

Artikel Penelitian

Penegakan Hukum Tindak Pidana terhadap Pemalsuan Kode QRIS di Rumah Ibadah

Studi Kasus Putusan PN Jakarta Selatan Nomor 419/Pid.Sus/2023/PN JKT.SEL

Kurniati Cahyowulandari*, Hendri Jayadi Pandiangan, Armunanto Hutahaean

Fakultas Hukum, Program Studi Magister Hukum, Universitas Kristen Indonesia, Jakarta, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 21 Juni 2026
Revisi Akhir: 25 Agustus 2026
Diterbitkan Online: 27 Agustus 2026

KATA KUNCI

Kejahatan Siber
Transaksi Elektronik
Pemalsuan
Penegakan Hukum
QRIS

KORESPONDENSI (*)

Phone: +62 812-1006-2659
E-mail: kurniati.cahyo@gmail.com

A B S T R A K

Perkembangan pesat QRIS (*Quick Response Code Indonesian Standard*) telah meningkatkan penggunaan sistem pembayaran digital di Indonesia, termasuk di rumah ibadah. Namun, penggunaan QRIS yang semakin luas juga menimbulkan peluang terjadinya kejahatan siber melalui pemalsuan kode QRIS dengan cara mengganti kode QR resmi menggunakan kode milik pribadi pelaku. Penelitian ini bertujuan untuk menganalisis penegakan hukum terhadap pelaku pemalsuan QRIS serta mengkaji pertanggungjawaban pihak terkait dalam transaksi elektronik melalui QRIS. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan pendekatan kasus melalui Putusan Pengadilan Negeri Jakarta Selatan Nomor 419/Pid.Sus/2023/PN JKT.SEL. Hasil penelitian menunjukkan bahwa penegakan hukum terhadap pemalsuan QRIS menerapkan Pasal 35 jo Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik sebagai *lex specialis* terhadap kejahatan elektronik. Selain itu, Pasal 263 jo Pasal 391 KUHP Nasional dapat memperkuat konstruksi hukum tindak pidana pemalsuan. Penelitian ini juga menemukan bahwa pertanggungjawaban tidak hanya dibebankan kepada pelaku, tetapi juga melibatkan Bank Indonesia dan Penyedia Jasa Pembayaran dalam pengawasan sistem pembayaran digital.

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat, khususnya dalam sistem pembayaran elektronik. Sistem pembayaran digital menggunakan kode *QR* semakin berkembang di berbagai negara, termasuk Indonesia, karena dinilai lebih efisien, cepat, dan mudah digunakan dalam transaksi elektronik.¹ Perkembangan tersebut mendorong transformasi sistem pembayaran dari transaksi konvensional menuju transaksi berbasis teknologi digital.

QRIS (*Quick Response Code Indonesian Standard*) diperkenalkan oleh Bank Indonesia sebagai standar nasional pembayaran berbasis kode *QR* yang bertujuan menciptakan interoperabilitas sistem pembayaran digital di Indonesia.² *QRIS* memungkinkan seluruh aplikasi pembayaran digital menggunakan satu standar kode *QR* sehingga mempermudah transaksi masyarakat. Setelah diluncurkan secara resmi pada 17 Agustus 2019, penggunaan *QRIS* mengalami perkembangan yang sangat signifikan di berbagai sektor, termasuk perdagangan, jasa, dan rumah ibadah.³

¹ E-Conomy SEA 2024, hlm. 36.

² Ana Srikaningsih. (2020). *QRIS dan Era Baru Transaksi Pembayaran 4.0*. Yogyakarta: Andi, hlm. 1-3.

³ Julang Aryowiloto & Dewa Gde Yoga Permana. (2024). *QRIS: Katalis Pertumbuhan UMKM Lokal Bali*. Sukabumi: CV Jejak, hlm. 7-9.

