

PENERAPAN TEKNOLOGI *QRIS* DALAM PERSPEKTIF UNDANG-UNDANG NOMOR 8 TAHUN 2010 TENTANG PENCEGAHAN DAN PEMBERANTASAN TINDAK PIDANA PENCUCIAN UANG¹

Oleh :

Elvian Janier Menanti²

elvianjenier@gmail.com

Jolly K. Pongoh³

Stevan O. Voges⁴

ABSTRAK

Penelitian ini bertujuan untuk menganalisis pengaturan hukum terhadap praktik pencucian uang melalui teknologi *QRIS* serta penerapan sanksi pidana terhadap pelaku dalam konteks penegakan hukum di Indonesia. Metode penelitian yang digunakan adalah metode yuridis normatif. Hasil penelitian menunjukkan bahwa pengaturan mengenai pencucian uang melalui *QRIS* telah memiliki dasar hukum dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang serta regulasi Bank Indonesia terkait sistem pembayaran digital. Meskipun demikian, belum terdapat pengaturan teknis yang secara khusus mengatur mitigasi risiko pencucian uang melalui *QRIS*, sehingga menimbulkan celah hukum dalam aspek verifikasi merchant, pengawasan transaksi mikro berulang, serta efektivitas penerapan KYC dan pelaporan transaksi mencurigakan oleh Penyelenggara Jasa Pembayaran (PJP/PJSP). Modus umum yang ditemukan meliputi penggunaan merchant fiktif, *structuring* melalui multi-akun, serta transaksi mikro berfrekuensi tinggi untuk menyamarkan asal-usul dana.

Dalam aspek penegakan hukum, aparat sebenarnya telah memiliki dasar untuk menjerat pelaku melalui Pasal 3, 4, dan 5 UU TPPU. Namun, hambatan teknis seperti keterbatasan deteksi transaksi real-time, minimnya koordinasi antar lembaga, dan kesulitan pembuktian digital menyebabkan proses penyidikan dan penuntutan belum optimal. Penelitian ini menegaskan perlunya pembaruan kebijakan, penguatan verifikasi merchant, serta pengembangan sistem deteksi otomatis agar inovasi *QRIS* tidak menjadi celah baru bagi kejahatan ekonomi digital.

Kata Kunci : *QRIS*; pencucian uang; UU TPPU; financial technology; merchant fiktif; transaksi digital.

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi finansial di Indonesia membawa kemudahan dalam sistem pembayaran, salah satunya melalui *Quick Response Code Indonesian Standard* (*QRIS*) yang diluncurkan oleh Bank Indonesia sejak 2019. *QRIS* memungkinkan masyarakat melakukan transaksi nontunai secara cepat, murah, dan praktis dengan hanya menggunakan satu kode QR yang terintegrasi untuk berbagai penyedia jasa pembayaran. Kehadiran *QRIS* tidak hanya meningkatkan efisiensi dan inklusi keuangan, tetapi juga mendukung upaya pemerintah dalam mendorong digitalisasi ekonomi.⁵ Untuk itu, sistem *QRIS* yang diluncurkan oleh Bank Indonesia ini juga mendukung berbagai platform pembayaran digital yang sudah mapan seperti e-wallet dan mobile banking, sehingga memudahkan pemerintah untuk melakukan pembayaran kepada penyedia barang dan jasa di seluruh Indonesia tanpa terhambat oleh perbedaan metode pembayaran. Data dari Bank Indonesia menunjukkan bahwa hingga akhir tahun 2023, penggunaan *QRIS* telah mencatat pertumbuhan transaksi yang eksponensial, dengan nilai transaksi yang mencapai ratusan triliun rupiah, melibatkan jutaan merchant baik skala besar, kecil, maupun mikro.⁶ Selain karena kemudahan dan kecepatan transaksinya, kerentanan *QRIS* terhadap penyalahgunaan juga dipengaruhi oleh aspek teknis dalam proses pendaftaran merchant. Tidak semua Penyelenggara Jasa Sistem Pembayaran (PJSP) menerapkan verifikasi lapangan secara mendalam terhadap calon merchant, terutama pada segmen usaha mikro dan kecil. Proses onboarding merchant yang cenderung cepat dan berbasis digital membuat celah verifikasi identitas maupun keabsahan usaha menjadi lebih longgar. Kondisi ini memungkinkan pelaku memanfaatkan data palsu, identitas pinjaman (*borrowed identity*), atau

⁵ Benny Eko Supriyanto, "Implementasi *QRIS* dalam Sistem Pembayaran Belanja Negara atas Bebas APBN" 25 Sept 2024, <https://djp.kemenkeu.go.id/kppn/watampone/id/data-publikasi/artikel/3752-implementasi-qr-is-dalam-sistem-pembayaran-belanja-negara-atas-beban-apbn.html>.

⁶ PBI No. 23/18/PBI/2021 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.

¹ Artikel Skripsi

² Mahasiswa Fakultas Hukum Unsrat NIM 220711010418

³ Fakultas Hukum Unsrat, Magister Ilmu Hukum

⁴ Fakultas Hukum Unsrat, Magister Ilmu Hukum

bahkan jasa joki pembuatan merchant QRIS untuk membuka akun yang tidak terdeteksi sebagai entitas berisiko tinggi. Hal ini menjadi titik rawan yang dapat digunakan untuk melakukan placement dana secara terselubung ke dalam sistem keuangan formal melalui transaksi fiktif.

Perkembangan teknologi pembayaran ini tidak terlepas dari risiko penyalahgunaan, termasuk untuk tindak pidana pencucian uang (*money laundering*) melalui modus-modus tertentu yang memanfaatkan sistem digital. Karakteristik QRIS yang bersifat instan, berbiaya rendah, serta memungkinkan transaksi berulang dalam jumlah kecil, membuka peluang bagi pelaku kejahatan untuk memanfaatkannya sebagai sarana penyamaran asal-usul dana hasil tindak pidana (*predicate crime*) seperti judi online, narkoba, penipuan, maupun korupsi. Beberapa modus operandi yang diduga kuat muncul dalam praktiknya antara lain: Structuring/ Smurfing melalui Multi – Akun, Penggunaan Merchant Fiktif, Penyamaran dalam Transaksi Cepat dan Massif.⁷ Pada tahun 2024, PPATK mengungkapkan adanya praktik pencucian uang yang memanfaatkan teknologi pembayaran digital QRIS melalui sebuah merchant fiktif di Kota Bandung bernama Kedai Kopi Lintang. Merchant tersebut tercatat memiliki transaksi harian hingga ratusan juta rupiah, namun setelah dilakukan pengecekan di lapangan, lokasi usaha ternyata tidak pernah beroperasi. Merchant QRIS palsu ini dibuat oleh pelaku dengan menggunakan identitas orang lain untuk menerima aliran dana dari jaringan judi online. Transaksi para pemain judi dialihkan melalui QRIS sehingga tampak seolah-olah sebagai pendapatan usaha. Selanjutnya, dana tersebut dipindahkan ke berbagai rekening, dipecah dalam jumlah kecil, dan digunakan untuk membeli aset seperti mobil dan emas guna menyamarkan asal-usulnya. Hasil analisis PPATK menemukan adanya pola transaksi tidak wajar, pemecahan transaksi (*smurfing*), serta pengiriman dana keluar negeri. Atas temuan tersebut, pelaku kemudian dijerat dengan ketentuan Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, karena terbukti menggunakan QRIS sebagai sarana placement dan layering uang hasil kejahatan. Dalam perspektif hukum, Indonesia telah memiliki

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU) telah mengatur kewajiban penerapan prinsip kehati-hatian, *Know Your Customer* (KYC), serta pelaporan transaksi mencurigakan. Di sisi lain, Bank Indonesia melalui Peraturan Anggota Dewan Gubernur Nomor 21/18/PADG/2019 tentang Implementasi Standar Nasional *Quick Response Code* untuk Pembayaran. Namun dalam praktiknya, muncul pertanyaan mengenai sejauh mana kerangka regulasi tersebut mampu menjangkau modus-modus baru pencucian uang yang memanfaatkan teknologi pembayaran digital. Persoalan ini menjadi perhatian karena sistem hukum nasional, khususnya UU TPPU, belum secara eksplisit mengatur tentang teknologi QRIS sebagai objek pencucian uang. Meskipun dalam Pasal 1 angka 13 UU TPPU disebutkan bahwa harta kekayaan adalah semua benda bergerak atau benda tidak bergerak, baik yang berwujud maupun yang tidak berwujud, yang diperoleh baik secara langsung maupun tidak langsung, sehingga belum ada regulasi teknis maupun petunjuk pelaksanaan yang secara khusus mengatur mekanisme pengawasan, pelaporan, dan penegakan hukum terhadap penggunaan QRIS. UU TPPU ini merepresentasikan harapan hukum masyarakat mengenai terciptanya sistem keuangan yang bersih dan transparan. Kasus-kasus yang ditemukan oleh PPATK maupun aparat penegak hukum menunjukkan bahwa teknologi pembayaran modern dapat dimanfaatkan sebagai bagian dari skema placement maupun layering dalam pencucian uang. Hal ini menegaskan perlunya evaluasi terhadap efektivitas pengaturan hukum yang berlaku, termasuk identifikasi celah pengawasan, kelemahan verifikasi merchant, serta tantangan dalam pemantauan transaksi digital secara real-time. Selain itu, penggunaan teknologi canggih oleh pelaku kejahatan siber menyulitkan aparat dalam mengidentifikasi dan membuktikan tindak pidana pencucian uang.⁸

Fenomena ini belum banyak dikaji secara mendalam dalam konteks hukum di Indonesia, terutama dari sisi pengaturan dalam UU TPPU terhadap modus operandi teknologi QRIS di era digital. Oleh karena itu, penelitian ini diharapkan dapat menjadi kontribusi awal dalam memberikan

⁷ PPATK. (2023). Laporan Tahunan 2022. Jakarta: Pusat Pelaporan dan Analisis Transaksi Keuangan, diakses 12/10/2025.

⁸ Cahyono, J., & Hidayati, A. (2020). *Peranan Kepolisian dalam Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang*. Jurnal Ilmiah Hukum: *InrichtingRecht*, 2(2).

kerangka yuridis untuk memahami dan menanggapi bentuk kejahatan baru dalam ruang digital. Maka dari itu, Penelitian ini kemudian menjadi kontribusi akademik dalam mendorong pembaruan hukum (*legal reform*) serta mengisi kekosongan normatif agar hukum Indonesia mampu menjawab tantangan kejahatan ekonomi digital berbasis QRIS.

B. Rumusan Masalah

1. Bagaimana pengaturan hukum terhadap praktik pencucian uang yang dilakukan melalui teknologi QRIS di Indonesia?
2. Bagaimana penerapan sanksi pidana terhadap pelaku pencucian uang melalui teknologi QRIS dalam proses penegakan hukumnya di Indonesia?

