ANALISIS KRITIS TERHADAP PENEGAKAN HUKUM TINDAK PIDANA PENCUCIAN UANG (TPPU) YANG BERASAL DARI KEJAHATAN SIBER DI INDONESIA

Fransma Putra Laia[1], Martono Anggusti[2]
fransma.laia@uhn.ac.id[1], martonoanggusti@uhn.ac.id[2]
Fakultas Hukum Universitas HKBP Nommensen Medan

Abstrak: Perkembangan teknologi informasi yang sangat cepat telah membuka ruang yang signifikan terhadap munculnya bentuk-bentuk kejahatan baru, salah satunya adalah kejahatan siber (cybercrime) yang kerap menjadi sumber dana ilegal bagi tindak pidana pencucian uang (TPPU). Penelitian ini bertujuan untuk menganalisis secara kritis hubungan antara kejahatan siber dan TPPU, serta mengkaji efektivitas penegakan hukum di Indonesia dalam menghadapi fenomena tersebut. Penelitian ini menggunakan metode penelitian hukum normatif, dengan pendekatan perundang-undangan (statute approach), konseptual (conceptual approach), dan perbandingan (comparative approach). Data yang digunakan berasal dari bahan hukum primer, sekunder, dan tersier yang dianalisis dengan cara kualitatif-deskriptif. Hasil penelitian menunjukkan bahwa TPPU yang bersumber dari kejahatan siber telah menjadi bentuk kejahatan lintas batas (transnational crime) yang kompleks, memanfaatkan sistem keuangan digital yaitu cryptocurrency dan platform fintech untuk menyamarkan hasil kejahatan. Pengaturan hukum dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang masih bersifat umum dan belum secara eksplisit mencakup mekanisme pengawasan terhadap aset digital. Hal ini menyebabkan lemahnya efektivitas penegakan hukum terhadap TPPU berbasis cybercrime, baik dari sisi normatif maupun teknis. Oleh karena itu, diperlukan pembaruan hukum nasional melalui revisi terhadap UU TPPU dan penguatan kerja sama antar-lembaga serta internasional, termasuk ratifikasi Budapest Convention on Cybercrime dan penerapan rekomendasi Financial Action Task Force (FATF) terkait pengawasan aset digital. Upaya ini diharapkan dapat memperkuat sistem hukum nasional dalam menghadapi tantangan kejahatan ekonomi digital dan mewujudkan penegakan hukum yang baik dan adaptif atas perkembangan teknologi global.
Kata Kunci: Anak Luar Perkawinan, Hak Waris, Hukum Perdata, Putusan Mahkamah Konstitusi, Yurisprudensi.

Abstract: *Rapid developments in information technology have had a significant impact on the emergence of new forms of crime, one of which is cybercrime, which is often a source of illegal funds for money laundering. This study aims to critically analyze the relationship between cybercrime and ML, as well as to examine the effectiveness of law enforcement in Indonesia in dealing with this phenomenon. This study uses a normative legal research method, with a statute approach, conceptual approach, and comparative approach. The data used comes from primary, secondary, and tertiary legal materials that are analyzed qualitatively and descriptively. The results show that ML originating from cybercrime has become a complex form of transnational crime, utilizing digital financial systems such as cryptocurrency and fintech platforms to disguise the proceeds of crime. The legal provisions in Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering are still general in nature and do not explicitly cover mechanisms for monitoring digital assets. This has resulted in weak law enforcement against cybercrime-based money laundering, both from a normative and technical perspective. Therefore, it is necessary to update national laws by revising the ML Law and strengthening inter-agency and international cooperation, including ratifying the Budapest Convention on Cybercrime and implementing the Financial Action Task Force (FATF) recommendations related to digital asset supervision. These efforts are expected to strengthen the national legal system in facing the challenges of digital economic crime and realize law enforcement that is adaptive to global technological developments.*
Keywords: *Money Laundering, Cybercrime, Law Enforcement.*

