Vol. 07, No. 2 2025, pp. 3856 – 3866

Sultra Law Review

Vol. 07, No. 02 Oktober 2025
ISSN: 2685-208X (Online)
Publisher: Fakultas Hukum Universitas Sulawesi Tenggara
Website: https://jurnal-unsultra.ac.id/index.php/sulrev

PERTANGGUNGJAWABAN PIDANA TERHADAP PENIPUAN KODE QR PALSU DALAM TRANSAKSI ELEKTRONIK (Studi di Polres Kendari)

Leni

Fakultas Hukum Universitas Sulawesi Tenggara

ARTICLE INFO

Keywords:
Criminal liability, Electronic transactions, Fake QR code, Kendari Police Department, QR code fraud

e-mail:
leni67@gmail.com

Corresponding Author:
Leni

Received:15/02/2025
Accepted:27/08/2025
Published:31/10/2025

ABSTRACT

This study investigates the phenomenon of fraud involving counterfeit QR codes in electronic transactions in Indonesia, alongside the associated legal implications and criminal liabilities of the offenders. The implementation of QRIS, developed by Bank Indonesia, has significantly accelerated the digitalization of the national payment system. A comprehensive legal analysis, utilizing the Indonesian Criminal Code (KUHP), the Information and Electronic Transactions Law (UU ITE), and Bank Indonesia regulations, reveals that perpetrators are subject to severe criminal penalties, including imprisonment of up to 12 years, multi-billion rupiah fines, and mandatory restitution to victims. Enforcement challenges include difficulties in identifying offenders due to the use of false identities and accounts, coupled with inadequate public awareness regarding the verification of QR codes prior to transaction execution. This research employs a descriptive-analytical methodology, The study recommends enhanced public education, bolstered digital security technologies, and the revision of pertinent regulations to effectively combat QR code–related fraud. In conclusion, counterfeit QR code fraud poses a significant legal challenge that necessitates coordinated efforts among legislators, law enforcement authorities, and the public to maintain the security and trustworthiness of digital transaction systems.

I. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi membawa dampak besar dalam berbagai aspek kehidupan, terutama pada sektor ekonomi dan sistem transaksi keuangan. Salah satu inovasi yang menjadi tren baru adalah penggunaan kode QR (Quick Response) sebagai metode pembayaran elektronik. Di Indonesia, sistem ini dikenal sebagai QRIS (Quick Response Code Indonesian Standard). Menurut informasi dari Bank Indonesia, QRIS merupakan integrasi berbagai jenis QR Code dari berbagai Penyelenggara Jasa Sistem Pembayaran (PJSP) untuk memudahkan transaksi masyarakat. QRIS disusun oleh industri pembayaran bersama Bank Indonesia agar penggunaan QR Code dapat berlangsung lebih sederhana, cepat, dan aman. Setiap penyelenggara jasa sistem pembayaran yang ingin mengimplementasikan QR Code kini diwajibkan mengikuti standar QRIS.

Dengan adanya QRIS, semua aplikasi pembayaran, baik dari bank maupun non-bank, bisa digunakan secara universal di berbagai lokasi seperti toko, pedagang kecil, warung, area parkir, destinasi wisata, hingga platform donasi, asalkan tersedia logo QRIS. Artinya, konsumen tidak perlu khawatir jika aplikasi pembayaran yang dimiliki berbeda dengan penyedia layanan QRIS yang digunakan oleh merchant. Para pedagang hanya perlu membuka rekening atau akun di salah satu penyedia QRIS resmi berlisensi Bank Indonesia, setelah itu mereka dapat menerima pembayaran digital dari berbagai aplikasi pembayaran yang sudah terkoneksi.

Teknologi kode QR menawarkan efisiensi, kecepatan, serta meminimalisasi ketergantungan pada uang tunai, sehingga memberikan nilai praktis bagi pelaku usaha maupun konsumen. Namun, meningkatnya penggunaan QR code juga menimbulkan tantangan berupa penyalahgunaan dalam bentuk kejahatan siber. Salah satu modus yang marak adalah pemalsuan kode QR. Dalam praktiknya, pelaku kriminal dapat memanipulasi kode QR sehingga pembayaran dialihkan ke rekening yang salah atau bahkan digunakan untuk mencuri data pribadi korban. Modus penipuan ini kerap mereplikasi identitas penjual, produk, dan total jumlah transaksi seolah-olah sah, sehingga pembeli secara tidak sadar mentransfer dana ke pelaku penipuan.

