, dan *joint cyber task forces* lintas negara.

Efektivitas Pengaturan Hukum Internasional dalam Menanggulangi Kejahatan ekonomi Digital Lintas Negara

Pengaturan hukum internasional yang berlaku saat ini telah menyediakan kerangka umum untuk penanggulangan kejahatan ekonomi lintas negara, termasuk yang berbasis teknologi. Instrumen seperti *United Nations Convention against Transnational Organized Crime* (UNTOC) dan *United Nations Convention against Corruption* (UNCAC) memuat ketentuan yang relevan untuk memperkuat kerja sama internasional dalam ekstradisi, bantuan hukum timbal balik (*mutual legal assistance*), dan pembekuan aset lintas yurisdiksi. Namun, meskipun konvensi tersebut dapat diterapkan pada kejahatan ekonomi digital, substansi regulasinya belum sepenuhnya mengantisipasi karakteristik unik aset virtual, *decentralized finance* (DeFi), dan teknologi kripto yang terus berkembang. Hal ini menyebabkan efektivitasnya terbatas pada kerangka hukum yang bersifat generik.

Selain itu, keberadaan *Financial Action Task Force* (FATF) sebagai lembaga pembuat standar global di bidang anti-pencucian uang (*anti-money laundering/AML*) dan pencegahan pendanaan terorisme (*counter-terrorism financing/CTF*) telah menghasilkan *FATF Recommendations* yang mencakup panduan pengaturan aset virtual dan *Virtual Asset Service Providers* (VASPs). Rekomendasi FATF tahun 2019 memperkenalkan prinsip *travel rule*, yang mewajibkan pertukaran informasi identitas pengirim dan penerima dalam transaksi aset virtual. Meskipun efektif di negara-negara dengan kepatuhan tinggi, implementasi di tingkat global masih timpang. Perbedaan kapasitas teknis dan resistensi politik di sebagian yurisdiksi menghambat pencapaian *level playing field* yang diperlukan untuk menghilangkan *regulatory arbitrage*.

Studi kasus internasional menunjukkan adanya keberhasilan parsial dan kegagalan yang signifikan. Misalnya, di Uni Eropa, penerapan *Fifth Anti-Money Laundering Directive* (5AMLD) yang mewajibkan pendaftaran penyedia layanan aset virtual mampu meningkatkan transparansi di sektor kripto (Capraro, 2021). Namun, di kawasan Asia Tenggara, disparitas regulasi antarnegara—seperti perbedaan dalam mengkriminalisasi *peer-to-peer crypto transactions*—masih menjadi celah yang dimanfaatkan pelaku. Contoh lain dapat dilihat dari kasus peretasan *Ronin Network* (2022) yang melibatkan kerugian lebih dari USD 600 juta, di

mana upaya pelacakan dan pemulihan aset terhambat oleh keterbatasan akses lintas yurisdiksi dan ketiadaan mekanisme koordinasi yang bersifat mengikat secara hukum.

Dari perspektif normatif-kritis, efektivitas pengaturan internasional dalam konteks ini sangat dipengaruhi oleh dua faktor utama: pertama, keberadaan norma internasional yang jelas, spesifik, dan adaptif terhadap perubahan teknologi; kedua, adanya mekanisme implementasi dan penegakan yang bersifat *mandatory* bagi seluruh negara anggota. Tanpa komitmen politik yang kuat dan penyesuaian regulasi yang konsisten, instrumen hukum internasional akan tertinggal dari laju inovasi teknologi yang dimanfaatkan oleh pelaku kejahatan ekonomi digital. Oleh karena itu, diperlukan reformasi regulasi internasional yang mengintegrasikan prinsip-prinsip *real-time cooperation*, *digital evidence standardization*, dan *cross-border asset recovery* yang diakui secara universal.

Model Pengaturan Internasional yang Ideal, Efektif, dan Adaptif terhadap Dinamika Teknologi

Model pengaturan internasional yang ideal dalam menanggulangi kejahatan ekonomi berbasis teknologi harus dibangun di atas tiga pilar utama: harmonisasi hukum, responsivitas terhadap perkembangan teknologi, dan penguatan mekanisme kerja sama lintas negara. Harmonisasi hukum berfungsi mengurangi *regulatory arbitrage* dengan menciptakan keseragaman definisi tindak pidana, mekanisme kriminalisasi, dan prosedur penegakan di seluruh yurisdiksi. Pendekatan ini dapat diwujudkan melalui protokol tambahan (*additional protocol*) terhadap *United Nations Convention against Transnational Organized Crime* (UNTOC) atau *United Nations Convention against Corruption* (UNCAC) yang secara eksplisit mengatur tata kelola aset virtual, *decentralized finance* (DeFi), dan instrumen keuangan berbasis teknologi lainnya.