Transformasi digital dalam sistem pembayaran nasional semakin meningkat setelah pandemi COVID-19 yang mendorong masyarakat menggunakan transaksi non-tunai. Berdasarkan data Bank Indonesia, transaksi *QRIS* pada kuartal III tahun 2024 tumbuh sebesar 209,61% dibandingkan periode yang sama tahun sebelumnya dengan jumlah pengguna mencapai sekitar 53,3 juta pengguna dan jumlah *merchant* mencapai 34,23 juta *merchant*.⁴ Selain itu, pada tahun 2025 jumlah pengguna *QRIS* telah mencapai lebih dari 56 juta pengguna dengan nilai transaksi mencapai Rp1,9 kuadriliun.⁵ *QRIS* bahkan telah digunakan lintas negara seperti Thailand, Malaysia, dan Jepang sebagai bagian dari sistem pembayaran digital internasional.

Perkembangan tersebut menunjukkan bahwa *QRIS* telah menjadi bagian penting dalam aktivitas ekonomi masyarakat Indonesia, termasuk dalam kegiatan sosial dan keagamaan. Saat ini banyak rumah ibadah menggunakan *QRIS* sebagai sarana pembayaran zakat, infak, sedekah, dan donasi lainnya. Namun di sisi lain, perkembangan teknologi pembayaran digital juga menimbulkan berbagai bentuk kejahatan berbasis teknologi informasi, salah satunya pemalsuan kode *QRIS*. Pemalsuan *QRIS* dilakukan dengan cara mengganti kode *QR* resmi milik *merchant* atau rumah ibadah menggunakan kode milik pribadi pelaku sehingga dana transaksi masyarakat masuk ke rekening pelaku. Tindakan tersebut tidak hanya menimbulkan kerugian ekonomi, tetapi juga menurunkan tingkat kepercayaan masyarakat terhadap sistem pembayaran digital.⁶ Penyalahgunaan *QRIS* menunjukkan bahwa perkembangan teknologi digital juga diikuti dengan meningkatnya potensi kejahatan siber dalam sistem transaksi elektronik.

Peningkatan tindak pidana berbasis teknologi informasi juga terlihat dari meningkatnya jumlah tindak pidana di bidang Informasi dan Transaksi Elektronik (ITE) di Indonesia. Berdasarkan data Badan Reserse Kriminal Polri Biro Pembinaan Operasional Tahun 2025, jumlah tindak pidana ITE tersebar di berbagai wilayah Indonesia dan mengalami fluktuasi setiap bulan. Kondisi tersebut menunjukkan bahwa perkembangan teknologi digital diikuti dengan meningkatnya potensi kejahatan siber, termasuk penyalahgunaan sistem pembayaran elektronik melalui *QRIS*.

Tabel 1. Jumlah Tindak Pidana ITE Per Bulan Tahun 2025⁷

Bulan	Jumlah Kasus
Januari	1.435
Februari	1.513
Maret	1.461
April	1.382
Mei	1.644
Juni	1.527
Juli	1.562
Agustus	1.410
September	1.573
Oktober	1.684
November	1.640
Desember	1.679
Total	18.510

Berdasarkan data tersebut, terlihat bahwa kejahatan di bidang ITE telah menjadi fenomena yang luas dan sistemik. Kondisi ini mengindikasikan bahwa ruang digital, termasuk sistem pembayaran elektronik, memiliki tingkat kerentanan terhadap berbagai bentuk kejahatan yang terus berkembang. Dari perspektif hukum, terdapat ketidaksesuaian antara *das sollen* dan *das sein*. Regulasi Bank Indonesia mengatur standar penggunaan *QRIS* sebagai instrumen pembayaran digital nasional, namun belum secara khusus mengatur pemalsuan *QRIS* sebagai tindak pidana tersendiri. Dalam praktik penegakan hukum, aparat penegak hukum menggunakan ketentuan Undang-Undang Informasi dan Transaksi Elektronik untuk menjerat pelaku, sementara penerapan Pasal 263 ayat (1) jo. Pasal 391 KUHP Nasional sebagai dasar hukum kumulatif belum dilakukan. Kondisi tersebut menunjukkan adanya kekosongan norma dan ketidakterpaduan pengaturan hukum terhadap tindak pidana pemalsuan *QRIS* dalam sistem hukum pidana Indonesia. Meskipun telah terdapat Putusan

⁴<https://www.beritasatu.com/ekonomi/2848876/transaksi-qr-is-tumbuh-20961-persen-pada-kuartal-iii-2024>

⁵<https://www.cnnindonesia.com/ekonomi/20251104130801-532-1291696/airlangga-qr-is-ditakuti-negara-lain-penggunanya-tembus-56-juta>

⁶ Satjipto Rahardjo. (2006). *Ilmu Hukum*. Bandung: Citra Aditya Bakti, hlm.53.