Kejahatan ini jelas merugikan konsumen dan pelaku usaha, serta mengikis kepercayaan masyarakat terhadap sistem pembayaran nontunai. Karena itu, masalah pemalsuan kode QR tidak hanya soal teknologi, tetapi juga aspek hukum. Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), pemalsuan kode QR dapat dikategorikan sebagai perbuatan kriminal. Pasal 35 jo. Pasal 51 ayat (1) UU ITE melarang individu membuat, mendistribusikan, atau menggunakan informasi elektronik dan/atau dokumen elektronik yang tidak sah dengan niat menipu atau merugikan pihak lain. Pelanggaran ini diancam dengan pidana penjara hingga 12 tahun dan/atau denda maksimal Rp12 miliar.

Selain itu, tindakan penipuan melalui kode QR palsu juga dapat dikenakan pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP). Pasal 378 KUHP mengatur tindak pidana penipuan dengan ancaman hukuman penjara hingga empat tahun. Dengan demikian, pelaku pemalsuan QR code bisa dijerat melalui kombinasi instrumen hukum yang berlaku, baik UU ITE maupun KUHP. Kasus ini memperlihatkan bahwa perkembangan teknologi digital selalu beriringan dengan modus kejahatan baru, sehingga perlu sikap waspada dari masyarakat.

Deputi Gubernur Bank Indonesia, Filianingsih Hendarta, menekankan bahwa platform QRIS dirancang dengan standar keamanan nasional dan praktik global terbaik. Menurutnya, “QRIS keamanannya itu tanggung jawab bersama. BI, ASPI [Asosiasi Sistem Pembayaran Indonesia] dan pelaku industri PJP [Perusahaan Jasa Penilai] selalu melakukan sosialisasi dan edukasi terkait keamanan transaksi QRIS kepada para merchant.” Hal ini menunjukkan bahwa keamanan digital bukan hanya tugas regulator, tetapi juga memerlukan partisipasi aktif dari penyedia layanan dan pelaku usaha.

Dari perspektif hukum pidana, penggunaan kode QR palsu menimbulkan persoalan serius mengenai bentuk pertanggungjawaban pidana. Pertanyaan yang muncul adalah bagaimana sistem hukum Indonesia mengklasifikasikan tindak pidana tersebut dan hukuman apa yang paling tepat untuk pelaku. Urgensi pengaturan ini terletak pada perlindungan konsumen dan penciptaan kepastian hukum di era ekonomi digital yang semakin kompleks.

Kerangka hukum di Indonesia sesungguhnya sudah memiliki perangkat yang cukup kuat untuk menindak pelaku kejahatan siber. UU ITE, KUHP, serta berbagai regulasi terkait perlindungan konsumen sudah mengatur tentang pemalsuan data elektronik, penipuan, serta perlindungan masyarakat dari praktik kejahatan daring. Meski demikian, hingga kini belum ada aturan spesifik yang mengatur secara terperinci tentang kejahatan penggunaan QR code palsu dalam transaksi

pembayaran. Kekosongan hukum ini menimbulkan tantangan bagi aparat penegak hukum, sehingga penelitian dan kajian lebih lanjut dianggap sangat penting.

Dengan meningkatnya penggunaan QRIS dan pesatnya perkembangan dunia digital, penelitian mengenai pertanggungjawaban pidana pelaku penggunaan QR palsu menjadi krusial sebagai langkah preventif. Kajian ini tidak hanya bermanfaat bagi pembentukan kebijakan hukum baru, tetapi juga diperlukan untuk memberikan kepastian hukum dan perlindungan optimal bagi masyarakat pengguna layanan pembayaran digital.

II. TINJAUAN PUSTAKA

Hukum pidana memainkan peran esensial dalam menjaga ketertiban dan keadilan di masyarakat. Dua konsep utama yang menjadi pondasi penegakan hukum pidana modern adalah pertanggungjawaban pidana dan definisi tindak pidana. Kedua konsep ini, yang diatur dan dikembangkan melalui undang-undang serta doktrin para ahli, sangat berkaitan dengan pengaturan sanksi pidana, di mana hak dan kewajiban individu sebagai warga negara diuji secara legal dan moral. Dalam era kemajuan teknologi dan digitalisasi, pembayaran berbasis kode QR dan transaksi elektronik menambah kompleksitas regulasi hukum pidana, khususnya terkait cybercrime dan penipuan berbasis elektronik.