PENDAHULUAN

Perkembangan teknologi informasi telah melahirkan paradoks hukum baru: di satu sisi, digitalisasi mempercepat transaksi ekonomi global; di sisi lain, membuka ruang bagi kejahatan siber yang menghasilkan keuntungan finansial luar biasa. Ketika keuntungan itu dialihkan dan disamarkan melalui sistem keuangan digital, maka kejahatan siber bertransformasi menjadi praktik tindak pidana pencucian uang. Fenomena tersebut menantang hukum nasional untuk berevolusi dari sistem analog menuju sistem hukum digital yang adaptif. Kejahatan ini memanfaatkan jaringan komputer dan internet sebagai sarana utama dalam melakukan tindak pidana, seperti penipuan daring, peretasan data, pencurian identitas digital, hingga transaksi keuangan ilegal lintas negara.1

Kejahatan siber sering kali tidak berdiri sendiri, melainkan menjadi pintu masuk bagi tindak pidana lain, salah satunya adalah tindak pidana pencucian uang (money laundering).2 Dalam pandangan hukum pidana kontemporer, Tindak Pidana Pencucian Uang TPPU merupakan bentuk kejahatan yang kompleks dan berdimensi transnasional karena melibatkan pergerakan dana melalui sistem keuangan global dengan tujuan untuk menyamarkan asal-usul hasil kejahatan. Ketika hasil kejahatan siber dimasukkan ke dalam sistem keuangan resmi, baik melalui transaksi perbankan, aset digital, maupun platform keuangan terdesentralisasi (decentralized finance), maka proses tersebut dapat dikategorikan sebagai bagian dari praktik pencucian uang

Indonesia sendiri telah memiliki instrumen hukum yang cukup komprehensif dalam menangani TPPU, yaitu Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Meskipun demikian, regulasi tersebut saat ini masih menghadapi tantangan serius dalam menghadapi modus praktik perbuatan tindak pidana pencucian uang yang bermula dari kejahatan terhadap siber. Hal tersebut dikarenakan karakteristik cybercrime yang bersifat lintas yurisdiksi, anonim, dan sulit dilacak, terutama ketika pelaku menggunakan teknologi enkripsi, mata uang kripto (cryptocurrency), dan jaringan dark web untuk menyembunyikan hasil kejahatannya.3

Fenomena meningkatnya kejahatan siber yang berujung pada tindak pidana pencucian uang (TPPU) menjadi salah satu tantangan terbesar dalam sistem hukum pidana modern. Dalam dua tahun terakhir, kejahatan siber di Indonesia menunjukkan tren kenaikan signifikan, baik dari segi jumlah kasus maupun kerugian finansial yang ditimbulkan. Bentuk-bentuk kejahatan tersebut antara lain phishing (pencurian data pribadi untuk akses rekening korban), ransomware (pemerasan digital dengan enkripsi data korban), skimming (penggandaan data kartu debit/kredit), dan investment scam (penipuan investasi digital dengan modus platform daring).

Menurut data yang dilapor oleh Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) tahun 2023, terdapat peningkatan sebesar 30% laporan transaksi keuangan mencurigakan (LTKM) yang terindikasi terkait dengan aktivitas kejahatan digital dalam dua tahun terakhir, terutama yang melibatkan penggunaan rekening digital, dompet elektronik (e-wallet), dan aset kripto seperti Bitcoin dan USDT. Demikian pula, Direktorat Tindak Pidana Siber (Dittipidsiber) dari Bareskrim Polri mendapat bahwa sepanjang tahun 2023 terdapat lebih dari 15.000 laporan kejahatan siber, dengan sebagian besar di antaranya mengandung unsur penipuan digital yang berpotensi menjadi sumber dana pencucian uang. Kejahatan siber telah berkembang dari sekadar pelanggaran teknologi informasi menjadi rantai kejahatan ekonomi digital, di mana pelaku tidak hanya melakukan penipuan atau peretasan, tetapi juga memanfaatkan hasil kejahatannya melalui proses pencucian uang digital (digital laundering). Modus yang digunakan antara lain penggunaan cryptocurrency, transaksi lintas platform keuangan digital (layering), dan penyimpanan aset melalui darknet atau sistem terdesentralisasi (darknet laundering), yang sulit dilacak oleh otoritas nasional. Fenomena ini memperlihatkan lemahnya system pengawasan dan penegakan hukum terhadap transaksi yang mencurigakan.4 Lembaga negara yaitu Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) telah berupaya meningkatkan kemampuan deteksi terhadap transaksi mencurigakan, namun keterbatasan sumber daya teknologi dan kerja sama internasional masih menjadi hambatan utama.5 Oleh karena itu, diperlukan analisis kritis terhadap bagaimana hukum positif di Indonesia merespons dinamika baru dari TPPU yang bersumber dari cybercrime, serta sejauh mana efektivitas penegakan hukumnya dapat melindungi stabilitas sistem keuangan dan keadilan hukum.