C. Metode Penelitian

Penelitian ini menggunakan pendekatan hukum Yuridis Normatif.

PEMBAHASAN

A. Pengaturan Hukum Terhadap Praktik Pencucian Uang Melalui Teknologi QRIS di Indonesia

Pengaturan mengenai pencucian uang melalui teknologi QRIS pada dasarnya berlandaskan pada kerangka hukum nasional yang mengatur pencegahan dan pemberantasan tindak pidana pencucian uang serta regulasi sistem pembayaran digital. Meskipun belum ada aturan yang secara khusus menyebut “pencucian uang melalui QRIS”, seluruh transaksi QRIS tetap tunduk pada ketentuan hukum yang telah ada, terutama Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU). Hal ini sejalan dengan prinsip *technology neutrality* dalam hukum pidana, yaitu bahwa suatu perbuatan pidana tidak dilihat dari sarana teknologinya, tetapi dari substansi perbuatan yang dilarang oleh undang-undang.⁹ Dengan demikian, penggunaan QRIS sebagai medium digital tidak mengubah karakter delik pencucian uang apabila unsur-unsur perbuatannya terpenuhi.

UU TPPU memberikan dasar hukum yang komprehensif bagi penegak hukum untuk menjerat pelaku yang menyamarkan asal-usul harta kekayaan melalui fasilitas QRIS. Pasal 3 dan Pasal 4 UU TPPU mengatur bahwa setiap orang yang menempatkan, mentransfer, membelanjakan, atau melakukan tindakan lain terhadap harta kekayaan hasil tindak pidana, dengan maksud menyembunyikan atau menyamarkan asal-usulnya, dapat dikenai sanksi sebagai pelaku tindak pidana pencucian uang. Rumusan norma tersebut bersifat luas dan teknologi-netral, sehingga dapat dikenakan pada berbagai modus digital seperti pembayaran melalui QR code, transaksi *e-wallet*, maupun sistem pembayaran terintegrasi lainnya. Selain itu, definisi “harta kekayaan” dalam Pasal 1 angka 13 UU TPPU mencakup seluruh aset, baik berwujud maupun tidak berwujud, termasuk dana elektronik dan saldo dompet digital yang digunakan dalam transaksi QRIS. Dengan demikian, dana yang mengalir melalui QRIS secara hukum dapat menjadi objek tindak pidana pencucian uang apabila memenuhi unsur perbuatan menurut UU TPPU.

UU TPPU juga mewajibkan penyedia jasa keuangan, termasuk penyelenggara jasa pembayaran (PJP/PJSP) non-bank yang mengoperasikan QRIS, untuk menerapkan prinsip mengenali pengguna jasa (*Customer Due Diligence*), melakukan verifikasi identitas merchant, memantau aktivitas transaksi, serta menyampaikan laporan transaksi keuangan mencurigakan (STR) kepada PPATK. Ketentuan ini ditegaskan dalam Pasal 17 dan Pasal 23 UU TPPU.¹⁰ Hal tersebut menunjukkan bahwa merchant QRIS diperlakukan sebagai “pengguna jasa” yang wajib diverifikasi identitasnya secara ketat. Kewenangan PPATK dalam menganalisis transaksi sebagaimana diatur Pasal 44 UU TPPU juga mencakup seluruh transaksi elektronik termasuk QRIS. Dalam beberapa laporan resmi tahun 2023-2024, PPATK mengonfirmasi meningkatnya pola *structuring* melalui merchant QRIS fiktif yang menerima transaksi mikro berulang bernilai kecil namun berfrekuensi tinggi.¹¹ Pengaturan sistem pembayaran yang dikeluarkan Bank Indonesia turut menjadi landasan penting dalam mencegah tindak pencucian uang melalui QRIS. Implementasi QRIS diatur dalam PADG BI No. 21/18/PADG/2019 yang mewajibkan penyelenggara QRIS menerapkan verifikasi identitas merchant, manajemen risiko,

⁹ Muladi & Dwidja Priyatno, *Pemberantasan Korupsi dan Pencucian Uang*, (Jakarta: Kencana, 2019), hlm. 221.

¹⁰ Ibid. Pasal 17 dan Pasal 23.

¹¹ PPATK, *Laporan Tahunan 2023–2024*, Jakarta: PPATK, 2024.

serta pemantauan transaksi yang tidak wajar. PBI No. 23/6/PBI/2021 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran menegaskan kewajiban PJP/PJSP untuk menerapkan prinsip mitigasi risiko, keamanan transaksi, dan kepatuhan terhadap ketentuan AML-CFT sesuai ketentuan PPATK.¹² Meskipun demikian, sejumlah kasus yang diungkap PPATK, termasuk kasus merchant fiktif di Bandung tahun 2024, menunjukkan bahwa proses verifikasi merchant *QRIS* masih rentan terhadap penyalahgunaan oleh pelaku kejahatan. Selain kerangka hukum nasional, Indonesia juga berkewajiban menerapkan standar internasional yang ditetapkan oleh *Financial Action Task Force* (FATF). Rekomendasi FATF, khususnya *Recommendation* tentang *Customer Due Diligence* dan *Recommendation* tentang *Suspicious Transaction Reporting*, memberikan standar global mengenai kewajiban verifikasi dan pelaporan transaksi mencurigakan bagi penyedia layanan pembayaran digital. *Recommendation* tentang *New Technologies* menggaris bawahi pentingnya negara melakukan *risk assessment* terhadap teknologi pembayaran baru, termasuk sistem pembayaran berbasis QR seperti *QRIS*, sebelum teknologi tersebut diadopsi secara luas.¹³ Kewajiban tersebut menuntut Bank Indonesia dan PPATK untuk memastikan adanya mitigasi risiko yang memadai dalam pemanfaatan layanan *QRIS*.

Menurut berbagai sumber dan doktrin hukum juga menegaskan bahwa perkembangan teknologi keuangan modern telah meningkatkan risiko pencucian uang melalui kanal digital. Muladi dan Priyatno menekankan bahwa esensi pencucian uang adalah upaya menyamarkan asal-usul harta kekayaan tanpa mempersoalkan sarana teknologi yang digunakan. Penelitian Saputra dan Silitonga (2022) menunjukkan bahwa proses registrasi merchant *QRIS* yang belum optimal dapat menjadi celah bagi pelaku untuk menggunakan identitas palsu.¹⁴ Sementara itu, laporan Europol tahun 2023 menyebutkan bahwa transaksi pembayaran berbasis QR termasuk dalam kategori *emerging threat* dalam pencucian uang karena sifatnya yang cepat, mudah, dan relatif sulit

dilacak pada merchant mikro.¹⁵ Dapat disimpulkan bahwa pengaturan terkait pencucian uang melalui *QRIS* telah memiliki dasar hukum yang kuat, baik dari sisi UU TPPU, regulasi Bank Indonesia, maupun standar internasional FATF. Namun implementasi teknis di lapangan masih menghadapi tantangan signifikan, terutama dalam aspek verifikasi merchant, deteksi transaksi mikro berulang, dan koordinasi antar lembaga. Oleh karena itu, penguatan regulasi dan peningkatan pengawasan menjadi diperlukan agar inovasi sistem pembayaran seperti *QRIS* tidak disalahgunakan sebagai medium pencucian uang.

Skema atau tahapan pencucian uang melalui *QRIS* pada dasarnya mengikuti tiga tahap klasik yang telah dikenal dalam rezim anti pencucian uang internasional, yaitu *placement*, *layering*, dan *integration*. Model tiga tahap ini diperkenalkan oleh *Financial Action Task Force* (FATF) sebagai kerangka global untuk memahami bagaimana pelaku kejahatan berupaya menyembunyikan asal-usul dana yang berasal dari aktivitas kriminal. Kerangka tersebut juga diadopsi dalam berbagai pedoman penegakan hukum, termasuk dalam doktrin dan literatur hukum Indonesia yang menekankan bahwa pencucian uang dilakukan melalui tahapan sistematis yang bertujuan memutus keterkaitan antara pelaku, tindak pidana asal, dan hasil kejahatannya. Dalam konteks layanan pembayaran digital, termasuk *QRIS*, ketiga tahapan ini tidak mengalami perubahan secara konsep, tetapi justru semakin mudah dilakukan karena karakteristik teknologi yang cepat, real-time, dan seringkali minim verifikasi identitas pada level merchant mikro. Ketiga tahapan tersebut, yaitu :

- 1) Tahap pertama adalah *placement*, yakni proses memasukkan dana ilegal ke dalam sistem keuangan formal. Pada fase ini, pelaku umumnya membuat merchant *QRIS* fiktif dengan memanfaatkan celah verifikasi identitas yang masih lemah dalam proses registrasi merchant. PPATK dalam Laporan Tahunan 2023 mencatat bahwa sejumlah penyelenggara *QRIS* hanya mensyaratkan unggahan KTP dan foto tempat usaha yang sangat mudah dimanipulasi, baik melalui rekayasa digital maupun penggunaan identitas pinjaman.¹⁶ Dana hasil kejahatan seperti judi online, penipuan, atau tindak pidana narkoba kemudian dialirkan melalui

¹² Peraturan Bank Indonesia No. 23/6/PBI/2021 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.

¹³ FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism*, Paris: FATF, 2021.

¹⁴ Saputra D. & Silitonga, "Analisis KYC pada Layanan QRIS", *Jurnal Lex Generalis*, Vol. 3 No. 2, 2022.

¹⁵ Europol, *Crypto Assets and Money Laundering: Emerging Threat Assessment*, 2023.

¹⁶ PPATK, *Laporan Tahunan 2023*, Jakarta: PPATK, 2024, hlm. 48–52.

transaksi *QRIS* yang tampak seperti pembayaran konsumen biasa. Melalui pola ini, pendapatan fiktif merchant menjadi sarana penempatan dana ilegal agar tercatat sebagai pemasukan usaha legal.