⁷ Data Badan Reserse Kriminal Polri Biro Pembinaan Operasional mengenai tindak pidana ITE Tahun 2025, diperoleh per 6 Maret 2026.

Pengadilan Negeri Jakarta Selatan Nomor 419/Pid.Sus/2023/PN JKT.SEL yang menjatuhkan pidana terhadap pelaku pemalsuan QRIS, masih terdapat perdebatan mengenai konstruksi hukum yang tepat untuk digunakan dalam perkara tersebut.

TINJAUAN PUSTAKA

Teori Perlindungan Hukum dan Penegakan Hukum

Penegakan hukum pada hakikatnya merupakan proses penyerasian nilai-bahan yang menjabarkan nilai-nilai secara konkrit guna mewujudkan ketertiban, kepastian hukum, dan keadilan dalam kehidupan bermasyarakat. Menurut Oki Irawan, dkk., penegakan hukum di Indonesia tidak boleh hanya dipandang dari dimensi kepastian formal-prosedural semata, melainkan harus menyentuh pemenuhan hak-hak substantif warga negara agar tercipta stabilitas dan keadilan sosial yang riil dalam dinamika masyarakat modern.⁸ Konsep ini sejalan dengan pandangan Satjipto Rahardjo yang menyatakan bahwa hukum tidak selainnya menjadi instrumen yang kaku, melainkan sebuah institusi yang bertujuan mengabdikan pada manusia dan beradaptasi secara proaktif terhadap percepatan peradaban, termasuk di dalamnya akselerasi teknologi informasi.⁹

Dalam memetakan kedudukan hukum korban kejahatan di ruang digital, teori perlindungan hukum dari Philipus M. Hadjon membaginya ke dalam dua bentuk utama, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif menitikberatkan pada penyediaan rambu-rambu regulasi, standar operasional, dan pengawasan sistematis guna mencegah terjadinya pelanggaran hukum sebelum kerugian itu nyata terjadi. Sebaliknya, perlindungan hukum represif bertumpu pada pelaksanaan sanksi pidana maupun perdata sebagai instrumen pemulihan keadaan dan penegakan keadilan setelah tindak pidana terjadi.¹⁰ Dalam konteks kejahatan digital berbasis keuangan, implementasi perlindungan hukum represif menjadi garda terdepan untuk memulihkan kepercayaan publik (*public trust*) terhadap ekosistem transaksi elektronik nasional.

Karakteristik Kejahatan Siber (Cybercrime) dan Transaksi Elektronik

Perkembangan teknologi internet telah melahirkan ruang baru yang dikenal sebagai ruang siber (*cyberspace*). Karakteristik ruang siber yang asimetris, lintas batas (*borderless*), dan anonim memicu pergeseran modus kejahatan konvensional menuju format digital. Menurut Abdul Wahid dan Mohammad Labib, *cybercrime* dapat diklasifikasikan sebagai segala bentuk pemanfaatan teknologi komputer, jaringan internet, dan perangkat elektronik secara melawan hukum untuk melakukan manipulasi atau perusakan data demi memperoleh keuntungan finansial atau non-finansial sepihak.¹¹ Kejahatan siber ini tidak lagi menargetkan fisik manusia atau barang secara langsung, melainkan menyasar integritas sistem dan validitas informasi elektronik.