Selain itu, perspektif kritis terhadap penegakan hukum TPPU yang bersumber dari kejahatan siber juga penting untuk menilai apakah instrumen hukum yang ada sudah mampu mengantisipasi

perkembangan modus operandi kejahatan digital. Hal ini meliputi perlunya pembaruan hukum terkait aset digital, peningkatan kerja sama internasional dalam pertukaran data keuangan lintas batas, serta penerapan teknologi forensik digital dalam proses pembuktian hukum.6 Tanpa adanya adaptasi hukum yang cepat dan strategis, Indonesia berpotensi menjadi safe haven bagi pelaku pencucian uang berbasis kejahatan siber di Indonesia.7 Sehingga, kajian ini menjadi relevan untuk dilakukan sebagai upaya memahami secara mendalam hubungan antara cybercrime dan TPPU, mengidentifikasi celah hukum yang masih ada, serta merumuskan langkah- langkah pembaruan hukum yang diperlukan agar penegakan hukum di Indonesia mampu menjawab tantangan kejahatan ekonomi digital yang kian kompleks.8

METODE PENELITIAN

Penelitian ini menggunakan metode hukum normatif, karena penelitiannya focus dalam menitik beratkan pada pengkajian peraturan hukum positif yang berlaku serta prinsip-prinsip hukum yang sangat relevan dengan suatu permasalahan yang dikaji. Penelitian hukum normatif ini berfokus terhadap studi bahan-bahan hukum, baik yang bersifat primer, sekunder, dan juga tersier, dengan tujuan untuk menemukan asas, doktrin, dan konsep hukum yang dapat menjelaskan serta memberikan solusi terhadap isu hukum yang diteliti.

Dalam konteks penelitian ini, pendekatan normatif digunakan untuk menganalisis secara kritis hubungan antara tindak pidana pencucian uang (TPPU) dan kejahatan siber (cybercrime) berdasar pada ketentuan yang termuat di dalam hukum positif di Indonesia dan instrumen hukum internasional. Penelitian ini menelaah bagaimana pengaturan hukum dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta ketentuan internasional seperti Budapest Convention on Cybercrime dan rekomendasi Financial Action Task Force (FATF) diimplementasikan untuk menghadapi praktik TPPU berbasis kejahatan siber.

Pendekatan utama yang dipaki di dalam penelitian hukum yuridis normatif ini meliputi pendekatan undang-undang (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan perbandingan (comparative approach). Pendekatan undang-undang digunakan sebagai cara untuk menelaah secara sistematis peraturan hukum positif yang berkaitan dengan TPPU dan cybercrime, baik di dalam tingkat nasional dan juga internasional. Pendekatan konseptual dilakukan untuk memahami konsep teoritis mengenai pencucian uang, kejahatan siber, serta hubungan antara keduanya dalam sistem hukum pidana modern. Sementara pendekatan perbandingan digunakan untuk menelaah praktik dan pengaturan hukum dari negara lain yang telah mengatur lebih komprehensif tentang pencucian uang berbasis kejahatan digital, seperti Amerika Serikat, Inggris, dan Singapura, sebagai bahan refleksi terhadap sistem hukum Indonesia.

Sumber hukum yang digunakan untuk penelitian ini meliputi tiga jenis, yakni bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan nasional dan instrumen hukum internasional yang relevan, antara lain: Undang-Undang Nomor 8 Tahun 2010, Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016, serta Budapest Convention on Cybercrime dan FATF Recommendations. Bahan yang dipakai dalam hukum sekunder mencakup literatur ilmiah seperti buku, jurnal hukum, hasil penelitian, laporan lembaga (PPATK),

UNODC, FATF), dan publikasi akademik yang membahas isu pencucian uang dan kejahatan siber. Sedangkan yang dipakai dalam bahan dari hukum tersier berupa kamus hukum, ensiklopedia hukum, serta referensi daring terpercaya yang mendukung pemahaman terminologi hukum yang digunakan.