- 2) Tahap kedua adalah *layering*, yaitu fase yang paling penting dalam menyamarkan jejak asal-usul dana. FATF menjelaskan bahwa *layering* dilakukan melalui serangkaian transaksi keuangan yang kompleks, cepat, dan sulit dilacak, termasuk memanfaatkan teknologi pembayaran baru seperti *digital wallet*, *instant payment*, dan *QR code*.¹⁷ Pada tahap ini, merchant *QRIS* fiktif menerima ratusan transaksi kecil dalam satu hari yang nilainya berkisar antara Rp10.000 hingga Rp50.000 (*micro-structuring*). PPATK dalam Pedoman Transaksi Keuangan Mencurigakan menyebut bahwa transaksi kecil berfrekuensi tinggi merupakan pola umum pencucian uang melalui kanal pembayaran digital karena tidak memicu sistem deteksi nilai maksimal (*threshold alert*).¹⁸ Setelah dana masuk, pelaku memindahkan uang tersebut ke berbagai rekening bank digital, *e-wallet* lain, atau akun atas nama pihak ketiga dalam jumlah yang semakin kecil untuk mempersulit penelusuran. Dengan demikian, tahapan *layering* melalui *QRIS* menjadi sangat efektif karena kecepatan transaksi dan kelonggaran pengawasan pada merchant mikro.
- 3) Tahap ketiga adalah *integration*, yaitu fase ketika dana yang telah “tercuci” masuk kembali kepada pelaku dalam bentuk yang tampak sah secara legal. Pada tahap ini, dana yang telah berpindah melalui berbagai *e-wallet* atau bank digital digunakan untuk membeli aset bernilai seperti emas, kendaraan bermotor, gadget dengan nilai tinggi, atau bahkan investasi jangka panjang. Europol dalam laporan tahun 2023 menyatakan bahwa teknologi pembayaran cepat seperti QR code mempermudah pelaku mengintegrasikan dana hasil *layering* karena histori transaksi yang tercipta pada merchant fiktif tampak seperti pendapatan usaha asli. Dengan demikian, uang ilegal berhasil

disamarkan dan digunakan tanpa menimbulkan kecurigaan.

Untuk memperjelas bagaimana seluruh tahapan ini bekerja dalam praktik, dapat dikemukakan satu contoh kasus hipotesis berdasarkan pola yang ditemukan PPATK pada 2024. Seseorang membuka merchant *QRIS* fiktif bernama “Warung Kopi Abadi” dengan menggunakan identitas orang lain. Dalam satu hari, merchant tersebut menerima sekitar 300-400 transaksi *QRIS* bernilai kecil dari jaringan perjudian online dengan total pemasukan mencapai Rp15 juta. Ini merupakan tahap *placement*. Pada malam hari, pelaku memindahkan dana tersebut ke enam *e-wallet* berbeda, tiga bank digital, dan dua rekening atas nama individu lain dalam nominal Rp1-3 juta per transfer sebagai bagian dari *layering*. Setelah 2-4 minggu, dana yang telah tersebar tersebut digunakan untuk membeli emas dan motor sport menggunakan rekening yang tampak “bersih”, yaitu tahap *integration*. Pola tersebut secara sempurna memenuhi unsur Pasal 3 UU TPPU karena melibatkan tindakan menempatkan, memindahkan, dan membelanjakan harta kekayaan hasil kejahatan dengan maksud menyembunyikan asal-usul dana.¹⁹

Unsur objektif dalam tindak pidana pencucian uang merupakan unsur yang berkaitan dengan perbuatan nyata (*actus reus*) yang dapat diamati secara empiris dan dirumuskan secara tegas dalam ketentuan peraturan perundang-undangan.²⁰ Dalam konteks ini, Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU) mengatur secara rinci bentuk-bentuk perbuatan yang dikualifikasikan sebagai tindak pidana pencucian uang. Berdasarkan Pasal 3 UU TPPU, unsur objektif mencakup perbuatan menempatkan, mentransfer, membelanjakan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga, atau perbuatan lain atas harta kekayaan yang diketahui atau patut diduga berasal dari tindak pidana.²¹ Dalam praktik penggunaan teknologi *QRIS*, unsur ini terpenuhi apabila pelaku memasukkan dana hasil tindak pidana ke dalam sistem pembayaran melalui akun merchant *QRIS* dan selanjutnya melakukan

¹⁹ UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Pasal 3.

²⁰ Andi Hamzah, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2019, hlm. 85.

²¹ Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Pasal 3.

¹⁷ FATF, *Money Laundering and Terrorist Financing Risks of New Payment Methods*, Paris: FATF, 2020.

¹⁸ PPATK, *Pedoman Transaksi Keuangan Mencurigakan*, 2023, hlm. 17–19.

pemindahan atau penggunaan dana tersebut secara berulang. Selanjutnya, Pasal 4 UU TPPU mengatur unsur objektif berupa perbuatan menyembunyikan atau menyamarkan asal-usul, sumber, lokasi, peruntukan, pengalihan hak, atau kepemilikan harta kekayaan yang berasal dari tindak pidana. Unsur ini relevan dalam konteks QRIS ketika pelaku menciptakan konstruksi transaksi seolah-olah berasal dari kegiatan usaha yang sah, padahal secara faktual tidak terdapat aktivitas usaha yang nyata.²² Pasal 5 UU TPPU mengatur unsur objektif berupa perbuatan menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau penggunaan harta kekayaan yang diketahui atau patut diduga berasal dari tindak pidana. Ketentuan ini berkaitan dengan praktik penggunaan pihak perantara atau pemilik akun QRIS yang digunakan untuk menampung dan menyalurkan dana hasil pencucian uang.²³ Maka, penggunaan teknologi QRIS sebagai sarana transaksi tidak menghilangkan sifat melawan hukum dari perbuatan pencucian uang, karena fokus pengaturan UU TPPU terletak pada perbuatan terhadap harta kekayaan hasil tindak pidana, bukan pada media teknologi yang digunakan.

Unsur subjektif dalam tindak pidana pencucian uang berkaitan dengan sikap batin atau kesalahan (*mens rea*) dari pelaku. UU TPPU merumuskan unsur subjektif ini melalui frasa “mengetahui” atau “patut menduga” sebagaimana tercantum dalam Pasal 3, Pasal 4, dan Pasal 5 UU TPPU. Frasa “mengetahui” menunjukkan adanya kesengajaan, yaitu keadaan ketika pelaku secara sadar memahami bahwa harta kekayaan yang dikelolanya berasal dari tindak pidana. Dalam konteks penggunaan QRIS, unsur ini dapat dibuktikan apabila pelaku secara aktif mengendalikan alur transaksi, membentuk merchant fiktif, atau mengatur pola transaksi tertentu dengan tujuan menghindari pengawasan. Sementara itu, frasa “patut menduga” sebagaimana diatur dalam Pasal 3 dan Pasal 5 UU TPPU menunjukkan adanya bentuk kesalahan yang dapat dipertanggungjawabkan secara hukum. Unsur ini terpenuhi apabila berdasarkan kondisi objektif, pelaku seharusnya menyadari bahwa transaksi yang diterima atau dikelolanya tidak sesuai dengan profil usaha, kemampuan ekonomi, atau kewajaran transaksi pada umumnya.²⁴ Dalam praktik

pencucian uang melalui QRIS, unsur subjektif tidak selalu dibuktikan melalui pengakuan langsung dari pelaku, melainkan dapat disimpulkan dari rangkaian perbuatan, pola transaksi, serta keterkaitan antara pelaku dengan tindak pidana asal. Pendekatan ini sejalan dengan karakteristik pembuktian dalam tindak pidana ekonomi yang menekankan pada analisis pola dan logika peristiwa.

Pemenuhan unsur objektif sebagaimana diatur dalam Pasal 3, Pasal 4, dan Pasal 5 UU TPPU merupakan syarat utama untuk menentukan bahwa suatu perbuatan dapat dikualifikasikan sebagai tindak pidana pencucian uang. Namun demikian, pertanggungjawaban pidana hanya dapat dibebankan apabila unsur subjektif berupa kesengajaan atau patut menduga juga dapat dibuktikan secara hukum. Dalam konteks penegakan hukum terhadap tindak pidana pencucian uang melalui teknologi QRIS, analisis unsur objektif dan unsur subjektif menjadi penting untuk membedakan antara pelaku utama, pelaku yang turut serta, dan pihak yang tidak memiliki kesalahan pidana. Oleh karena itu, aparat penegak hukum dituntut untuk mengombinasikan pendekatan normatif dengan pemahaman terhadap karakteristik transaksi digital agar penerapan sanksi pidana dapat dilakukan secara tepat, proporsional, dan sesuai dengan asas kepastian hukum.

Berdasarkan uraian di atas, tampak bahwa *QRIS* tidak hanya menjadi inovasi sistem pembayaran, tetapi juga menawarkan peluang baru bagi pelaku kejahatan untuk melakukan pencucian uang dengan cara yang lebih cepat dan lebih sulit dideteksi. Karakteristik *QRIS* yang memungkinkan transaksi kecil dalam jumlah banyak, pendaftaran merchant yang mudah, dan minimnya verifikasi fisik menjadikan sistem ini rentan dimanfaatkan dalam ketiga tahapan pencucian uang. Oleh karena itu, diperlukan peningkatan pengawasan, pengetatan KYC, dan pengembangan algoritma deteksi transaksi mikro berulang agar potensi penyalahgunaan *QRIS* dapat diminimalisir.

Meskipun Indonesia telah memiliki kerangka hukum yang cukup komprehensif dalam upaya pencegahan dan pemberantasan tindak pidana pencucian uang melalui UU No. 8 Tahun 2010, Peraturan Bank Indonesia (PBI), serta standar internasional FATF, namun dalam praktiknya masih terdapat sejumlah kesenjangan regulasi (*regulatory gaps*) yang menyebabkan *QRIS* rentan digunakan sebagai sarana pencucian uang. Kesenjangan ini bersumber dari ketidaksiapan regulasi menghadapi kecepatan

²² *Ibid*, Pasal 4.

²³ *Ibid*, Pasal 5.

²⁴ Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Pasal 3 dan Pasal 5.

inovasi teknologi pembayaran digital, lemahnya aspek verifikasi merchant, sistem deteksi transaksi yang belum adaptif terhadap pola *micropayment laundering*, serta keterbatasan koordinasi antar lembaga. Kondisi ini secara umum menggambarkan adanya *regulatory lag*, yaitu keterlambatan hukum mengimbangi perkembangan teknologi.

Salah satu kesenjangan mendasar terletak pada ketiadaan regulasi teknis AML yang secara khusus mengatur *QRIS*. Hingga saat ini, tidak ada satu pun PBI atau peraturan PPATK yang secara rinci memberikan pedoman anti-pencucian uang untuk transaksi *QRIS* atau merchant *QRIS*. Regulasi AML yang berlaku masih bersifat umum bagi Penyelenggara Jasa Pembayaran (PJP/PJSP) tanpa mempertimbangkan karakteristik unik *QRIS* seperti tingginya volume transaksi kecil, *real-time settlement*, dan minimnya pembatasan geografis.²⁵ Padahal, FATF *Recommendation* mewajibkan negara untuk melakukan pengkajian risiko (*risk assessment*) sebelum mengadopsi teknologi pembayaran baru dan memastikan adanya mitigasi AML yang spesifik terhadap teknologi tersebut.²⁶ Ketiadaan pedoman AML khusus *QRIS* membuat penyelenggara jasa pembayaran beragam dalam menerapkan standar verifikasi dan pemantauan, sehingga menimbulkan celah sistemik yang dimanfaatkan pelaku.