Seiring dengan tren digitalisasi finansial, instrumen *Quick Response Code Indonesian Standard* (QRIS) hadir sebagai standar nasional untuk mengintegrasikan berbagai kanal pembayaran non-tunai di Indonesia. Namun, keandalan sistem pembayaran ini dihadapkan pada ancaman manipulasi data. Menurut Widodo, aspek hukum kejahatan mayantara menegaskan bahwa dokumen elektronik atau kode digital yang memiliki fungsi hukum setara dengan surat berharga konvensional, sangat rentan terhadap intervensi ilegal (*unauthorized access*) dan manipulasi.¹² Manipulasi kode pembayaran ini pada dasarnya merusak rantai kepercayaan dalam transaksi elektronik (*electronic transaction trust*) yang diamanatkan oleh regulasi hukum siber nasional.

Konstruksi Yuridis Tindak Pidana Pemalsuan dalam Hukum Pidana Nasional

Dalam hukum pidana konvensional yang bersumber pada Kitab Undang-Undang Hukum Pidana (KUHP), tindak pidana pemalsuan diatur secara ketat dalam Pasal 263 KUHP. Unsur materiil dari pasal ini mensyaratkan adanya tindakan membuat surat palsu atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan, atau pembebasan utang, dengan maksud untuk menggunakan atau menyuruh orang lain menggunakan seolah-olah surat tersebut asli dan tidak dipalsukan. Menurut I Made Widnyana, asas-asas hukum pidana menekankan bahwa unsur kesalahan (*mens rea*) dan

⁸ Oki Irawan, et al., "Penegakan Hukum di Negara Republik Indonesia", *Federalisme: Jurnal Kajian Hukum dan Ilmu Komunikasi*, Vol. 2, No. 1, 2025, hal. 45.

⁹ Satjipto Rahardjo, *Ilmu Hukum*, (Bandung: Citra Aditya Bakti, 2006), hal. 112-115.

¹⁰ Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat di Indonesia*, (Surabaya: PT Bina Ilmu, 1987), hal. 38.

¹¹ Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, (Bandung: Refika Aditama, 2010), hal. 89.

¹² Widodo, *Aspek Hukum Kejahatan Mayantara*, (Yogyakarta: Aswindo, 2011), hal. 142.

perbuatan melawan hukum (*actus reus*) harus dibuktikan secara akumulatif, di mana pelaku memiliki kehendak sadar untuk mengonstruksikan keadaan palsu yang merugikan orang lain.¹³

Seiring diundangkannya Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Nasional, perluasan tafsir terhadap objek pemalsuan diakomodasi melalui Pasal 391. Regulasi baru ini memperluas cakupan frasa "surat" tidak hanya terbatas pada dokumen fisik di atas kertas, tetapi juga mencakup dokumen, data, dan instrumen elektronik yang memiliki fungsi hukum atau fungsi autentikasi finansial serupa. M. Hanafi menegaskan bahwa perluasan ini merupakan bentuk penyesuaian asas legalitas materiil agar hukum pidana tidak mengalami kekosongan norma (*recht vacuüm*) ketika berhadapan dengan tindak pidana modern yang memanipulasi kode-kode digital fungsional.¹⁴ Dengan demikian, secara teoretis, kode QRIS yang berfungsi memindahkan hak atas dana dapat dikategorikan sebagai objek pemalsuan dalam konstruksi hukum pidana nasional yang diperbarui.

METODOLOGI

Penelitian ini menggunakan metode penelitian hukum normatif (yuridis normatif) dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan kasus (*case approach*). Pendekatan kasus dilakukan melalui analisis mendalam terhadap Putusan Pengadilan Negeri Jakarta Selatan Nomor 419/Pid.Sus/2023/PN JKT.SEL. Data sekunder yang digunakan mencakup bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, serta bahan hukum sekunder berupa literatur hukum, jurnal, dan data statistik resmi terkait kejahatan siber.

HASIL DAN PEMBAHASAN

Peran Penegak Hukum terhadap Pelaku dalam Tindak Pidana Pemalsuan QRIS

Penegakan hukum merupakan proses pelaksanaan norma hukum oleh aparat yang berwenang guna mewujudkan ketertiban, kepastian hukum, dan keadilan dalam masyarakat. Menurut Oki Irawan, penegakan hukum tidak hanya berkaitan dengan penerapan hukum secara formal, tetapi juga menyangkut pelaksanaan hukum secara substantif agar tercipta perlindungan hukum bagi masyarakat.¹⁵ Dalam konteks tindak pidana pemalsuan QRIS, aparat penegak hukum memiliki peran penting dalam melakukan penyelidikan, penyidikan, penuntutan, hingga pelaksanaan putusan pengadilan terhadap pelaku tindak pidana elektronik.