Efektivitas model ini juga memerlukan integrasi yang erat antara instrumen hukum dan mekanisme teknis. Salah satu opsi adalah membentuk *Global Digital Financial Crime Task Force* di bawah koordinasi PBB atau *Financial Action Task Force* (FATF) dengan mandat mengoordinasikan investigasi, pembekuan aset, serta penuntutan lintas yurisdiksi secara serentak. Mekanisme tersebut perlu dilengkapi dengan sistem komunikasi aman (*secure communication channels*) yang sesuai dengan standar keamanan siber global serta memiliki kemampuan *real-time information sharing*. Contoh penerapan yang dapat diadaptasi adalah model *European Cybercrime Centre* (EC3) di bawah Europol, yang berhasil memfasilitasi operasi gabungan antarnegara anggota Uni Eropa dalam menangani kejahatan siber kompleks.

Adaptivitas terhadap perubahan teknologi merupakan elemen esensial agar pengaturan internasional tetap relevan dan efektif. Kecepatan inovasi di sektor keuangan digital, seperti munculnya protokol *cross-chain bridges*, *flash loans*, dan *non-fungible tokens* (NFT) sebagai instrumen pencucian uang, menuntut adanya unit pengawasan teknologi (*technology foresight unit*) di dalam badan internasional yang bertugas memantau tren, menilai risiko, dan merekomendasikan pembaruan regulasi secara berkala. Dengan demikian, pengaturan yang dihasilkan tidak hanya reaktif terhadap kejadian kriminal, tetapi juga proaktif dalam mencegah penyalahgunaan teknologi baru.

Implementasi model ini memerlukan kolaborasi erat dengan sektor swasta dan penyedia layanan teknologi keuangan, mengingat mereka memegang peranan penting dalam deteksi dini aktivitas mencurigakan. Penyedia *Virtual Asset Service Providers* (VASPs) dapat diwajibkan untuk mengadopsi *know your customer* (KYC) yang diperketat, *transaction monitoring systems*, serta protokol pelaporan yang terintegrasi dengan pusat intelijen keuangan nasional dan internasional. Di sisi lain, keterlibatan lembaga riset dan akademisi dapat memastikan bahwa desain kebijakan berbasis bukti (*evidence-based policy*) dan mempertimbangkan implikasi sosial-ekonomi dari setiap intervensi regulasi.

Dalam jangka panjang, model pengaturan internasional yang ideal harus bersifat inklusif, mengakomodasi partisipasi negara maju maupun berkembang, serta memberikan dukungan

teknis bagi negara dengan kapasitas terbatas. Tanpa inklusivitas ini, kesenjangan regulasi akan terus menjadi titik lemah yang dapat dieksploitasi pelaku kejahatan. Oleh karena itu, dibutuhkan mekanisme pendanaan bersama (*pooled funding mechanism*) untuk memperkuat infrastruktur penegakan hukum, membangun kapasitas teknis, dan memperluas jaringan kerja sama lintas batas. Dengan menggabungkan harmonisasi regulasi, dukungan teknis global, adaptasi berkelanjutan, serta kolaborasi multisektor, pengaturan internasional dapat menjadi instrumen yang efektif sekaligus berkelanjutan dalam menghadapi tantangan kejahatan ekonomi berbasis teknologi di era digital.

KESIMPULAN

Sesuai dengan hasil analisis dan pembahasan di atas, bisa ditarik kesimpulan bahwa kejahatan ekonomi berbasis teknologi telah menjadi bagian integral dari kejahatan ekonomi global yang bersifat lintas yurisdiksi, memanfaatkan kemajuan teknologi digital untuk memperluas jangkauan, mempercepat transaksi, dan meminimalkan risiko deteksi. Karakteristik seperti anonimitas pelaku, kecepatan perpindahan dana, serta sifat terdesentralisasi membuat modus operandi kejahatan ini sulit diantisipasi oleh kerangka hukum nasional yang bersifat teritorial. Meskipun instrumen hukum internasional seperti UNTOC, UNCAC, dan rekomendasi FATF telah menyediakan landasan kerja sama, efektivitasnya masih terbatas akibat disparitas regulasi, perbedaan kapasitas teknis, dan lemahnya komitmen politik negara-negara anggota.

Kajian ini menegaskan bahwa pengaturan internasional yang ideal harus berlandaskan pada harmonisasi hukum yang mengikat, integrasi mekanisme teknis *real-time cooperation*, serta adaptasi berkelanjutan terhadap inovasi teknologi. Tanpa langkah-langkah ini, risiko *regulatory arbitrage* dan fragmentasi regulasi akan terus dimanfaatkan oleh pelaku kejahatan, sehingga mengancam stabilitas sistem keuangan global. Oleh karena itu, pembaruan regulasi internasional yang inklusif, komprehensif, dan berbasis kolaborasi multisektor menjadi kebutuhan mendesak.