Kesenjangan kedua muncul pada aspek verifikasi identitas merchant (*merchant onboarding*). PPATK dalam Laporan Tahunan 2023 menegaskan bahwa banyak merchant *QRIS* didaftarkan hanya dengan mengunggah foto KTP dan foto lokasi usaha, tanpa verifikasi fisik atau wawancara mendalam. Akibatnya, muncul fenomena merchant fiktif yang menggunakan identitas palsu, identitas pinjaman (*borrowed identity*), atau identitas yang dibeli melalui pasar gelap digital. Dalam kasus *QRIS* fiktif di Bandung (2024), PPATK menemukan bahwa merchant dapat dibuat secara massal dalam waktu singkat tanpa melalui proses verifikasi yang memadai, sehingga mempermudah aktivitas penempatan dana ilegal. Celah verifikasi ini menunjukkan bahwa standar KYC yang diatur dalam PBI No. 23/6/PBI/2021 dan ketentuan AML PPATK belum diimplementasikan secara efektif oleh sebagian PJSP. Kesenjangan lainnya adalah sistem deteksi transaksi mencurigakan yang belum mampu

mengidentifikasi pola *micropayment laundering*. Sistem AML tradisional dirancang untuk mendeteksi transaksi yang bernilai besar (*high-value alert*), sementara modus pencucian uang melalui *QRIS* menggunakan transaksi bernilai kecil namun berulang ratusan kali dalam sehari.²⁷ FATF telah memperingatkan bahwa sistem deteksi berbasis *threshold* tidak lagi memadai untuk menghadapi teknologi pembayaran instan, karena pelaku memecah dana menjadi unit-unit kecil untuk menghindari sistem pemantauan otomatis.²⁸ Keterbatasan ini juga dikonfirmasi oleh Bank Indonesia, yang mengakui bahwa sebagian besar PJSP belum memiliki algoritma deteksi transaksi abnormal untuk merchant mikro.²⁹ Hal ini semakin diperburuk oleh kecepatan transaksi *QRIS* yang real-time, sehingga membuat PJSP tidak memiliki waktu analisis yang cukup untuk memblokir transaksi mencurigakan. Selain itu, terdapat kesenjangan pada koordinasi antar lembaga, khususnya antara Bank Indonesia (BI), PPATK, OJK, dan aparat penegak hukum. Hingga kini, belum terdapat sistem pelaporan dan pertukaran data lintas lembaga secara real-time untuk transaksi *QRIS*. PPATK dalam Kajian Risiko Sistem Pembayaran 2024 menyebutkan bahwa keterlambatan pelaporan dan ketidaksinkronan data antar lembaga menyebabkan penanganan transaksi mencurigakan sering terlambat dan sulit ditindaklanjuti. Padahal, FATF mendorong pembentukan *inter-agency task force* yang bersifat responsif terhadap dinamika teknologi pembayaran digital. Ketiadaan mekanisme koordinasi berbasis real-time ini memberikan ruang bagi pelaku untuk mengalihkan dana ke berbagai akun sebelum pihak berwenang dapat melakukan tindakan pengamanan.

Kesenjangan berikutnya berkaitan dengan karakter teknologi *QRIS* itu sendiri, yang dirancang sangat inklusif, cepat, dan berbiaya rendah. Inklusivitas ini berdampak positif pada UMKM, tetapi sekaligus menciptakan risiko AML yang tinggi karena banyak merchant mikro tidak memiliki dokumentasi usaha formal atau alamat fisik yang jelas. Penelitian Saputra & Silitonga (2022) menyatakan bahwa merchant mikro merupakan kelompok dengan risiko AML tertinggi dalam *QRIS* karena lemahnya kemampuan PJSP melakukan verifikasi lapangan serta tingginya

²⁷ Europol, *Emerging Threats in Online Payments*, Den Haag: Europol, 2023

²⁸ FATF, *Money Laundering and Terrorist Financing Risks of New Payment Methods*, Paris: FATF, 2020

²⁹ Bank Indonesia, *Laporan Sistem Pembayaran 2023*, Jakarta: BI, 2024.

²⁵ PBI No. 23/6/PBI/2021 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran

²⁶ FATF, *International Standards on Combating Money Laundering and Terrorist Financing*, Paris: FATF, 2021 (*Recommendation 15*).hlm.5.

peluang penyalahgunaan identitas.³⁰ Dalam konteks ini, regulasi Indonesia belum menyediakan standar pengawasan yang berbeda antara merchant mikro berisiko rendah dan merchant mikro berisiko tinggi (*risk-based supervision*), sebagaimana dianjurkan FATF.

Secara keseluruhan, kesenjangan regulasi ini menunjukkan bahwa meskipun Indonesia memiliki fondasi hukum AML yang kuat, implementasi teknis terhadap pembayaran digital berbasis *QRIS* masih perlu diperkuat. *QRIS* sebagai teknologi baru menuntut pendekatan pengaturan yang berbeda dari sistem pembayaran konvensional. Tanpa penyesuaian regulasi yang bersifat spesifik, pelaku tindak pidana akan selalu menemukan ruang untuk memanfaatkan celah dalam sistem. Oleh karena itu, penutupan kesenjangan regulasi menjadi agenda krusial untuk memastikan bahwa inovasi sistem pembayaran nasional tidak berubah menjadi medium efektif bagi pencucian uang.

Penguatan regulasi dalam pencegahan pencucian uang melalui teknologi *QRIS* merupakan kebutuhan mendesak yang tidak dapat ditunda. Hal ini disebabkan oleh semakin meningkatnya penggunaan *QRIS* dalam transaksi keuangan nasional yang pada tahun 2024 mencapai lebih dari 3,8 miliar transaksi menurut data Bank Indonesia, jumlah yang jauh melebihi ekspektasi awal ketika sistem ini dikembangkan.³¹ Peningkatan tersebut membawa manfaat besar dalam inklusi keuangan, namun sekaligus membuka ruang yang signifikan bagi penyalahgunaan oleh pelaku tindak pidana. Oleh karena itu, regulasi dan kebijakan yang ada harus diperbaharui agar mampu mengimbangi dinamika teknologi pembayaran digital yang berkembang dengan sangat cepat.

Salah satu langkah yang paling krusial adalah penyusunan pedoman *anti-money laundering* (AML) yang secara spesifik mengatur *QRIS*. Selama ini, regulasi AML bagi penyelenggara jasa pembayaran masih bersifat umum dan tidak dirancang untuk menghadapi kompleksitas pola transaksi *QRIS* yang bersifat real-time, bernilai kecil, namun berfrekuensi sangat tinggi. PBI No. 23/6/PBI/2021 telah mengatur kewajiban penerapan prinsip kehati-hatian dan pengelolaan risiko, namun tidak memerinci standar AML khusus untuk transaksi

QRIS. Padahal, FATF melalui *Recommendation 15* secara tegas menyatakan bahwa negara harus menerapkan kebijakan AML-CFT yang secara spesifik menilai risiko teknologi baru (*new technologies*), dan tidak cukup hanya mengandalkan regulasi AML generik.³² Tanpa pedoman khusus, penyelenggara *QRIS* cenderung menerapkan standar AML yang berbeda-beda, sehingga risiko penyalahgunaan layanan oleh pelaku kejahatan menjadi lebih besar. Selain penyusunan pedoman AML khusus *QRIS*, langkah penting berikutnya adalah penguatan verifikasi merchant (*merchant onboarding*). Banyaknya kasus merchant *QRIS* fiktif, seperti laporan PPATK dalam kasus Bandung (2024), mengindikasikan bahwa proses pendaftaran merchant masih sangat longgar.³³ Menurut PPATK, sejumlah merchant *QRIS* dapat dibuat hanya dalam hitungan menit tanpa verifikasi lapangan, tanpa wawancara identitas, dan bahkan menggunakan identitas palsu yang dibeli di pasar gelap digital. Celah inilah yang dimanfaatkan pelaku tindak pidana untuk menciptakan merchant palsu dengan nama usaha yang terlihat meyakinkan, sehingga transaksi ilegal dapat berpura-pura sebagai transaksi usaha yang sah. Untuk mengatasi hal tersebut, Bank Indonesia perlu memperketat regulasi dengan mewajibkan penggunaan teknologi verifikasi biometrik, integrasi data Dukcapil secara penuh, serta validasi geolocation dan verifikasi fisik virtual sebagai syarat pendaftaran merchant. Langkah ini sejalan dengan rekomendasi Europol yang menyatakan bahwa merchant fiktif adalah titik paling lemah dalam ekosistem pembayaran cepat seperti QR code. Di samping verifikasi merchant, penguatan penting lainnya adalah penerapan sistem deteksi transaksi berbasis *Artificial Intelligence* (AI) dan machine learning. Sistem deteksi transaksi mencurigakan yang saat ini digunakan oleh sebagian besar penyelenggara *QRIS* masih mengandalkan parameter berbasis ambang batas (*threshold-based*), misalnya mendeteksi transaksi bernilai di atas jumlah tertentu. Namun, modus pencucian uang melalui *QRIS* justru dilakukan melalui transaksi mikro bernilai kecil, tetapi dilakukan ratusan hingga ribuan kali dalam satu hari (*micropayment laundering*), sehingga tidak terdeteksi oleh sistem tradisional.³⁴ Karena itu,

³² FATF, *International Standards on Combating Money Laundering and Terrorist Financing*, Paris: FATF, 2021 (*Recommendation 15*).

³³ PPATK, *Analisis Kasus Merchant QRIS Fiktif Bandung*, 2024.

³⁴ FATF, *Money Laundering and Terrorist Financing Risks of New Payment Methods*, Paris: FATF, 2020.

³⁰ Saputra D. & Silitonga, "Analisis KYC pada Layanan QRIS," *Jurnal Lex Generalis*, Vol. 3 No. 2, 2022. hlm.15.

