



Pengaturan Hukum terhadap Penipuan Kode QR Palsu dalam Transaksi Elektronik di Indonesia

INFO PENULIS

Niken Yulian Yusuf
Universitas Sulawesi Tenggara
nikenyyu@gmail.com

INFO ARTIKEL

ISSN: 2808-1307
Vol. 6, No. 2, Agustus 2026
<https://jurnal.ardenjaya.com/index.php/ajsh>

© 2026 Arden Jaya Publisher All rights reserved

Saran Penulisan Referensi

Yusuf, N. Y., & Yusuf, V. S. (2026). Pertanggungjawaban Pidana terhadap Penggunaan Kode QR Palsu dalam Transaksi Elektronik di Indonesia. *Arus Jurnal Sosial dan Humaniora*, 6 (2), 2931-2936.

Abstrak

Transformasi sistem pembayaran digital telah meningkatkan penggunaan kode *Quick Response* (QR) sebagai instrumen pembayaran yang praktis, termasuk melalui *Quick Response Code Indonesian Standard* (QRIS). Bersamaan dengan manfaat tersebut, penggunaan kode QR membuka ruang bagi penipuan melalui penggantian kode QR milik pedagang, pembuatan kode QR palsu, pengalihan dana ke rekening pelaku, maupun pengiriman kode QR yang mengarahkan pengguna pada tautan berbahaya. Artikel ini bertujuan menganalisis pengaturan hukum terhadap penipuan kode QR palsu dalam transaksi elektronik di Indonesia serta menilai kecukupan konstruksi hukumnya. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum primer meliputi Kitab Undang-Undang Hukum Pidana, Undang-Undang tentang Informasi dan Transaksi Elektronik, regulasi sistem pembayaran Bank Indonesia, dan ketentuan perlindungan konsumen. Analisis dilakukan secara preskriptif-kualitatif melalui identifikasi unsur perbuatan, kepentingan hukum yang dilindungi, dan relasi antarregulasi. Hasil penelitian menunjukkan bahwa Indonesia belum memiliki delik yang secara eksplisit diberi nomenklatur "penipuan kode QR palsu". Namun, perbuatan tersebut dapat dijangkau secara kumulatif atau alternatif melalui ketentuan penipuan dalam KUHP, larangan manipulasi atau penciptaan informasi dan/atau dokumen elektronik yang seolah-olah otentik dalam UU ITE, serta pengaturan keamanan dan manajemen risiko dalam sistem pembayaran. Fragmentasi pengaturan menimbulkan kebutuhan harmonisasi norma, pedoman kualifikasi modus, penguatan mekanisme pengamanan QRIS, dan peningkatan literasi keamanan digital bagi pengguna serta pedagang.

Kata Kunci: Penipuan Digital, Kode QR Palsu, QRIS, Transaksi Elektronik, UU ITE.

Abstract

The transformation of digital payment systems has increased the use of Quick Response (QR) codes as practical payment instruments, including through the Quick Response Code Indonesian Standard (QRIS). Alongside these benefits, QR code payments create opportunities for fraud through the replacement of merchants' QR codes, the creation of fraudulent QR codes, diversion of funds to offenders' accounts, and the distribution of QR codes directing users to malicious links. This article examines the legal regulation of fraudulent QR code practices in electronic transactions in Indonesia and assesses the adequacy of the existing legal framework. It employs normative legal research using statutory and conceptual approaches. Primary legal materials include the Criminal Code, the Electronic Information and Transactions Law, Bank Indonesia payment-system regulations, and consumer-protection provisions. The materials are analysed qualitatively and prescriptively by identifying the elements of conduct, protected legal interests, and the relationships among relevant regulations. The study finds that Indonesian law does not yet provide a criminal offence expressly labelled as "fraudulent QR code fraud." Nevertheless, such conduct may be addressed cumulatively or alternatively through fraud provisions in the Criminal Code, prohibitions on the manipulation or creation of electronic information and/or documents made to appear authentic under the Electronic Information and Transactions Law, and payment-system security and risk-management rules. The fragmented framework calls for harmonisation, guidance on qualifying QR-code fraud patterns, stronger QRIS safeguards, and improved digital-security literacy for users and merchants.