Pemalsuan *QRIS* merupakan bentuk kejahatan siber (*cybercrime*) yang dilakukan melalui manipulasi sistem pembayaran elektronik dengan cara mengganti kode QR resmi menggunakan kode *QR* milik pribadi pelaku. Menurut Wahid dan Labib, *cybercrime* merupakan segala bentuk penggunaan teknologi komputer dan jaringan internet untuk tujuan kriminal.¹⁶ Dalam konteks *QRIS*, pelaku memanfaatkan kelemahan pengawasan terhadap sistem pembayaran digital untuk memperoleh keuntungan secara melawan hukum.

Dalam Putusan Pengadilan Negeri Jakarta Selatan Nomor 419/Pid.Sus/2023/PN JKT.SEL, pelaku terbukti melakukan manipulasi kode *QRIS* dengan mengganti kode *QR* resmi milik rumah ibadah menggunakan kode *QR* milik pribadi sehingga dana transaksi masyarakat masuk ke rekening pelaku.¹⁷ Atas perbuatannya, aparat penegak hukum menerapkan Pasal 35 jo Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Penerapan Pasal 35 UU ITE menunjukkan bahwa tindak pidana pemalsuan QRIS dipandang sebagai bentuk manipulasi informasi elektronik. Pasal tersebut mengatur larangan melakukan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dengan tujuan agar informasi elektronik dianggap seolah-olah data yang otentik. Dalam perkara pemalsuan *QRIS*, tindakan mengganti kode *QR* resmi menggunakan kode milik pelaku memenuhi unsur manipulasi informasi elektronik karena menyebabkan sistem pembayaran digital seolah-olah menunjukkan data yang sah.

¹³ I Made Widnyana, *Asas-Asas Hukum Pidana*, (Jakarta: Fikahati Aneska, 2010), hal. 32.

¹⁴ M. Hanafi, *Sistem Pertanggungjawaban Pidana*, (Jakarta: Rajawali Pers, 2015), hal. 204.

¹⁵ Oki Irawan, (et.al) (2025). "Penegakan Hukum di Negara Republik Indonesia". *Federalisme: Jurnal Kajian Hukum dan Ilmu Komunikasi*, 2(1):hlm. 24-25.

¹⁶ Wahid, A., & Labib, M. (2010). *Kejahatan Mayantara*. Bandung: Refika Aditama, hlm. 40

¹⁷ Putusan Pengadilan Negeri Jakarta Selatan Nomor 419/Pid.Sus/2023/PN JKT.SEL.

Selain menggunakan ketentuan UU ITE, tindak pidana pemalsuan QRIS juga dapat dikaitkan dengan Pasal 263 KUHP mengenai pemalsuan.¹⁸ Hal tersebut karena secara substantif terdapat unsur membuat atau menggunakan objek palsu untuk menimbulkan kerugian pihak lain. Walaupun *QRIS* berbentuk kode digital dan bukan surat sebagaimana dimaksud dalam KUHP konvensional, manipulasi kode QRIS memiliki karakteristik yang menyerupai tindak pidana pemalsuan karena terdapat tindakan mengubah objek elektronik demi memperoleh keuntungan secara melawan hukum.

Dalam perspektif hukum pidana nasional, perbuatan pelaku tidak hanya memenuhi unsur manipulasi informasi elektronik sebagaimana diatur dalam Pasal 35 UU ITE, tetapi juga memenuhi unsur pemalsuan sebagaimana diatur dalam Pasal 263 ayat (1) KUHP dan Pasal 391 Undang-Undang Nomor 1 Tahun 2023 tentang KUHP Nasional. Unsur membuat surat palsu atau memalsukan surat yang dapat menimbulkan hak, perikatan, pembebasan utang, atau diperuntukkan sebagai alat bukti dapat ditafsirkan secara ekstensif terhadap dokumen elektronik yang memiliki fungsi hukum dalam transaksi digital. Kode QRIS sebagai instrumen pembayaran elektronik memiliki fungsi autentikasi transaksi dan menjadi dasar perpindahan dana dalam sistem pembayaran digital. Oleh karena itu, penggantian kode QRIS resmi dengan kode QRIS milik pelaku dapat dipandang sebagai bentuk pemalsuan terhadap instrumen elektronik yang menimbulkan kerugian bagi pihak lain.