³¹ Bank Indonesia, *Laporan Sistem Pembayaran 2023*, Jakarta: BI, 2024

diperlukan pembaruan regulasi yang mewajibkan penyelenggara *QRIS* menggunakan model deteksi berbasis perilaku (*behavioral risk scoring*), klasterisasi anomali, serta analisis pola transaksi real-time berbasis AI. Model ini telah menjadi standar di banyak negara yang menerapkan instant payment system karena terbukti lebih efektif dalam mendeteksi pola kejahatan finansial modern. Dalam Kajian Risiko Sistem Pembayaran 2024, PPATK bahkan merekomendasikan kewajiban penggunaan algoritma prediktif karena tingginya risiko penyalahgunaan *QRIS* dalam *layering* transaksi.³⁵ Penguatan regulasi harus dilakukan pada tingkat koordinasi antar lembaga. Saat ini, mekanisme pelaporan antara Bank Indonesia, PPATK, OJK, dan aparat penegak hukum belum terintegrasi secara real-time. PPATK dalam Laporan Tahunan 2023 menyebutkan bahwa keterlambatan pelaporan dan ketidaksinkronan data antar lembaga menjadi hambatan utama penanganan pencucian uang berbasis transaksi digital. Padahal, transaksi *QRIS* bersifat instan, sehingga aliran dana ilegal dapat berpindah platform dalam hitungan detik sebelum dapat dianalisis oleh sistem pelaporan tradisional. Penguatan koordinasi melalui pembentukan *National Digital Payment Task Force* perlu dilakukan untuk memastikan adanya pertukaran data secara langsung antara seluruh lembaga terkait. Model ini telah diterapkan di Singapura dan Korea Selatan dalam mengatasi kejahatan keuangan berbasis teknologi cepat, dan direkomendasikan oleh FATF dalam *Best Practices on New Payment Technologies*.³⁶

Penguatan regulasi berikutnya berkaitan dengan penerapan *risk-based supervision*. *QRIS* dirancang untuk menjangkau segmen UMKM dan pedagang mikro, namun kelompok ini juga merupakan segmen yang paling rentan terhadap risiko AML. Bank Indonesia perlu menyusun kategori risiko merchant secara lebih rinci, misalnya merchant mikro risiko rendah, merchant mikro risiko tinggi, merchant menengah risiko sedang, dan merchant korporasi. Merchant risiko tinggi harus dikenai kewajiban tambahan seperti pelaporan transaksi lebih sering, evaluasi berkala, atau peningkatan *enhanced due diligence*.³⁷ Menurut penelitian Saputra & Silitonga (2022), merchant mikro berisiko tinggi sering menjadi target pelaku pencucian uang karena lemahnya

kapasitas verifikasi PJSP.³⁸ Pendekatan berbasis risiko telah menjadi standar global, dan kegagalan menerapkannya akan menyebabkan sistem pembayaran rentan dimanfaatkan sebagai jalur pencucian uang.

Penguatan regulasi harus bersifat komprehensif, berlapis, dan adaptif terhadap perkembangan teknologi. Tidak cukup hanya memperketat peraturan formal; diperlukan pula peningkatan kapasitas penegak hukum, pelatihan PJSP dalam deteksi kejahatan digital, dan edukasi masyarakat agar tidak meminjamkan identitas untuk pendaftaran merchant *QRIS*. Tanpa pendekatan multi-dimensi, regulasi akan kembali tertinggal dari inovasi teknologi, sehingga *QRIS* tetap menjadi medium yang mudah dieksploitasi dalam praktik pencucian uang. Dengan melihat dinamika dan risiko yang telah muncul, penguatan regulasi dalam semua aspek ini merupakan syarat mutlak agar sistem pembayaran nasional yang modern tidak justru menjadi sarana kejahatan keuangan berteknologi tinggi.

B. Penerapan Sanksi Pidana Terhadap Pelaku Pencucian Uang Melalui Teknologi *QRIS* dalam Penegakan Hukum di Indonesia

Ketentuan sanksi pidana bagi pelaku pencucian uang melalui teknologi *QRIS* secara prinsip diatur dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU). Undang-undang ini menggunakan pendekatan teknologi-netral, artinya seluruh mekanisme pencucian uang, baik melalui rekening bank, perusahaan cangkang, maupun instrumen pembayaran digital seperti *e-wallet* dan *QRIS* tetap dapat dipidana tanpa memerlukan aturan baru yang secara khusus menyebutkan teknologi tersebut.³⁹ Pendekatan teknologi-netral ini memungkinkan penegak hukum menyesuaikan diri terhadap perkembangan modus kejahatan digital, termasuk pencucian uang melalui *QRIS* yang memanfaatkan kemudahan transaksi dan anonimitas relatif dalam proses pendaftaran merchant ataupun akun pengguna.

Pasal 3 UU TPPU menjadi ketentuan utama yang digunakan untuk menjerat pelaku pencucian

³⁵ PPATK, *Kajian Risiko Sistem Pembayaran 2024*, hlm. 44–59.

³⁶ FATF, *Best Practices on Combating Abuse of New Payment Technologies*, Paris: FATF, 2022.

³⁷ BI, *QRIS for UMKM Development Report*, 2023.

³⁸ Saputra D. & Silitonga, “Analisis KYC pada Layanan QRIS,” *Jurnal Lex Generalis*, Vol. 3 No. 2, 2022.hlm.22.

³⁹ Muladi & Dwidja Priyatno, *Pemberantasan Korupsi dan Pencucian Uang*, Jakarta: Kencana, 2019, hlm. 221.

uang melalui *QRIS*. Pasal ini memidana setiap orang yang dengan sengaja menempatkan, mentransfer, mengubah bentuk, membelanjakan, membayarkan, menitipkan, membawa ke luar negeri, atau melakukan perbuatan lain atas harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana.⁴⁰ Dengan demikian, pelaku pencucian uang digital yang memanfaatkan *QRIS* sebagai media *placement* (penempatan dana awal), *layering* (pemecahan dan pemindahan dana berulang), maupun *integration* (penggabungan dana kembali ke sistem keuangan formal) dapat dijerat karena ketiga tahapan tersebut termasuk dalam ruang lingkup tindakan aktif yang diatur oleh Pasal 3. Selain Pasal 3, Pasal 4 UU TPPU juga sangat relevan untuk menjerat aktor yang terlibat dalam proses penerimaan dana *layering* melalui *QRIS*, misalnya pemilik rekening penampung atau pemilik akun *e-wallet* yang menerima dana hasil kejahatan dan menyamakannya dalam bentuk transaksi *QRIS* yang seolah-olah merupakan pendapatan usaha. Pasal 4 memidana setiap orang yang menerima atau menguasai harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana, dengan ancaman pidana penjara paling lama 20 tahun dan denda paling banyak Rp5 miliar. Dalam praktik, pasal ini sering menjadi alat penting untuk menjerat bagian dari jaringan pencucian uang yang berperan menerima dana dalam proses *layering*. Di samping pelaku individu, Pasal 5 UU TPPU memperluas pertanggungjawaban pidana kepada korporasi, termasuk Penyelenggara Jasa Pembayaran (PJSP) dan entitas yang mengelola layanan transaksi *QRIS*.⁴¹ Korporasi dapat dipidana jika terbukti:

- memberikan kesempatan, sarana, atau fasilitas terjadinya pencucian uang;
- tidak menerapkan prinsip kehati-hatian; atau
- lalai melakukan pencegahan sebagaimana diwajibkan undang-undang.

Dalam konteks *QRIS*, ketentuan ini sangat relevan apabila terdapat PJSP yang lalai melakukan verifikasi identitas merchant (KYC), tidak melaporkan transaksi mencurigakan, atau ikut memfasilitasi transaksi *layering* melalui kelemahan sistem pengawasan internal. UU TPPU juga mengatur sanksi tambahan berupa perampasan aset, pembekuan rekening, pencabutan izin usaha, hingga pembubaran korporasi

sebagaimana diatur dalam Pasal 7 sampai Pasal 10. Ketentuan ini sangat penting dalam konteks kejahatan digital karena pelaku pencucian uang sering memindahkan dana dengan cepat sehingga sanksi administratif dan tindakan pemblokiran menjadi instrumen awal yang krusial untuk mencegah penghilangan aset.⁴² Lebih jauh lagi, Pasal 77 hingga Pasal 79 mengatur tentang pembuktian terbalik, yaitu mekanisme di mana terdakwa wajib membuktikan bahwa harta kekayaan yang dimilikinya bukan berasal dari tindak pidana.⁴³ Mekanisme ini merupakan inovasi penting dalam penanganan pencucian uang digital, karena mempersingkat proses pembuktian dan memaksa pelaku menjelaskan asal-usul dana yang terdeteksi mengalir melalui *QRIS*. Jika dicermati, struktur ketentuan pidana dalam UU TPPU menunjukkan bahwa undang-undang ini memang dirancang untuk menghadapi berbagai model pencucian uang, termasuk model-model yang berkembang akibat digitalisasi sistem pembayaran seperti *QRIS*. Keberadaan ancaman pidana yang berat, mekanisme pembuktian terbalik, pertanggungjawaban korporasi, serta tindakan administratif menunjukkan bahwa UU TPPU memberikan kerangka hukum yang kuat untuk menindak pelaku pencucian uang berbasis teknologi. Namun, efektivitasnya tetap sangat bergantung pada kemampuan aparat dalam menelusuri aliran dana digital dan kecermatan penyelenggara *QRIS* dalam menerapkan kewajiban *customer due diligence*.

Mekanisme penegakan hukum dalam tindak pidana pencucian uang yang dilakukan melalui transaksi *QRIS* melibatkan rangkaian proses yang kompleks dan lintas lembaga, mulai dari deteksi awal oleh Penyelenggara Jasa Pembayaran (PJSP), pelaporan kepada Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), penyidikan oleh Kepolisian atau Kejaksaan, hingga proses penuntutan dan pemeriksaan di pengadilan. Sistem yang berlapis ini merupakan implementasi dari model *Anti-money laundering* (AML) nasional sebagaimana dirumuskan dalam UU No. 8 Tahun 2010, di mana setiap lembaga memiliki peran khusus untuk memastikan bahwa aliran dana ilegal dapat ditangani sejak tahap awal.⁴⁴ Dalam konteks *QRIS*, proses penegakan hukum menjadi lebih menantang karena sifat transaksi yang *real-time*, jumlah transaksi yang sangat besar, dan

⁴² *Ibid.* Pasal 7–10.

⁴³ *Ibid.* Pasal 77–79.

⁴⁴ Muladi dan Dwidja Priyatno, *Pemberantasan Korupsi dan Pencucian Uang*, Jakarta: Kencana, 2019, hlm. 221.

⁴⁰ UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Pasal 3.

⁴¹ *Ibid.* Pasal 5.

kemudahan pelaku untuk menciptakan merchant fiktif atau menggunakan identitas palsu dalam proses *onboarding*.

Tahap pertama penegakan hukum dimulai dari deteksi dini oleh PJSP, yang diwajibkan untuk menerapkan *customer due diligence* (CDD) dan *ongoing monitoring* sebagaimana diatur dalam Pasal 17 UU TPPU dan dipertegas dalam PBI No. 23/6/PBI/2021. Dalam transaksi *QRIS*, indikasi awal yang sering ditemukan antara lain pola transaksi yang tidak sesuai profil merchant, frekuensi transaksi mikro berulang yang sangat tinggi, penggunaan *QRIS* di lokasi yang tidak konsisten, atau lonjakan pendapatan yang tidak sejalan dengan kegiatan usaha. PJSP yang menemukan pola mencurigakan wajib menyampaikan Laporan Transaksi Keuangan Mencurigakan (LTKM) kepada PPATK dalam waktu paling lama 3 hari kerja sejak terdeteksinya indikasi tersebut.⁴⁵ Pada tahap ini, kapasitas analisis internal PJSP sangat menentukan efektivitas deteksi, karena transaksi *QRIS* seringkali tidak bernilai besar namun berjumlah ribuan, sehingga membutuhkan sistem analitik berbasis algoritma dan *behavioral analysis* untuk mengidentifikasi anomali.