Keywords: Digital Fraud, Fraudulent QR Code, QRIS, Electronic Transactions, Electronic Information and Transactions Law.

A. Pendahuluan

Digitalisasi ekonomi telah mengubah pola masyarakat dalam melakukan pembayaran. Pembayaran tidak lagi hanya dilakukan dengan uang tunai atau instrumen perbankan konvensional, melainkan melalui aplikasi, dompet digital, transfer elektronik, dan pemindaian kode *Quick Response* (QR). Dalam konteks Indonesia, Bank Indonesia bersama industri sistem pembayaran mengembangkan QRIS sebagai standar nasional QR Code pembayaran. Standardisasi tersebut dimaksudkan untuk mendorong interoperabilitas antarpelaku jasa pembayaran dan memudahkan transaksi konsumen maupun pedagang.

Penggunaan kode QR menghadirkan efisiensi: pengguna cukup memindai kode yang tersedia, memeriksa identitas penerima dan nominal, lalu mengonfirmasi transaksi melalui aplikasi pembayaran. Akan tetapi, kesederhanaan mekanisme tersebut juga menciptakan kerentanan. Kode QR pada dasarnya merupakan representasi visual dari data atau instruksi elektronik. Apabila kode milik pedagang diganti, ditemplei dengan kode lain, dibuat menyerupai QRIS yang sah, atau dikirim kepada calon korban melalui media elektronik, pemindaian dapat mengarahkan pembayaran kepada rekening yang dikendalikan pelaku atau ke situs yang dirancang untuk mengambil data korban.

Penipuan kode QR palsu tidak cukup dipahami sebagai persoalan teknis. Perbuatan tersebut memuat dimensi hukum pidana, hukum informasi dan transaksi elektronik, hukum sistem pembayaran, serta perlindungan konsumen. Dimensi pidananya terlihat pada kehendak pelaku untuk memperoleh keuntungan secara melawan hukum melalui tipu muslihat. Dimensi elektroniknya timbul karena objek, sarana, dan jejak perbuatan berhubungan dengan informasi elektronik, dokumen elektronik, sistem elektronik, atau transaksi elektronik. Sementara itu, dimensi sistem pembayaran berkaitan dengan keandalan, keamanan, perlindungan pengguna, dan manajemen risiko pada penyelenggaraan pembayaran digital.

Persoalannya, peraturan perundang-undangan Indonesia belum merumuskan tindak pidana dengan istilah khusus "penipuan kode QR palsu". Ketidadaan nomenklatur khusus tidak semata berarti terdapat kekosongan hukum. Penilaian harus dilakukan dengan menguji unsur-unsur setiap modus terhadap norma pidana umum dan pidana khusus yang berlaku. Dengan demikian, fokus penelitian ini bukan sekadar mencari satu pasal yang menyebut QR code, melainkan membangun konstruksi hukum yang tepat untuk menilai penggunaan kode QR palsu sebagai modus penipuan digital.

Berdasarkan latar belakang tersebut, artikel ini mengkaji pertanyaan: **bagaimanakah pengaturan hukum terhadap penipuan kode QR palsu dalam transaksi elektronik di Indonesia?** Tujuannya adalah menjelaskan konstruksi regulasi yang dapat diterapkan, menemukan keterbatasan pengaturannya, serta merumuskan arah penguatan hukum dan kebijakan pencegahan.

B. Metodologi

Penelitian ini merupakan penelitian hukum normatif. Penelitian berfokus pada norma hukum yang mengatur perbuatan penipuan, informasi dan dokumen elektronik, transaksi elektronik, sistem pembayaran, serta perlindungan pengguna transaksi digital.