Dalam perspektif teori perlindungan hukum Philipus M. Hadjon, penegakan hukum terhadap pelaku tindak pidana pemalsuan *QRIS* merupakan bentuk perlindungan hukum represif yang bertujuan memberikan kepastian hukum dan perlindungan terhadap masyarakat sebagai korban kejahatan digital.¹⁹ Perlindungan hukum represif dilakukan melalui penjatuhan sanksi pidana terhadap pelaku yang terbukti melakukan tindak pidana elektronik.

Penegakan hukum terhadap tindak pidana pemalsuan *QRIS* juga menunjukkan bahwa perkembangan teknologi digital memerlukan penyesuaian sistem hukum pidana agar mampu mengantisipasi bentuk-bentuk kejahatan siber yang terus berkembang. Oleh karena itu, diperlukan penguatan regulasi dan peningkatan kapasitas aparat penegak hukum dalam menangani tindak pidana berbasis teknologi informasi.

Dalam Putusan Pengadilan Negeri Jakarta Selatan Nomor 419/Pid.Sus/2023/PN JKT.SEL, hakim menilai bahwa unsur manipulasi informasi elektronik sebagaimana dimaksud dalam Pasal 35 UU ITE telah terpenuhi karena terdakwa secara sengaja mengganti kode QRIS resmi yang digunakan sebagai sarana pembayaran donasi dengan kode QRIS miliknya sendiri. Perbuatan tersebut mengakibatkan informasi elektronik yang digunakan dalam sistem pembayaran menjadi seolah-olah otentik dan sah, padahal telah mengalami perubahan yang dilakukan tanpa hak. Berdasarkan fakta persidangan, hakim berpendapat bahwa tindakan terdakwa telah menimbulkan kerugian bagi pihak rumah ibadah dan masyarakat yang melakukan transaksi melalui QRIS tersebut. Oleh karena itu, hakim menjatuhkan pidana berdasarkan ketentuan Pasal 35 jo. Pasal 51 ayat (1) UU ITE.

Meskipun demikian, menurut penulis, konstruksi hukum dalam perkara ini masih dapat diperkuat melalui penerapan Pasal 263 ayat (1) jo. Pasal 391 KUHP Nasional secara kumulatif. Pendekatan tersebut akan memberikan dasar hukum yang lebih komprehensif karena perbuatan pelaku tidak hanya merupakan manipulasi informasi elektronik, tetapi juga mengandung unsur pemalsuan terhadap instrumen elektronik yang digunakan dalam sistem pembayaran digital.²⁰

Pertanggungjawaban Pihak Terkait dalam Transaksi Elektronik melalui QRIS

Pertanggungjawaban pidana dalam tindak pidana pemalsuan *QRIS* pada dasarnya dibebankan kepada pelaku yang secara sengaja melakukan manipulasi kode QRIS demi memperoleh keuntungan pribadi. Dalam hukum pidana, seseorang dapat dimintai pertanggungjawaban pidana apabila melakukan perbuatan melawan hukum dan memiliki kesalahan atas perbuatan yang dilakukannya.²¹ Pelaku pemalsuan QRIS bertanggung jawab atas kerugian yang timbul akibat manipulasi sistem pembayaran digital dan dapat dikenakan pidana penjara maupun denda sesuai ketentuan UU ITE.

Selain pelaku, terdapat pula tanggung jawab administratif dari Bank Indonesia dan Penyedia Jasa Pembayaran (PJP) sebagai pihak yang memiliki kewenangan dalam pengawasan sistem pembayaran digital. Bank Indonesia sebagai

¹⁸ I Made Widnyana. (2010). *Asas-Asas Hukum Pidana*. Jakarta: Fikahati Aneska, hlm. 32.