Tahap berikutnya adalah analisis oleh PPATK, yang menjadi pusat dalam mekanisme deteksi tindak pidana pencucian uang. PPATK melakukan serangkaian analisis strategis dan operasional menggunakan metode *link analysis*, *network mapping*, *pattern recognition*, hingga *device tracing* untuk memetakan hubungan antara merchant *QRIS*, pemilik rekening penerima, dan jaringan kejahatan yang lebih luas. Dalam banyak kasus, PPATK menemukan bahwa transaksi *QRIS* menjadi medium tahap *placement* dengan cara menerima dana dalam jumlah kecil namun berulang, lalu dipindahkan ke berbagai akun *e-wallet* atau rekening bank. Pola ini dapat terlihat ketika merchant *QRIS* menerima ribuan pembayaran dalam waktu singkat tanpa profil usaha yang jelas. Selain itu, PPATK memiliki kewenangan untuk melakukan pemblokiran sementara atas rekening atau dompet digital selama 5 hari kerja sebagaimana diatur dalam Pasal 44 UU TPPU apabila terdapat dugaan kuat bahwa transaksi berkaitan dengan tindak pidana pencucian uang.⁴⁶ Pemblokiran ini penting untuk mencegah pelaku memindahkan dana ke luar sistem keuangan sebelum aparat penegak hukum dapat menindaklanjutinya. Setelah analisis selesai,

PPATK menerbitkan hasil analisis yang kemudian disampaikan kepada Kepolisian atau Kejaksaan untuk proses penyidikan. Tahap penyidikan merupakan fase kritis karena pada tahap ini penyidik harus membuktikan hubungan antara transaksi *QRIS* dengan tindak pidana asal (*predicate crime*). Banyak kasus menunjukkan bahwa pelaku menggunakan merchant *QRIS* fiktif atau disamarkan untuk menerima hasil kejahatan seperti perjudian online, narkoba, atau penipuan daring. Pada tahap ini, penyidik memerlukan teknik digital forensics untuk melacak aliran dana, termasuk menelusuri alamat IP, perangkat yang digunakan (*device fingerprinting*), lokasi transaksi (*geo-tracking*), serta identifikasi nomor telepon dan SIM card yang terhubung ke akun *QRIS*. Penyidikan kejahatan berbasis *QRIS* menjadi lebih kompleks karena seringkali pelaku menggunakan perangkat burner phone, VPN, atau identitas palsu, sehingga penyidik harus bekerja sama dengan operator seluler, Dukcapil, dan PJSP.⁴⁷ Jika penyidik meyakini bahwa unsur-unsur Pasal 3, 4, atau 5 UU TPPU terpenuhi, berkas perkara akan diserahkan kepada penuntut umum untuk tahap penuntutan. Pada tahap ini, jaksa harus menjelaskan secara sistematis pola transaksi pencucian uang melalui *QRIS*, termasuk aliran dana, peran masing-masing pelaku, dan hubungan antara transaksi dengan tindak pidana asal. Pembuktian dalam kasus *QRIS* umumnya mengandalkan dokumen transaksi elektronik, hasil analisis PPATK, saksi ahli forensik digital, serta bukti elektronik lainnya sesuai UU ITE dan KUHP.⁴⁸ Tantangan utama pada tahap ini adalah meyakinkan hakim bahwa ribuan transaksi kecil melalui *QRIS* merupakan bagian dari satu skema pencucian uang terstruktur, bukan transaksi dagang biasa.

Tahap terakhir adalah pemeriksaan di persidangan, di mana hakim menilai terpenuhinya unsur-unsur tindak pidana pencucian uang. Dalam beberapa laporan kasus, hakim cenderung mempertimbangkan pola transaksi dan ketidakwajaran aktivitas merchant sebagai bukti kuat adanya niat (*mens rea*) untuk menyamarkan asal-usul dana. Dalam kasus *QRIS* di Bandung, hakim menyatakan bahwa penerimaan ribuan transaksi *QRIS* tanpa usaha nyata merupakan indikator kuat terjadinya tindak pidana pencucian uang, meskipun transaksi bersifat mikro. Putusan seperti ini menunjukkan bahwa *QRIS* telah diakui

⁴⁵ UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan TPPU, Pasal 23.

⁴⁶ UU No. 8 Tahun 2010, Pasal 44 ayat (1).

⁴⁷ PPATK, *Pedoman Digital Forensics Keuangan*, 2024.

⁴⁸ UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 5–6.

sebagai sarana yang dapat digunakan dalam proses pencucian uang, sehingga mekanisme pembuktiannya dapat disamakan dengan pembuktian tindak pidana pencucian uang berbasis rekening bank atau *e-wallet* lainnya. Melalui rangkaian proses tersebut, terlihat bahwa mekanisme penegakan hukum dalam pencucian uang berbasis *QRIS* sangat bergantung pada kemampuan deteksi awal oleh PJSP, kecepatan analisis PPATK, efektivitas penyidikan digital, dan ketepatan pembuktian di pengadilan. Tantangan terbesar berasal dari sifat transaksi *QRIS* yang *real-time* dan melibatkan banyak akun, sehingga membutuhkan adaptasi teknologi dan peningkatan kapasitas penegakan hukum secara terus-menerus. Dengan demikian, meskipun kerangka hukum telah tersedia, efektivitas penegakan hukum akan sangat dipengaruhi oleh kesiapan institusi dalam menghadapi perkembangan teknologi keuangan digital. Analisis yuridis terhadap penerapan sanksi pidana dalam kasus pencucian uang yang memanfaatkan teknologi *QRIS* menunjukkan bahwa instrumen hukum yang telah tersedia pada prinsipnya cukup memadai untuk menjerat pelaku, namun implementasinya menghadapi tantangan yang bersifat teknis dan faktual. Kasus-kasus awal yang diidentifikasi oleh PPATK pada tahun 2023 dan 2024 menunjukkan pola yang relatif seragam: pelaku memanfaatkan kelemahan proses verifikasi merchant (*merchant onboarding*), tingginya volume transaksi kecil (*micropayments*), dan kecepatan sistem settlement *QRIS* untuk menyamarkan hasil tindak pidana seperti perjudian online, penipuan digital, dan narkoba.⁴⁹ Pola inilah yang kemudian menjadi dasar utama dalam analisis yuridis untuk membuktikan unsur-unsur tindak pidana pencucian uang sebagaimana diatur dalam Pasal 3, Pasal 4, dan Pasal 5 UU TPPU. Kasus *QRIS* Bandung 2024, misalnya, menunjukkan bagaimana merchant *QRIS* dengan identitas palsu dapat menerima lebih dari 80.000 transaksi dalam beberapa minggu, di mana setiap transaksi memiliki nilai kecil antara Rp5.000 hingga Rp20.000.⁵⁰ PPATK menemukan bahwa transaksi tersebut tidak berasal dari aktivitas bisnis yang nyata, tetapi merupakan transaksi yang sengaja dilakukan oleh jaringan pelaku untuk memecah dana hasil perjudian online sebelum dipindahkan ke berbagai rekening atas nama orang lain. Fakta ini secara jelas memenuhi unsur perbuatan “menempatkan” dan “mentransfer” dana

sebagaimana unsur *actus reus* dalam Pasal 3 UU TPPU.⁵¹

Analisis PPATK menunjukkan adanya struktur *layering* berlapis, di mana dana yang diterima merchant *QRIS* fiktif dipindahkan ke puluhan rekening perantara dalam pecahan nominal kecil yang sengaja disebar untuk menghindari deteksi sistem anti-fraud perbankan.⁵² Dari perspektif yuridis, tindakan ini merupakan upaya untuk “menyamarkan asal-usul harta kekayaan”, sebuah unsur penting yang harus dibuktikan dalam tindak pidana pencucian uang. Penjelasan Pasal 3 UU TPPU menyebutkan bahwa perbuatan *layering* melalui pemisahan dana ke berbagai rekening merupakan bentuk pencucian uang yang secara eksplisit masuk dalam ruang lingkup ketentuan pidana. Oleh sebab itu, meskipun pelaku memanfaatkan teknologi *QRIS* dan bukan mekanisme transfer bank konvensional, unsur perbuatan tetap terpenuhi karena undang-undang bersifat teknologi-netral. Analisis yuridis juga menggarisbawahi bahwa pelaku dalam kasus *QRIS* fiktif tersebut memiliki unsur *mens rea*, yaitu niat untuk menyembunyikan atau menyamarkan asal-usul dana. Hal ini terlihat dari penggunaan identitas palsu pada saat pendaftaran merchant *QRIS*, manipulasi alamat usaha, hingga penggunaan perangkat elektronik tidak terdaftar (*burner devices*) untuk menghindari pelacakan digital.⁵³ Unsur kesengajaan ini memperkuat pemenuhan elemen subjektif dalam tindak pidana pencucian uang, sehingga pelaku dapat dijerat dengan ancaman pidana maksimal berdasarkan Pasal 3. Selain aktor utama, pelaku lain yang menerima dana dari merchant fiktif juga dapat dijerat dengan Pasal 4 UU TPPU sebagai pihak yang “menerima atau menguasai harta kekayaan yang diketahuinya atau patut diduganya berasal dari hasil tindak pidana”.⁵⁴ Dalam beberapa kasus yang dianalisis PPATK, penerima dana *layering* mengklaim bahwa transaksi tersebut merupakan “komisi”, “gaji freelance”, atau “pendapatan online”, namun pembuktian di pengadilan bergantung pada analisis struktur aliran dana. Apabila ditemukan pola berulang yang tidak konsisten dengan profil penerima, maka unsur “patut diduga” terpenuhi, dan yang bersangkutan dapat dijatuhi sanksi pidana.

⁵¹ UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan TPPU, Pasal 3.

⁵² PPATK, *Laporan Analisis 2023–2024*, hlm. 56–59.

⁵³ PPATK, *Pedoman Digital Forensics Keuangan*, 2024.

⁵⁴ UU No. 8 Tahun 2010, Pasal 4.

⁴⁹ PPATK, *Laporan Tahunan 2024*, Jakarta: PPATK, 2024, hlm. 72–75.

⁵⁰ PPATK, *Analisis Kasus Merchant QRIS Fiktif Bandung*, 2024.