Teknik dari pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), dengan menelaah bermacam-macam sumber hukum yang relevan untuk mendapatkan pemahaman

yang komprehensif terhadap isu penelitian. Sumber hukum yang didapatkan yang kemudian ditelaah menggunakan metode analisis kualitatif-deskriptif, yaitu dengan cara menggambarkan, menafsirkan, dan mengkaji keterkaitan antar- norma hukum serta penerapannya dalam praktik penegakan hukum terhadap TPPU yang bersumber dari kejahatan siber.

Hasil dari analisis normatif dapat diharapkan akan dapat memberikan suatu gambaran mengenai kesesuaian antara ketentuan peraturan positif di Indonesia dengan prinsip- prinsip hukum internasional dalam upaya pemberantasan TPPU berbasis cybercrime, serta mengidentifikasi kekosongan atau kelemahan hukum yang masih memerlukan pembaruan regulasi. Dengan demikian, penelitian ini tidak hanya berfungsi untuk menguraikan kondisi hukum yang berlaku, tetapi juga memberikan rekomendasi yuridis terhadap upaya pembaruan sistem hukum nasional agar lebih responsif terhadap dinamika kejahatan digital yang semakin kompleks.

HASIL DAN PEMBAHASAN

Dalam praktiknya Tindak pidana pencucian uang (TPPU) yang indifikasi berasal dari suatu kejahatan siber merupakan bentuk kejahatan lintas batas negara (transnational crime) yang menimbulkan tantangan besar bagi sistem hukum nasional dan internasional. Dalam praktiknya, kejahatan siber seperti phishing, ransomware, hacking, carding, maupun illegal online trading sering kali menghasilkan keuntungan ekonomi ilegal yang kemudian disamarkan melalui mekanisme pencucian uang agar tampak sah. Proses penyamaran tersebut biasanya dilakukan melalui serangkaian transaksi digital yang kompleks, melibatkan penggunaan mata uang kripto, rekening lintas negara, dan platform keuangan digital (fintech), sehingga sulit dilacak oleh otoritas penegak hukum.14

Kejahatan siber (cybercrime) menjadi sumber utama dana ilegal dalam banyak kasus TPPU modern. Data yang didapat dari United Nations Office on Drugs and Crime (UNODC) tahun 2023 sebagai pendukung bukti menunjukkan bahwa lebih dari 30% hasil kejahatan siber global berakhir dalam sistem pencucian uang digital. Dalam konteks Indonesia, PPATK mencatat peningkatan signifikan laporan transaksi keuangan mencurigakan (LTKM) yang berkaitan dengan aktivitas digital sejak 2020, sejalan dengan peningkatan penetrasi ekonomi digital.

Di dalam UU.NO. 8 Tahun 2010 telah menegaskan bahwa (TPPU) merupakan suatu tindak pidana sebagai lanjutan (follow up crime), dapat di simpulkan kejahatan ini muncul setelah adanya tindak pidana asal (predicate crime). Kejahatan siber yang menghasilkan keuntungan ekonomi ilegal dapat dikategorikan sebagai tindak pidana asal sebagaimana disebutkan dalam Pasal 2 ayat (1) huruf z UU (TPPU), bahwa tindak pidana kejahatan lainnya yang diancam dengan pidana penjara 4 (empat) tahun atau lebih.15 Dengan demikian, hasil kejahatan dari cyber fraud, data theft, atau ransomware dapat diproses melalui mekanisme hukum TPPU jika memenuhi unsur ,menyembunyikan atau menyamarkan asal-usul harta kekayaan yang diperoleh dari tindak pidana, sehingga kejahatan ini sangat penting dan urgensi untuk di kaji lebih dalam.

Penegakan hukum terhadap TPPU yang berasal dari kejahatan siber di Indonesia masih menghadapi berbagai hambatan, baik dalam aspek yuridis maupun teknis. Dilihat dari segi yuridis, di dalam sistem yang mengatur peraturan dan perundang-undangan yang berlaku belum sepenuhnya memuat/mengakomodasi sebagaima karakteristik kejahatan digital. UU TPPU dan UU ITE masih menitik beratkan pada transaksi konvensional dan belum mengatur secara detail penggunaan aset digital seperti cryptocurrency sebagai instrumen pencucian uang.