Pendekatan yang digunakan terdiri atas pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menelaah keterkaitan antara Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta regulasi Bank Indonesia mengenai standar nasional QR Code pembayaran dan penyelenggaraan sistem pembayaran. Pendekatan konseptual digunakan untuk memahami penipuan, pemalsuan atau manipulasi informasi elektronik, keamanan sistem pembayaran, dan kepastian hukum.

Bahan hukum primer berupa peraturan perundang-undangan dan regulasi terkait. Bahan hukum sekunder mencakup buku, artikel ilmiah, dan doktrin hukum pidana serta hukum siber. Pengumpulan bahan dilakukan melalui studi kepustakaan. Bahan dianalisis secara kualitatif dan preskriptif, yakni dengan menguraikan norma yang berlaku, membandingkan unsur-unsur delik dengan karakter perbuatan, lalu merumuskan rekomendasi hukum.

C. Hasil dan Pembahasan

Karakteristik Penipuan Kode QR Palsu

Kode QR adalah kode dua dimensi yang dapat menyimpan data dan dibaca melalui perangkat elektronik. Dalam pembayaran, kode tersebut dapat berisi identitas penerima, instruksi transaksi, tautan pembayaran, atau informasi lain yang diperlukan dalam proses pembayaran. QRIS merupakan standar nasional untuk QR Code pembayaran yang dikembangkan agar satu kode dapat menerima pembayaran dari berbagai aplikasi penyelenggara jasa sistem pembayaran.

Penipuan kode QR palsu dapat terjadi melalui beberapa pola. Pertama, pelaku mengganti kode QR milik pedagang dengan kode yang mengarahkan dana ke akun pelaku. Kedua, pelaku membuat kode QR yang menyerupai kode pembayaran resmi atau memanfaatkan tampilan yang menimbulkan kepercayaan palsu. Ketiga, pelaku menyebarkan kode QR melalui pesan singkat, media sosial, atau media lainnya dengan klaim adanya hadiah, tagihan, verifikasi akun, atau bantuan layanan. Keempat, kode QR digunakan untuk membawa korban ke laman palsu yang meminta kredensial, kode verifikasi, atau data pribadi.

Walaupun modusnya bervariasi, elemen pokok perbuatan umumnya terdiri atas: adanya rekayasa atau penggunaan data elektronik yang menyesatkan; adanya maksud memperoleh keuntungan atau manfaat secara tidak sah; adanya tindakan korban yang dipengaruhi oleh representasi palsu tersebut; serta adanya kerugian atau risiko kerugian bagi korban, pedagang, penyedia jasa pembayaran, atau pihak lain. Oleh sebab itu, QR code bukan satu-satunya objek analisis; ia merupakan sarana digital yang digunakan untuk mewujudkan tipu muslihat.

Pengaturan dalam Hukum Pidana Umum

Secara konseptual, penipuan merupakan perbuatan memperoleh keuntungan secara melawan hukum dengan menggerakkan orang lain melalui penggunaan identitas palsu, keadaan palsu, rangkaian kebohongan, atau tipu muslihat, sehingga orang tersebut menyerahkan sesuatu, membuat utang, atau menghapuskan piutang. Dalam modus kode QR palsu, pelaku membentuk tampilan atau instruksi pembayaran yang tidak benar agar korban menyetujui perpindahan dana. Hubungan antara tampilan palsu, kepercayaan korban, dan pengalihan dana menjadi inti pembuktian penipuan.

Sejak berlakunya Kitab Undang-Undang Hukum Pidana Nasional berdasarkan Undang-Undang Nomor 1 Tahun 2023, analisis harus merujuk pada ketentuan KUHP nasional yang berlaku dan tidak lagi semata-mata pada rumusan Pasal 378 KUHP lama. Namun demikian, struktur pokok tindak pidana penipuan tetap relevan secara doktrinal: adanya maksud

menguntungkan diri sendiri atau orang lain secara melawan hukum dan penggunaan cara-cara menyesatkan untuk menggerakkan korban melakukan perbuatan yang merugikan dirinya.