Rekomendasi Kebijakan

1) Pembentukan Protokol Internasional Khusus Kejahatan ekonomi Digital di bawah UNTOC atau UNCAC, yang memuat definisi, kriminalisasi, dan prosedur penegakan hukum terkait aset virtual, *decentralized finance*, dan teknologi keuangan lainnya.
2) Pendirian *Global Digital Financial Crime Task Force* di bawah mandat PBB atau FATF, dengan kewenangan koordinasi investigasi, pembekuan aset, pertukaran data *real-time*, dan penyusunan protokol *digital evidence* yang diakui lintas yurisdiksi.
3) Penguatan Kapasitas Negara Berkembang melalui mekanisme pendanaan bersama (*pooled funding mechanism*) untuk mendukung infrastruktur teknologi, pelatihan *digital forensics*, dan pembaruan regulasi domestik.
4) Kolaborasi Multisektor yang melibatkan sektor swasta, penyedia teknologi, akademisi, dan lembaga internasional dalam pengembangan kebijakan berbasis bukti dan teknologi pendukung deteksi dini aktivitas mencurigakan.
5) Penerapan Mekanisme Evaluasi Kepatuhan Global yang bersifat *mandatory*, dengan sanksi bagi negara yang tidak mematuhi standar pengaturan internasional, guna memastikan efektivitas dan keseragaman implementasi.

REFERENSI

Capraro, T. (2021). *The 5th anti-money laundering directive in the light of virtual currencies: The exploitation of the decentralized system and rising legislative challenges* (Doctoral dissertation, Thesis (Bachelor in Law, European Union and International Law)-School of Business and Governance, Tallinn University of Technology).

Disantara, F. P. (2024). Innovative Legal Approaches for Contemporary Challenges in Indonesia: Pendekatan Hukum Inovatif untuk Tantangan Kontemporer di Indonesia. *Indonesian Journal of Innovation Studies*, *25*(4), 10-21070.

Grabosky, P. (2016). *Keynotes in criminology and criminal justice series: Cybercrime*. Oxford University Press.

Haider, A. (2024). Application of the United Nation Convention against Transnational Organized Crime: An Analysis. *Available at SSRN 4686710*.

Handoko, R. M., Trisna, B. A. A., Pratama, R. D., & Parhusip, J. (2024). Implementasi Blockchain untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *4*(2), 64-74.

Minto, A., Prinz, S., & Wulff, M. (2021). A risk characterization of regulatory arbitrage in financial markets. *European Business organization law review*, *22*(4), 719-752.

Mufty, A. M., SH, M., & SH, M. (2025). *Hukum Pidana Internasional*. Tahta Media Group.

Munajat, A. A., & Yusuf, H. (2024). Peran teknologi informasi dalam pencegahan dan pengungkapan tindak pidana ekonomi khusus: Studi tentang kejahatan keuangan berbasis digital. *Jurnal Intelek Insan Cendikia*, *1*(9), 4853-4865.

Nanyun, N. M., & Nasiri, A. (2021). Role of FATF on financial systems of countries: successes and challenges. *Journal of Money Laundering Control*, *24*(2), 234-245.

Nuryanto, U. W., & Pramudianto, P. (2021, October). Revolusi Digital & Dinamika Perkembangan Cryptocurrency Ditinjau Dari Perspektif Literatur Review. In *National Conference on Applied Business, Education, & Technology (NCABET)* (Vol. 1, No. 1, pp. 264-291).

Pangestu, D. A. (2023). *Penggunaan teknologi blockchain dalam transaksi keuangan syari'ah* (Doctoral dissertation, Universitas Islam Indonesia).

Romadhonia, A. (2025). Mewujudkan Peradilan Pidana Ekonomi yang Inklusif: Kajian atas Praktik dan Regulasi Securities Crowdfunding. *National Multidisciplinary Sciences*, *4*(3), 88-99.

Rose, C. (2020). The creation of a review mechanism for the UN Convention Against Transnational Organized Crime and its protocols. *American Journal of International Law*, *114*(1), 51-67.

Semenoh, A. Y., Perekrestov, M. B., Dmytrishyn, D. M., & Bohachenko, M. M. (2025). Economic Consequences of Crypto-Asset Fraud in the Context of Digital Transformation: Analysis of Costs and the Potential of Preventive Technologies.

Setiawan, D. A. (2024). Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa. *Masalah-Masalah Hukum*, *53*(1), 79-90.

Supanto, D. R., & SH, M. (2023). *Kejahatan ekonomi global dan kebijakan hukum pidana*. Penerbit Alumni.

World Health Organization (WHO). United Nations Office on Drugs and Crime (UNODC).(2020). *International standards for the treatment of drug use disorders: Revised edition incorporating results of field-testing*.