¹⁹ Philipus M. Hadjon. (1987). *Perlindungan Hukum Bagi Rakyat di Indonesia*. Surabaya: PT Bina Ilmu, hlm. 38.

²⁰ I Made Widnyana, *Asas-Asas Hukum Pidana* (Jakarta: Fikahati Aneska, 2010), hlm. 32.

²¹ Hanafi, M. (2015). *Sistem Pertanggungjawaban Pidana*. Jakarta: Rajawali Pers, hlm. 16.

regulator sistem pembayaran nasional memiliki tanggung jawab menjaga keamanan dan stabilitas sistem pembayaran elektronik, termasuk *QRIS*.²²

Berdasarkan hasil penelitian, Bank Indonesia sebagai regulator sistem pembayaran nasional tidak hanya memiliki kewajiban menetapkan standar *QRIS*, tetapi juga melakukan pengawasan terhadap implementasi sistem pembayaran digital. Dalam hal ditemukan penyalahgunaan *QRIS* yang berkaitan dengan tindak pidana, Bank Indonesia dapat berkoordinasi dengan Penyedia Jasa Pembayaran untuk melakukan pemblokiran *QRIS* yang digunakan sebagai sarana tindak pidana dan melakukan langkah mitigasi guna mencegah kerugian yang lebih luas.²³

PJP juga memiliki kewajiban memastikan keamanan layanan pembayaran digital yang digunakan *merchant* dan masyarakat. Lemahnya pengawasan terhadap penggunaan *QRIS* dapat membuka peluang terjadinya penyalahgunaan kode *QR* oleh pihak tertentu. Oleh karena itu, penguatan sistem keamanan dan pengawasan terhadap penggunaan *QRIS* menjadi hal yang sangat penting untuk mencegah terjadinya tindak pidana pemalsuan *QRIS*. Rumah ibadah sebagai pengguna *QRIS* juga memiliki tanggung jawab melakukan pengawasan terhadap media pembayaran digital yang digunakan. Kurangnya pengawasan terhadap kode *QRIS* yang ditempatkan di area publik menjadi salah satu faktor yang mempermudah terjadinya manipulasi kode *QRIS* oleh pelaku.

Dalam perspektif teori kejahatan siber, perkembangan teknologi digital selalu diikuti dengan perkembangan bentuk kejahatan elektronik yang semakin kompleks.²⁴ Oleh karena itu, hukum harus mampu beradaptasi terhadap perkembangan teknologi informasi agar dapat memberikan perlindungan hukum secara efektif kepada masyarakat.

KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penegakan hukum terhadap tindak pidana pemalsuan kode *QRIS* dilakukan melalui penerapan Pasal 35 jo. Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik terhadap pelaku yang melakukan manipulasi kode *QRIS* untuk memperoleh keuntungan secara melawan hukum. Penegakan hukum tersebut dilaksanakan oleh kepolisian, kejaksaan, dan pengadilan melalui proses penyidikan, penuntutan, dan pemeriksaan perkara berdasarkan ketentuan tindak pidana elektronik. Namun demikian, dalam konstruksi dakwaan dan putusan perkara, aparat penegak hukum belum memasukkan Pasal 263 ayat (1) jo. Pasal 391 KUHP Nasional sebagai dasar hukum kumulatif, padahal perbuatan pelaku juga memenuhi unsur pemalsuan. Dalam praktiknya, UU ITE berfungsi sebagai *lex specialis* terhadap tindak pidana berbasis elektronik, sedangkan Pasal 263 ayat (1) jo. Pasal 391 KUHP Nasional dapat digunakan secara kumulatif untuk memperkuat konstruksi hukum pemalsuan dalam dakwaan. Selain itu, belum adanya pengaturan khusus mengenai pemalsuan *QRIS* menyebabkan aparat penegak hukum masih menggunakan ketentuan dalam KUHP dan UU ITE untuk menangani tindak pidana tersebut.