Penerapan sanksi pidana terhadap korporasi, terutama Penyelenggara Jasa Pembayaran (PJSP), juga tidak luput dari analisis yuridis. Apabila terbukti bahwa PJSP lalai melakukan verifikasi merchant atau tidak menyampaikan laporan transaksi mencurigakan kepada PPATK, maka PJSP dapat dijerat melalui Pasal 5 UU TPPU, di mana korporasi dapat dikenakan denda, perampasan aset, atau bahkan pencabutan izin. Walaupun belum ada kasus resmi yang sampai pada tahap pemidanaan korporasi dalam konteks *QRIS*, PPATK dalam laporan risikonya tahun 2024 telah mengingatkan bahwa kelemahan verifikasi merchant oleh PJSP merupakan salah satu pintu masuk pencucian uang digital. Dengan demikian, penerapan tanggung jawab pidana korporasi bukan hanya dimungkinkan, tetapi juga sudah mulai dipertimbangkan dalam kebijakan penegakan hukum.

Tantangan terbesar bukan pada norma hukum, tetapi pada teknis pembuktian, yaitu bagaimana aparat penegak hukum mampu membuktikan keterkaitan antara transaksi *QRIS* dengan tindak pidana asal. Dalam proses ini, bukti elektronik, rekam jejak digital, dan analisis PPATK memegang peran sentral.⁵⁵ Dengan semakin meningkatnya kompleksitas skema pencucian uang digital, analisis yuridis menjadi semakin menekankan pentingnya kolaborasi antara penyidik, ahli forensik digital, dan PPATK untuk memastikan bahwa bukti yang diajukan di persidangan memenuhi standar pembuktian. Dengan demikian, analisis yuridis menunjukkan bahwa penerapan sanksi pidana dalam kasus pencucian uang melalui *QRIS* bukan hanya bergantung pada ketentuan normatif dalam UU TPPU, tetapi juga pada efektivitas analisis struktur transaksi, kemampuan digital forensik, dan kolaborasi antar lembaga. Penerapan hukum akan semakin efektif apabila kasus-kasus yang ada digunakan sebagai yurisprudensi untuk memperkuat pendekatan pembuktian pada kasus serupa di masa mendatang.

Efektivitas sanksi pidana dalam UU No. 8 Tahun 2010 terhadap pelaku pencucian uang melalui *QRIS* pada prinsipnya sangat bergantung pada kemampuan sistem hukum untuk mengidentifikasi, membuktikan, dan menindak secara komprehensif seluruh tahapan pencucian uang yang dilakukan melalui instrumen pembayaran digital. Walaupun ancaman pidana bagi pelaku sangat berat yakni hingga 20 tahun penjara dan denda miliaran rupiah efektivitas

sanksi tersebut bergantung pada sejauh mana aparat penegak hukum mampu mengungkap modus operandi yang kompleks, cepat, serta sangat terfragmentasi dalam jaringan transaksi *QRIS*.⁵⁶ Dengan karakteristik transaksi *QRIS* yang real-time, berbasis instant settlement, dan didominasi oleh transaksi mikro berfrekuensi tinggi, proses penegakan hukum menghadapi tantangan teknis yang jauh lebih sulit dibandingkan pencucian uang melalui perbankan konvensional. Salah satu tantangan terbesar adalah pembuktian hubungan antara transaksi *QRIS* dan tindak pidana asal (*predicate crime*). UU TPPU menganut pendekatan *follow the money*, yang mengharuskan penyidik membuktikan bahwa dana yang mengalir merupakan hasil dari tindak pidana tertentu seperti perjudian online, narkoba, korupsi, atau penipuan. Namun, pola transaksi *QRIS* yang melibatkan ribuan transaksi kecil yang dilakukan secara otomatis menggunakan bot, APK modifikasi, atau jaringan akun yang terkoordinasi menyebabkan identifikasi hubungan antara dana *QRIS* dan kejahatan asal membutuhkan kemampuan analitik yang sangat tinggi. PPATK mencatat bahwa skema *layering* melalui *QRIS* sering kali melibatkan pergerakan dana antar akun *e-wallet* tanpa pola yang mudah dikenali, sehingga memerlukan teknologi *advanced analytics* untuk menganalisis pola tersebut.⁵⁷ Tanpa teknologi ini, banyak indikasi pencucian uang gagal ditindak lanjuti karena tidak terpenuhinya pembuktian hukum. Tantangan berikutnya adalah kecepatan pelaku dalam mengalihkan dana, yang jauh melebihi kecepatan respons lembaga penegak hukum. *QRIS* memungkinkan dana berpindah dalam hitungan detik, sedangkan proses pelaporan STR, analisis transaksi, dan permintaan pemblokiran rekening membutuhkan waktu jam hingga hari. Akibatnya, dana hasil kejahatan seringkali telah dipindahkan atau ditarik sebelum sistem deteksi mampu mengidentifikasinya.⁵⁸ Meski PPATK berwenang melakukan pemblokiran sementara berdasarkan Pasal 44 UU TPPU, kewenangan ini terbatas pada 5 hari kerja, sehingga pelaku dapat kembali mengakses dana apabila penyidik belum mengeluarkan penetapan lanjutan. Ketidakseimbangan kecepatan ini menjadi salah satu faktor utama yang mengurangi efektivitas penegakan hukum.

⁵⁶ Muladi dan Dwidja Priyatno, *Pemberantasan Korupsi dan Pencucian Uang*, Jakarta: Kencana, 2019, hlm. 229.

⁵⁷ PPATK, *Laporan Analisis 2023–2024*, hlm. 56–60.

⁵⁸ Bank Indonesia, *Laporan Sistem Pembayaran 2024*, hlm. 145–150.

⁵⁵ Bank Indonesia, *Laporan Sistem Pembayaran 2024*, hlm. 142–150.

Tindak pidana pencucian uang melalui *QRIS* sering kali menggunakan identitas palsu, identitas “pinjaman” (*borrowed identity*), atau identitas hasil pembelian dari pasar gelap digital (*dark web identity kits*). Hal ini menyebabkan proses verifikasi dan pemanggilan tersangka menjadi jauh lebih sulit. PPATK dalam Kajian Risiko Sistem Pembayaran 2024 menemukan bahwa sekitar 42% merchant *QRIS* berisiko tinggi tidak memiliki kecocokan data lokasi atau identitas dengan data kependudukan dari Dukcapil.⁵⁹ Kondisi ini memperlihatkan adanya kesenjangan serius dalam proses KYC oleh penyelenggara *QRIS*. Tanpa verifikasi yang kuat, upaya penegakan hukum berada dalam posisi yang lemah karena identitas pelaku mudah digantikan atau dihapus. Dari aspek teknis, keterbatasan kemampuan *digital forensics* aparat penegak hukum menjadi tantangan yang signifikan. Penyidik harus mampu menelusuri jejak digital yang bersifat sangat dinamis, seperti alamat IP yang berubah-ubah, penggunaan VPN, perangkat bergerak (*mobile devices*) yang tidak terdaftar, hingga penggunaan aplikasi modifikasi yang tidak menyimpan log dengan baik.⁶⁰ Selain itu, tidak semua aparat penegak hukum memiliki keahlian khusus dalam membaca pola transaksi numerik dalam jumlah besar. Padahal, pencucian uang melalui *QRIS* sering kali dilakukan melalui ribuan titik data transaksi, sehingga penyidik harus memiliki kemampuan data analytics dan pattern detection. Tanpa keahlian ini, dakwaan yang disusun berisiko lemah karena tidak dapat menunjukkan konstruksi aliran dana secara runtut.

Tantangan berikutnya adalah fragmentasi kewenangan antar lembaga, di mana Bank Indonesia berwenang mengawasi penyelenggara *QRIS*, PPATK berwenang menganalisis data transaksi mencurigakan, sementara penyidikan dilakukan oleh Kepolisian atau Kejaksaan. Ketidakselarasan sistem pelaporan dan perbedaan standar data sering kali menyebabkan keterlambatan atau inkonsistensi dalam proses penegakan hukum. Misalnya, laporan Bank Indonesia dalam Laporan Sistem Pembayaran 2024 mencatat bahwa sebagian besar PJSP belum memiliki integrasi langsung ke sistem pelaporan PPATK secara real-time, sehingga menyebabkan proses deteksi dan respons terhadap transaksi mencurigakan menjadi lambat. Hal ini bertentangan dengan rekomendasi FATF yang menuntut negara untuk membangun real-time data

exchange system antar lembaga AML. Dari perspektif sanksi, meskipun ancaman pidana dalam UU TPPU cukup berat, efektivitasnya menurun apabila pelaku tidak dapat ditangkap atau dana tidak dapat ditemukan kembali. PPATK mencatat bahwa dalam sebagian kasus pencucian uang digital, total dana yang dapat disita atau dibekukan hanya berkisar antara 20-30% dari total aliran dana, sisanya telah dipindahkan ke rekening luar negeri, platform aset digital, atau ditarik tunai melalui berbagai metode.⁶¹ Kondisi ini menunjukkan bahwa sanksi pidana tidak dapat berdiri sendiri tanpa mekanisme pengawasan yang cepat, teknologi pemantauan yang canggih, dan koordinasi antar lembaga yang optimal. Akhirnya, tantangan terbesar terletak pada kurangnya literasi dan kesadaran pelaku usaha dan masyarakat, terutama pengguna *QRIS* dan merchant mikro. Banyak merchant bersedia meminjamkan identitas atau akun *QRIS* karena ketidaktahuan mengenai risiko hukum. Dalam laporan PPATK, sekitar 29% akun merchant berisiko tinggi dimiliki oleh individu yang “tidak mengetahui bahwa akun mereka digunakan untuk menampung dana hasil kejahatan”. Kondisi ini memungkinkan pelaku pencucian uang menggunakan masyarakat awam sebagai perantara (*money mule*), sehingga semakin memperumit proses penegakan hukum. Tanpa penguatan tersebut, ancaman pidana yang berat pun tidak akan memberikan efek jera yang optimal karena pelaku tetap dapat mengandalkan kecepatan teknologi dan anonimitas digital untuk mengaburkan jejak kejahatan.⁶²

PENUTUP

A. Kesimpulan

1. Secara normatif, Indonesia telah memiliki landasan hukum yang memadai untuk mengatasi praktik pencucian uang melalui *QRIS*, terutama melalui UU TPPU yang bersifat *technology-neutral* dan dapat menjangkau berbagai bentuk teknologi pembayaran digital. Didukung oleh regulasi teknis dari Bank Indonesia seperti PADG No. 21/18/PADG/2019 dan PBI No. 23/6/PBI/2021, serta standar internasional dari FATF, kerangka hukum tersebut pada prinsipnya mampu menjerat pelaku penyalahgunaan *QRIS*. Namun, dalam implementasinya, pengaturan hukum ini belum sepenuhnya efektif karena adanya

⁵⁹ PPATK, *Kajian Risiko Sistem Pembayaran 2024*, hlm. 66–72.

⁶⁰ PPATK, *Pedoman Digital Forensics Keuangan*, 2024.

⁶¹ PPATK, *Laporan Tahunan 2024*, hlm. 88–93.