Penerapan ketentuan penipuan pada kasus kode QR palsu membutuhkan pembuktian yang cermat. Penuntut harus menunjukkan, antara lain, bahwa kode yang digunakan bukan kode yang sah milik pedagang atau penerima yang diinformasikan kepada korban; pelaku mengetahui atau menghendaki ketidakbenaran tersebut; korban melakukan transaksi karena percaya pada representasi yang diciptakan; dan dana atau manfaat lain beralih kepada pelaku atau pihak yang dikendalikannya. Bukti transaksi, rekaman kamera pengawas, keterangan saksi, catatan akun, alamat IP, komunikasi digital, dan pemeriksaan forensik perangkat dapat berperan penting dalam membangun hubungan kausal tersebut.

Ketentuan penipuan dalam KUHP tepat digunakan apabila pusat perbuatannya adalah penggerakan korban melalui tipu muslihat hingga korban melakukan pembayaran. Akan tetapi, karakter digital dari QR code sering kali melibatkan manipulasi informasi elektronik. Karena itu, penipuan umum perlu dibaca bersama ketentuan pidana khusus dalam UU ITE.

Pengaturan dalam UU ITE

UU ITE membentuk dasar hukum bagi pengakuan informasi elektronik, dokumen elektronik, transaksi elektronik, dan sistem elektronik. Undang-undang tersebut juga mengatur sejumlah larangan yang relevan terhadap tindakan tanpa hak, manipulasi, penciptaan, perubahan, penghilangan, perusakan, atau penyebaran informasi dan/atau dokumen elektronik tertentu.

Dalam konteks kode QR palsu, salah satu ketentuan yang sangat relevan ialah larangan terhadap perbuatan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi atau dokumen itu dianggap seolah-olah data yang otentik. Norma tersebut dapat digunakan ketika pelaku menciptakan QR code, identitas merchant, halaman pembayaran, atau tampilan digital yang tidak sah tetapi dibuat sedemikian rupa agar korban meyakini sebagai instrumen pembayaran yang autentik. Sanksi terhadap pelanggaran norma ini diatur dalam ketentuan pidana UU ITE.

Perlu ditegaskan bahwa tidak setiap kasus penipuan QR otomatis harus dipidana hanya dengan satu pasal UU ITE. Kualifikasi bergantung pada modus konkret. Jika pelaku hanya memanfaatkan rangkaian kebohongan untuk membujuk korban membayar, ketentuan penipuan mungkin lebih dominan. Jika pelaku menciptakan atau memanipulasi data elektronik agar tampak otentik, ketentuan manipulasi informasi atau dokumen elektronik menjadi sangat relevan. Jika perbuatan dilanjutkan dengan akses tanpa hak terhadap akun atau sistem, intersepsi, pengubahan data, atau perusakan sistem, ketentuan lain dalam UU ITE dapat pula dipertimbangkan sesuai unsur perbuatannya.

Perubahan UU ITE dan peralihan sebagian ketentuan ke KUHP Nasional menuntut kehati-hatian dalam mengutip dasar hukum. Analisis hukum tidak boleh menggunakan pasal yang telah dicabut, diubah, atau dialihkan tanpa memeriksa status keberlakuannya. Prinsip legalitas mengharuskan penegak hukum dan peneliti mengaitkan suatu perbuatan dengan rumusan delik yang berlaku pada waktu perbuatan dilakukan, termasuk ketentuan peralihan yang relevan.

Regulasi Sistem Pembayaran dan QRIS

Hukum pidana berorientasi pada penindakan terhadap pelaku, sedangkan regulasi sistem pembayaran berorientasi pula pada pencegahan risiko dan perlindungan ekosistem. Bank Indonesia memiliki kewenangan mengatur dan menjaga kelancaran sistem pembayaran. Dalam kerangka ini, QRIS ditempatkan sebagai standar nasional QR Code untuk pembayaran yang mendukung interoperabilitas sekaligus standardisasi tata kelola.