Pertanggungjawaban dalam transaksi elektronik melalui *QRIS* tidak hanya dibebankan kepada pelaku tindak pidana, tetapi juga melibatkan Bank Indonesia dan Penyedia Jasa Pembayaran sebagai pihak yang memiliki kewajiban melakukan pengawasan dan pengamanan sistem pembayaran digital. Di samping itu, rumah ibadah sebagai pengguna *QRIS* juga memiliki tanggung jawab dalam menjaga keamanan penggunaan *QRIS* untuk mencegah terjadinya penyalahgunaan. Dengan demikian, pertanggungjawaban dalam transaksi *QRIS* tidak hanya berkaitan dengan pelaku tindak pidana, tetapi juga dengan kewajiban pengawasan dan pengamanan sistem pembayaran digital oleh pihak-pihak terkait.

Berdasarkan hasil penelitian, pemerintah dan pembentuk undang-undang perlu melakukan penguatan dan harmonisasi regulasi terkait tindak pidana dalam sistem pembayaran digital, khususnya mengenai pemalsuan *QRIS*, guna mewujudkan kepastian hukum dalam penanganan kejahatan berbasis elektronik. Selain itu, Bank Indonesia, Penyedia Jasa Pembayaran, dan pengguna *QRIS*, termasuk rumah ibadah, perlu meningkatkan pengawasan melalui verifikasi berkala terhadap kode *QRIS*, edukasi kepada masyarakat, serta penguatan sistem keamanan transaksi elektronik untuk mencegah penyalahgunaan *QRIS* dan meningkatkan kepercayaan masyarakat terhadap sistem pembayaran digital.

²² Bank Indonesia, *QRIS*, <https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/ritel/kanal-layanan/qr/default.aspx>

²³ *Ibid.*

²⁴ Widodo. (2011). *Aspek Hukum Kejahatan Mayantara*. Yogyakarta: Aswindo, hlm. 15.

1. DAFTAR PUSTAKA

Buku

- Hadjon, P. M. (1987). *Perlindungan hukum bagi rakyat di Indonesia*. PT Bina Ilmu.
- Hanafi, M. (2015). *Sistem pertanggungjawaban pidana*. Rajawali Pers.
- Rahardjo, S. (2006). *Ilmu hukum*. Citra Aditya Bakti.
- Wahid, A., & Labib, M. (2010). *Kejahatan mayantara (cyber crime)*.
- Refika Aditama. Widodo. (2011). *Aspek hukum kejahatan mayantara*.
- Aswindo. Widnyana, I M. (2010). *Asas-asas hukum pidana*. Fikahati Aneska.

Jurnal

- Irawan, O., et al. (2025). Penegakan hukum di Negara Republik Indonesia. *Federalisme: Jurnal Kajian Hukum dan Ilmu Komunikasi*, 2(1), 40-52.

Peraturan Perundang-Undangan & Dokumen Hukum Resmi

- Indonesia. (1946). *Undang-Undang Nomor 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana*.
- Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.
- Indonesia. (2023). *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842.
- Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6921.
- Pengadilan Negeri Jakarta Selatan. (2023). *Putusan Nomor 419/Pid.Sus/2023/PN JKT.SEL*.

Data Statistik & Informasi Daring

- Badan Reserse Kriminal Polri Biro Pembinaan Operasional. (2025). *Data tindak pidana ITE tahun 2025*. Markas Besar Kepolisian Negara Republik Indonesia.
- Bank Indonesia. (2024). *Kanal layanan Quick Response Code Indonesian Standard (QRIS)*. <https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/ritel/kanal-layanan/qr/default.aspx>.
- Berita Satu. (2024, November). *Transaksi QRIS tumbuh 209,61 persen pada kuartal III 2024*. <https://www.beritasatu.com/ekonomi/2848876/transaksi-qr-is-tumbuh-20961-persen-pada-kuartal-iii-2024>.
- CNN Indonesia. (2025, November). *Airlangga: QRIS ditakuti negara lain, penggunaanya tembus 56 juta*. <https://www.cnnindonesia.com/ekonomi/20251104130801-532-1291696/airlangga-qr-is-ditakuti-negara-lain-penggunaanya-tembus-56-juta>.