⁶² FATF, *Money Laundering Risks in Fast Payment Systems*, Paris: FATF, 2023.

kesenjangan regulasi yang signifikan. Dalam praktiknya, modus pencucian uang melalui QRIS umumnya mengikuti tiga tahapan klasik yaitu, *Placement*, *Layering*, *Integration*.

2. Penerapan sanksi pidana bagi pelaku pencucian uang melalui QRIS telah memiliki dasar hukum yang jelas dalam UU TPPU, khususnya Pasal 3, Pasal 4, dan Pasal 5. Ancaman sanksi yang berat hingga 20 tahun penjara dan denda miliaran rupiah secara teoritis diharapkan dapat memberikan efek jera. Namun, efektivitas penerapan sanksi tersebut masih terhambat oleh berbagai tantangan operasional, antara lain: Kompleksitas pembuktian elektronik dalam transaksi digital yang melibatkan banyak akun yang tidak terdaftar, Kecepatan transaksi QRIS yang *real-time*, Penggunaan identitas palsu, serta Keterbatasan kapasitas forensik digital aparat penegak hukum dalam menganalisis data transaksi dalam jumlah besar.

B. Saran

1. Perlu segera dibuat regulasi yang secara eksplisit mengatur pencegahan penyalahgunaan QRIS untuk pencucian uang. Bank Indonesia bersama PPATK harus menyusun Pedoman APU-PPT khusus QRIS yang mencakup standar verifikasi merchant berbasis biometrik dan integrasi data *real-time* dengan Dukcapil, kewajiban penerapan sistem deteksi transaksi mencurigakan berbasis kecerdasan buatan untuk mengidentifikasi pola *micropayment laundering*, serta mekanisme pelaporan otomatis dan *real-time* oleh PJP/PJSP. Di tingkat kelembagaan, dibutuhkan pembentukan Kelompok Kerja Pembayaran Digital Nasional (*Nasional Digital Payment Task Force*) yang memfasilitasi koordinasi dan pertukaran data terintegrasi secara *real-time* antara BI, PPATK, OJK, Kepolisian, dan Kejaksaan guna mempercepat respons terhadap indikasi kejahatan keuangan digital.
2. Kapasitas teknis aparat penegak hukum harus ditingkatkan melalui program pelatihan berkelanjutan di bidang forensik digital dan analisis aliran dana elektronik, agar penyidik, jaksa, dan hakim mampu mengolah bukti digital dan menerapkan

mekanisme pembuktian terbalik secara efektif.

DAFTAR PUSTAKA

BUKU

- Alvi Syahrin, M. A. (2024). *Tindak Pidana Korupsi dan Tindak Pidana Pencucian Uang pada sektor sumber daya alam*, Merdeka Kreasi
- Arief, Barda Nawawi. (2018) *Masalah Penegakan Hukum dan Kebijakan Kriminal*. Bandung: Citra Aditya Bakti
- Arifin, R. M. (2021). *Tindak Pidana Pencucian Uang di Indonesia: Peran Profesi Advokat Sebagai Pihak Pelapor Terhadap Unusual Transaction*. LPPM Institut Agama Islam (IAI) Sunan Giri Ponorogo.
- Arsyad, Ahmad. (2020) *Hukum Pembuktian dalam Perkara Pidana*. Bandung: Refika Aditama.
- Fatmawati, Indira (2021). *Hukum Perbankan dan Anti Pencucian Uang*. Jakarta: Sinar Grafika.
- Muladi dan Dwidja Priyatno. (2019) *Pemberantasan Korupsi dan Pencucian Uang*. Jakarta: Kencana.
- Kristiana, Y. (2021). *Pemberantasan Tindak Pidana Pencucian Uang, Perspektif Hukum Progresif*, Thafa Media.
- Kristiawanto. (2023). *Pengantar Memahami Tindak Pidana Pencucian Uang (Money Laundering)*, Nasmedia.
- PPATK. (2024) *Pedoman Digital Forensics Keuangan*. Jakarta: PPATK.
- Priyatno, M. (2019). *Pemberantasan Korupsi dan Pencucian Uang; Asas, Teori, dan Praktik*. Bandung: Refika Aditama.
- Sriekaningsih, A. (2020). *QRIS dan Era Baru Transaksi Pembayaran 4.0*.
- Suteki & Galang Taufani. (2020) *Metode Penelitian Hukum*. Malang: Setara Press.
- Sutedi, A. (2008). *Tindak Pidana Pencucian Uang*, PT. Citra Aditya Bakti.
- Sutedi, A. (2021). *Hukum Perbankan: Suatu Tinjauan Pencucian Uang dan Sanksi Hukum Perbankan: Suatu Tinjauan Pencucian Uang dan Sanksi*. Jakarta: Sinar Grafika.
- Winatasya, M., & Rahayuningsih, C. D. (2025). Hukum Pidana: Kajian Literature Review. *Journal of Literature Review*, 1(1), 154–160.

Wiyono, R. (2022). *Pembahasan Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang*, Jakarta: Sinar Grafika.

JURNAL ILMIAH

Fauzan, Irfan. (2023) “Efektivitas Penegakan Hukum terhadap Tindak Pidana Pencucian Uang di Indonesia.” *Jurnal Yudisial*, Vol. 16 No. 2.

Lestari, R. & Hidayat, A. (2021) “Penerapan Pembuktian Terbalik dalam Tindak Pidana Pencucian Uang.” *Jurnal Hukum dan Pembangunan*, Vol. 51 No. 1.

Putra, R. A. & Nurhaliza. (2022) “Peran PPATK dalam Sistem Peradilan Pidana pada Tindak Pidana Pencucian Uang Digital.” *Jurnal Ius Quia Iustum*, Vol. 29 No. 3.

Saputra D, & S. (2022). Analisis Hukum Terhadap Efektivitas Penerapan Prinsip *Know Your Customer* (KYC) Pada Layanan *QRIS* dalam Rangka Pencegahan Money Laundering. *Jurnal Hukum Lex Generalis*, 3(5).

Siregar, Reza F (2020). “Perkembangan Financial Technology dan Tantangan Regulasi di Indonesia.” *Jurnal Hukum dan Pembangunan*, Vol. 50 No. 4.

Wibisono, Adrian. (2022) “Teknik Forensik Digital dalam Pembuktian Kejahatan Siber.” *Jurnal Ilmu Hukum Forum*, Vol. 8 No. 2.

Wijaya, T. (2021). Tantangan Regulasi Pencegahan Pencucian Uang di Era Financial Technology (Fintech). *Jurnal Legislasi Indonesia*, 18(2), 215–230.

PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 1 Tahun 2024, yang merupakan perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Peraturan Bank Indonesia Nomor 23/18/PBI/2021 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran

Peraturan Bank Indonesia Nomor 21/18/PBI/2019 tentang Penyediaan Layanan *Quick Response Indonesian Standard (QRIS)*.

Peraturan PPATK Nomor 10 Tahun 2017 tentang Penerapan APU-PPT.

Peraturan Mahkamah Agung Nomor 5 Tahun 2014 tentang Pembuktian Elektronik

SKRIPSI

Alfath, Rizky Putra. (2023) *Analisis Risiko Penyalahgunaan QRIS pada Sistem Pembayaran Nasional*. Skripsi. Universitas Airlangga.

Ananda, Fitrah. (2022) *Penegakan Hukum terhadap Pencucian Uang Menggunakan Rekening Digital*. Skripsi. Universitas Diponegoro.

Fadilah, Rahma. (2021) *Efektivitas Pembuktian Elektronik dalam Perkara TPPU*. Tesis. Universitas Indonesia.

Mulyono, Dimas. (2020) *Analisis Sistem Pelaporan PPATK dalam Pengungkapan Kejahatan Pencucian Uang*. Skripsi. Universitas Brawijaya.

Muhammad Yusuf Abustam: Tinjauan Yuridis Terhadap Tindak Pidana Pencucian Uang Dari Hasil Korupsi Melalui Permainan Kasino

Nugraheni, Ayu. (2022) *Penerapan Prinsip KYC terhadap Merchant QRIS dalam Perspektif AML-CFT*. Tesis. Universitas Indonesia.

INTERNET

Asep Nursobah, (2025) “Pencucian Uang”, Glosarium Hukum, Situs Web Kepaniteraan Mahkamah Agung RI. Tanggal Akses 02 Agustus

Supriyanto, B. E. (2024, September 25). *Implementasi QRIS dalam Sistem Pembayaran Belanja Negara Atas Beban APBN*. Retrieved from Ditjen Perbendaharaan Kemenkeu RI: <https://djpb.kemenkeu.go.id/kppn/watampone/id/data-publikasi/artikel/3752-implementasi-QRIS-dalam-sistem-pembayaran-belanja-negara-atas-beban-apbn.html>

Mahendra, R. A. (2025, Mei 07). *Begini Cara Tersangka Samarkan Aliran Uang Hasil Judol di Perusahaan Cangkang*. Retrieved from detik news: <https://news.detik.com/berita/d-7903686/begini-cara-tersangka-samarkan-aliran-uang-hasil-judol-di-perusahaan-cangkang>

Nasution, E. (2020). Memahami Praktik Pencucian Uang Hasil Kejahatan. In Dokumen KPK. academia.edu. <https://www.academia.edu/download/35690956/Praktik-pencucianuang-Edi->

Nasution.pdf. Tanggal Akses 02 Oktober 2025

“Profil dan Fungsi PPATK,” Portal Resmi PPATK,
<https://www.ppatk.go.id/ppatk/profil.html>
Tanggal Akses 02 November 2025

SUMBER LAINNYA

- Bank Indonesia (2024). *Laporan Sistem Pembayaran 2023*. Jakarta: Bank Indonesia.
- Chainalysis. (2022). *The 2022 Crypto Crime Report*. New York: Chainalysis Inc.
- FATF. (2023). *Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*. Paris: FATF.
- INTERPOL. (2023). *Global Report on Cybercrime and CryptocurrencyRelated Laundering*. Lyon: INTERPOL.
- OJK. (2022). *Pedoman Penerapan Prinsip Mengenali Pengguna Jasa (Know Your Customer) di Lembaga Keuangan Nonbank*. Jakarta: OJK.
- OJK. (2023). *Kajian Aset Kripto dan Risiko AML/CFT di Indonesia*. Jakarta: OJK.
- PPATK & Kominfo. (2023). *Pedoman Literasi Keuangan Digital dan Pencegahan TPPU Berbasis Aset Kripto*. Jakarta: PPATK
- PPATK. (2023). *Laporan Analisis Transaksi Keuangan: Risiko Pencucian Uang Berbasis Aset Digital di Indonesia*. Jakarta: PPATK.
- PPATK. (2023). *Laporan Tahunan PPATK 2023: Transaksi Keuangan Digital dan Tantangan Pengawasan*. Jakarta: PPATK.
- PPATK. (2023). *Laporan Tahunan: Transaksi Keuangan Mencurigakan di Era Digital*. Jakarta: PPATK.