Dana yang didapat dari hasil cybercrime sering dialirkan melalui cryptocurrency, akun fiktif, atau lintas platform (e-commerce laundering). Modus baru seperti mixing service dan money mule networks sulit dilacak dengan mekanisme perbankan konvensional. Sertakan contoh kasus: misalnya Kasus Indra Kenz (binary option), Kasus DNA Pro, atau Kasus investasi kripto fiktif 2022–2024. Pembuktian “asal usul harta kekayaan” sulit karena digital trace tersebar lintas server luar negeri. Koordinasi antar lembaga (PPATK, OJK, Polri, Kemenkominfo) belum terintegrasi secara real-time. Instrumen hukum (UU No. 8/2010 dan UU ITE) belum sinkron dengan konsep virtual assets dan digital wallets. Perlunya revisi regulasi: menambahkan pengakuan eksplisit terhadap virtual currency dan digital assets dalam tindak pidana asal TPPU. Penguatan kapasitas forensik digital bagi penyidik

dan jaksa. Mendorong kerjasama internasional berbasis Mutual Legal Assistance (MLA) dan Joint Investigation Team (JIT). Integrasi sistem pelaporan otomatis (AI-driven suspicious transaction reports) di PPATK dan lembaga keuangan digital. Penanganan TPPU yang berasal dari kejahatan siber tidak cukup dengan paradigma hukum konvensional. Diperlukan transformasi dari legal formalism menuju digital legal realism, di mana hukum harus mampu mengikuti dinamika ruang siber yang tanpa batas. Sinkronisasi antara UU TPPU, UU ITE, dan regulasi aset digital merupakan keharusan agar sistem anti-pencucian uang nasional tidak menjadi "macan kertas" di tengah ekonomi digital yang kian kompleks. Adanya revisi UU 8/2010 untuk memasukkan kategori "aset virtual" sebagai instrumen pencucian uang. Penguatan cyber financial intelligence di PPATK dan kolaborasi lintas negara ASEAN. Pendidikan hukum digital di fakultas hukum agar calon penegak hukum memahami digital evidence chain of custody.

Selain itu, keterbatasan kapasitas lembaga penegak hukum dalam menelusuri aliran dana digital juga menjadi kendala. PPATK, Bareskrim Polri, dan OJK belum memiliki sistem terpadu untuk melakukan pelacakan real-time terhadap transaksi lintas platform digital.16 Hal ini berdampak pada rendahnya efektivitas pembuktian tindak pidana TPPU yang bersumber dari cybercrime, terutama karena banyak transaksi melibatkan decentralized exchanges (DEX) yang sulit diawasi oleh otoritas keuangan nasional.

Di sistem hukum Indonesia masih sangat tertinggal melihat pengaturan dengan negara lain yaitu seperti Amerika Serikat (U.S) dan Inggris yang lebih dulu mengatur secara eksplisit mekanisme penelusuran aset digital hasil kejahatan melalui Anti-Money Laundering Act dan Proceeds of Crime Act.17 Negara-negara tersebut juga telah memperluas kewenangan lembaga pengawas keuangan untuk bekerja sama dengan Virtual Asset Service Providers (VASPs) dalam rangka memblokir aset hasil kejahatan digital.

Secara normatif, sistem hukum Indonesia perlu menyesuaikan diri dengan perkembangan modus kejahatan siber dan praktik pencucian uang digital. Pembaruan ini dapat dilakukan melalui mekanisme yang terdapat UU. No. 8 Tahun 2010 agar mencakup secara eksplisit pengaturan mengenai aset digital, virtual currency, serta tanggung jawab penyedia layanan keuangan berbasis teknologi (fintech).18 Selain itu, kerja sama internasional juga harus diperkuat. Kejahatan siber dan TPPU bersifat lintas batas, sehingga penegakannya tidak dapat dilakukan hanya melalui instrumen hukum nasional. Ratifikasi penuh terhadap Budapest Convention on Cybercrime dan penerapan rekomendasi FATF terkait virtual asset monitoring menjadi langkah penting untuk meningkatkan efektivitas deteksi dan penegakan hukum terhadap TPPU dari kejahatan siber.