Pengaturan QRIS penting dalam penipuan kode QR palsu karena menyediakan konteks mengenai kode yang sah, pihak yang berwenang menyelenggarakan layanan, identitas merchant, tata kelola keamanan, dan penanganan pengaduan. Penyelenggara jasa sistem pembayaran perlu menerapkan prinsip kehati-hatian, manajemen risiko, keamanan sistem, perlindungan konsumen, dan mekanisme penanganan insiden. Pedagang juga mempunyai kepentingan untuk memastikan kode pembayaran yang dipajang berasal dari penyedia yang berizin dan tidak mengalami penggantian secara fisik maupun digital.

Meskipun demikian, standar sistem pembayaran tidak menggantikan hukum pidana. Pengaturan administrasi dan manajemen risiko berfungsi mencegah serta memulihkan gangguan dalam sistem pembayaran. Ketika terdapat unsur kesengajaan, tipu muslihat, manipulasi data, dan pengambilan keuntungan secara melawan hukum, maka tindakan tersebut memasuki wilayah pertanggungjawaban pidana. Karena itu, respons terhadap QR code palsu harus bersifat

terintegrasi: pencegahan teknis, pengawasan penyelenggara, edukasi pengguna, mekanisme pengaduan, pemulihan kerugian yang memungkinkan, dan penegakan hukum terhadap pelaku.

Perlindungan Konsumen dan Kepastian Hukum

Pengguna layanan pembayaran digital berada dalam posisi yang dapat dirugikan oleh asimetri informasi. Konsumen sering tidak memiliki kemampuan untuk menilai secara teknis apakah kode QR yang dipindai benar-benar terhubung dengan merchant atau penerima yang sah. Perlindungan konsumen karena itu tidak cukup hanya dibebankan kepada kehati-hatian pengguna. Pelaku usaha, penyelenggara jasa sistem pembayaran, dan pihak yang membangun antarmuka transaksi harus memperhatikan keamanan, transparansi informasi, saluran pengaduan, dan penanganan insiden.

Kepastian hukum terhadap penipuan QR palsu harus dibangun melalui dua lapis pendekatan. Pertama, kepastian pada tahap kualifikasi tindak pidana: aparat perlu memiliki pedoman yang membedakan penipuan biasa, manipulasi dokumen elektronik, akses tanpa hak, dan perbuatan lain yang mungkin menyertai modus QR palsu. Kedua, kepastian pada tahap perlindungan pengguna: konsumen perlu mengetahui prosedur verifikasi penerima, cara pelaporan, batas tanggung jawab para pihak, serta tindakan awal ketika menemukan kode yang mencurigakan.

Ketiadaan delik dengan istilah spesifik “penipuan kode QR palsu” bukan alasan untuk membiarkan pelaku bebas dari pertanggungjawaban. Namun, fragmentasi norma dapat memunculkan variasi penerapan dan kesulitan pembuktian. Oleh sebab itu, diperlukan harmonisasi antara hukum pidana, UU ITE, regulasi sistem pembayaran, dan perlindungan konsumen. Harmonisasi dapat dilakukan melalui pedoman penegakan hukum, penguatan standar autentikasi merchant, sistem pelaporan cepat lintas penyelenggara, serta rumusan kebijakan yang mengakui karakter khas kejahatan pembayaran berbasis QR.

Arah Penguatan Pengaturan

Penguatan pengaturan hukum terhadap penipuan kode QR palsu perlu ditempuh melalui beberapa arah. Pertama, otoritas dan penegak hukum perlu membangun pedoman klasifikasi modus. Pedoman itu harus menjelaskan indikator pembeda antara penggantian QR fisik, pembuatan QR digital palsu, phishing berbasis QR, dan pengambilalihan akun yang menggunakan QR sebagai pintu masuk.

Kedua, penyelenggara sistem pembayaran perlu memperkuat autentikasi penerima pembayaran. Identitas merchant dan nama penerima harus ditampilkan secara jelas sebelum pengguna memberikan persetujuan akhir. Fitur pelaporan kode mencurigakan, pembekuan cepat rekening tujuan yang terindikasi fraud sesuai prosedur hukum, serta pertukaran informasi insiden perlu dikembangkan secara terukur dan akuntabel.

Ketiga, edukasi publik harus diarahkan pada tindakan yang konkret: memeriksa nama merchant/penerima dan nominal sebelum mengonfirmasi transaksi; menghindari pemindaian kode dari sumber tidak terpercaya; tidak memasukkan kredensial atau kode verifikasi pada tautan yang dibuka dari QR mencurigakan; serta segera menyimpan bukti dan menghubungi penyedia jasa pembayaran bila terdapat transaksi tidak dikenal.

Keempat, pembaruan hukum perlu mempertimbangkan perkembangan teknologi tanpa menciptakan kriminalisasi berlebihan. Perumusan norma yang terlalu sempit berisiko cepat tertinggal oleh modus baru, sedangkan norma yang terlalu luas dapat mengganggu kepastian hukum. Pilihan yang lebih proporsional adalah mempertahankan delik yang berbasis pada unsur penipuan, manipulasi data elektronik, akses tanpa hak, dan kerugian, lalu melengkapinya dengan pedoman interpretasi serta standar keamanan sektoral yang adaptif.

D. Kesimpulan

Pengaturan hukum terhadap penipuan kode QR palsu dalam transaksi elektronik di Indonesia bersifat tersebar dan saling melengkapi. KUHP memberikan dasar untuk menilai perbuatan yang menggerakkan korban menyerahkan uang atau manfaat melalui tipu muslihat dengan maksud memperoleh keuntungan secara melawan hukum. UU ITE relevan ketika modus dilakukan melalui penciptaan, manipulasi, perubahan, atau penggunaan informasi dan/atau dokumen elektronik agar tampak otentik, maupun ketika disertai bentuk kejahatan siber lain sesuai unsur yang terbukti. Di sisi lain, regulasi Bank Indonesia mengenai sistem pembayaran dan QRIS memberikan kerangka pencegahan melalui standardisasi, keamanan, manajemen risiko, dan perlindungan pengguna.

Indonesia belum memiliki rumusan delik yang secara eksplisit dinamai “penipuan kode QR palsu”. Namun, keadaan tersebut tidak menunjukkan ketiadaan hukum karena modus tersebut dapat dijangkau oleh norma penipuan dan norma elektronik yang berlaku berdasarkan karakter perbuatan konkret. Tantangan utamanya terletak pada fragmentasi aturan, dinamika perubahan regulasi, pembuktian digital, dan kebutuhan respons cepat untuk mengurangi kerugian korban.

Penguatan hukum perlu dilakukan melalui harmonisasi penerapan KUHP dan UU ITE, pedoman kualifikasi modus penipuan QR, penguatan keamanan dan autentikasi dalam sistem pembayaran, mekanisme pengaduan serta respons insiden yang efektif, dan literasi keamanan digital bagi konsumen maupun pedagang. Dengan pendekatan tersebut, hukum tidak hanya berfungsi menindak pelaku setelah kerugian terjadi, tetapi juga mencegah penggunaan teknologi pembayaran sebagai sarana kejahatan.

E. Referensi

- Bank Indonesia. (2019). *Peraturan Anggota Dewan Gubernur Nomor 21/18/PADG/2019 tentang Implementasi Standar Nasional Quick Response Code untuk Pembayaran*.
- Bank Indonesia. (2021). *Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran*.
- Kitab Undang-Undang Hukum Pidana. Undang-Undang Nomor 1 Tahun 2023.
- Marzuki, P. M. (2021). *Penelitian Hukum*. Kencana.
- Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Rineka Cipta.
- Mulyadi, L. (2022). *Hukum Pidana Siber: Perlindungan Hukum terhadap Kejahatan di Ruang Digital*. Alumni.
- Republik Indonesia. (1999). Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
- Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Soekanto, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Pers.
- Yahya, A. M. (2020). *Hukum Pidana di Bidang Teknologi Informasi*. Sinar Grafika.