Efektivitas pemberantasan TPPU berbasis cybercrime tidak semata bergantung terhadap regulasi yang ada, namun juga terhadap kemampuan teknologi lembaga penegak hukum serta kesadaran publik terhadap risiko penyalahgunaan sistem keuangan digital. Pendekatan hukum yang adaptif, kolaboratif, dan berbasis teknologi merupakan prasyarat utama untuk menekan laju perkembangan kejahatan siber dan pencucian uang di era digital saat ini.19

KESIMPULAN

Berdasarkan hasil analisis atau studi (TPPU) yang mengungkap asal sumber dari kejahatan terhadap siber, dapat disimpulkan bahwasannya kejahatan seperti ini merupakan bentuk evolusi baru dari kriminalitas ekonomi yang memanfaatkan kemajuan teknologi informasi. Kejahatan siber menghasilkan keuntungan ekonomi ilegal yang kemudian disamarkan melalui mekanisme pencucian uang digital, seperti penggunaan cryptocurrency, rekening lintas wilayah negara, dan dalam sistem keuangan berbasis daring. Dari sisi hukum positif,di atur dalam UU.NO. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang sebenarnya telah mengatur secara umum mengenai delik pencucian uang. Namun, pengaturan tersebut belum sepenuhnya mengakomodasi bentuk-bentuk kejahatan baru yang menggunakan teknologi digital. Hal ini mengakibatkan lemahnya efektivitas terhadap penegakan hukum yang dilakukan terhadap TPPU berbasis kejahatan dalam siber di wilayah Indonesia, baik di dalam hal pelacakan aset, pembuktian, maupun kerja sama lintas negara.

Penegakan hukum TPPU dari kejahatan siber masih menghadapi kendala dalam aspek normatif dan teknis. Secara normatif, regulasi nasional belum secara eksplisit mencantumkan aset digital

sebagai objek pencucian uang. Sedangkan secara teknis, lembaga penegak hukum belum memiliki infrastruktur digital yang memadai untuk mendeteksi dan menelusuri transaksi digital yang bersifat anonim dan lintas yurisdiksi. Oleh karena itu, diperlukan pembaruan hukum dan peningkatan kapasitas lembaga penegak hukum agar mampu beradaptasi terhadap perkembangan kejahatan ekonomi digital yang semakin kompleks

DAFTAR PUSTAKA

Bambang Sadono. (2022). Cybercrime dalam Perspektif Hukum Pidana Indonesia.
Jakarta: Rajawali Pers.
Council of Europe. (2001). Budapest Convention on Cybercrime. Strasbourg: Council of Europe.
Eko Riyadi. (2022). "Keterkaitan Antara Kejahatan Siber dan Tindak Pidana
FATF. (2023). Guidance for a Risk-Based Approach to Virtual Assets and VASPs.
Paris: Financial Action Task Force
Financial Crimes Enforcement Network (FinCEN). (2022). Anti-Money Laundering Act of 2020 Implementation Report. Washington D.C.: FinCEN.
Hadjon, Philipus M. (2020). Argumentasi Hukum. Yogyakarta: Gadjah Mada University Press.
Ibrahim, Johnny. (2020). Teori dan Metodologi Penelitian Hukum Normatif. Malang: Bayumedia.
Moeljatno. (2021). Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.
Otoritas Jasa Keuangan (OJK). (2023). Laporan Stabilitas Sistem Keuangan Indonesia Triwulan IV 2023. Jakarta: OJK.
PPATK. (2023). Pedoman Penerapan Prinsip Know Your Customer dan Anti Money Laundering di Indonesia. Jakarta: Pusat Pelaporan dan Analisis Transaksi Keuangan.
PPATK. (2024). Laporan Tahunan Pusat Pelaporan dan Analisis Transaksi Keuangan Tahun 2023. Jakarta: PPATK.
Rizky, M., & Prasetyo, A. (2023). "Penegakan Hukum terhadap Pencucian Uang Berbasis Aset Digital di Indonesia." Jurnal Hukum dan Pembangunan, Vol. 52 No. 3.
Setiawan, Dwi. (2020). Kejahatan Siber dan Penegakan Hukumnya di Indonesia.
Jakarta: Sinar Grafika.
Sihombing, N. K. & Marbun, L. (2023). "Penerapan Digital Forensics dalam Pengungkapan Tindak Pidana Pencucian Uang di Indonesia." Jurnal Hukum Ius Quia Iustum, Vol. 30 No. 1.
Suharsil. (2021). Kriminalitas Digital dan Penegakan Hukum Pidana Ekonomi.
Bandung: Refika Aditama.
Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.
UNODC. (2023). Global Report on Cybercrime and Financial Crimes. Vienna: United Nations Office on Drugs and Crime.