A. Pertanggungjawaban Pidana: Konsep dan Landasannya

Pertanggungjawaban pidana atau criminal responsibility merupakan suatu mekanisme yuridis untuk menilai apakah seseorang layak dijatuhi pidana atas perbuatan yang telah dilakukan. Sejalan dengan Pasal 3 Rancangan KUHP, tanggung jawab pidana merupakan konsekuensi dari penilaian objektif terhadap tindak pidana secara hukum. Esensi dari konsep ini adalah bahwa pelaku dapat dijatuhi pidana apabila memenuhi syarat yang ditentukan undang-undang: adanya unsur kesalahan berupa niat jahat maupun kelalaian.

Pasal 27 konsep KUHP menegaskan bahwa pertanggungjawaban pidana terjadi ketika terdapat celaan objektif terhadap perbuatan yang melanggar hukum, yang kemudian dialamatkan secara subjektif kepada individu yang memenuhi syarat untuk dijatuhi pidana. Artinya, tindak pidana baru bermakna manakala disertai pertanggungjawaban pidana; tidak setiap pelaku tindak pidana merupakan objek yang bisa dijatuhi hukuman. Dalam istilah hukum Belanda, pertanggungjawaban pidana dikenal dengan istilah aansprakelijk (bertanggung jawab), verantwoordelijk (dapat dimintai pertanggungjawaban), dan toerekenbaar (perbuatan yang dapat dipertanggungjawabkan). Pompee menegaskan bahwa yang seharusnya menjadi fokus ialah pada perbuatan, bukan pada subjeknya.

Romli Atmasasmita dalam pengkajian filosofisnya, memperluas makna liability sebagai suatu situasi yang mana seseorang dapat diminta pertanggungjawaban secara legal atas ekses dari perbuatan tertentu. Perkembangan konsep liability atau pertanggungjawaban menunjukkan pergeseran dari sekadar mekanisme pembalasan menjadi kewajiban sosial untuk menjaga dan mengembalikan keseimbangan masyarakat.

Penting pula untuk mengenal istilah-istilah hukum lain yang bermakna tindak pidana, seperti perbuatan melawan hukum, pelanggaran pidana, perbuatan yang boleh dihukum, serta perbuatan yang dapat dihukum. Menurut R. Soesilo, tindak pidana adalah perbuatan yang dilarang atau diwajibkan oleh hukum. Moeljatno dan Simons menambahkan bahwa tindak pidana adalah perbuatan bertentangan dengan hukum yang dilakukan oleh orang yang dapat dipertanggungjawabkan, yang karenanya dikenakan sanksi.

Dogmatik hukum pidana memandang ada tiga aspek utama, yaitu: tindakan yang dilarang, individu pelaku, dan ancaman hukuman pidana. Pasal-pasal Kitab Undang-Undang Hukum Pidana (KUHP)

mengadopsi istilah “straafbaarfeit” (perbuatan yang dapat dihukum), walaupun tanpa definisi literal, namun dalam doktrin dijelaskan sebagai “kenyataan hukum yang dapat dihukum”.

Hazewinkel Suringa memaknai “straafbaarfeit” sebagai perilaku manusia yang tidak dapat diterima masyarakat sehingga harus dihapuskan melalui sanksi pidana. Berbagai pendapat ahli seperti Van Hamel, Pompe, dan Simons menyepakati bahwa perbuatan pidana adalah pelanggaran hukum yang dilakukan subjek hukum yang mampu dimintai pertanggungjawabannya, dengan ancaman sanksi dalam sistem pidana.

Prinsip dasar yang dipegang dalam penjatuhan pidana adalah “Nulla poena sine culpa” (tidak ada hukuman tanpa kesalahan). Maka, syarat utama penjatuhan pidana adalah adanya kemampuan bertanggung jawab, yang secara psikologis dapat diuji menurut pendapat Simons, Van Hamel, dan Van Bemmelen. Sudikno Mertokusumo menegaskan, kejahatan terdiri dari perbuatan manusia yang bersifat melawan hukum, menimbulkan akibat merugikan, dan dilakukan dalam kondisi tertentu yang menguatkan karakter pidana.

Batasan-batasan konseptual ini tetap relevan dalam berbagai tantangan hukum pidana kontemporer, seperti munculnya tindak pidana siber, penipuan elektronik, dan kejahatan berbasis digital, yang menuntut pembuktian kesalahan dan kemampuan bertanggung jawab secara spesifik.

B. Tindak Pidana Penipuan: Norma, Unsur, dan Variasinya

Tindak pidana penipuan atau bedrog diatur dalam Pasal 378 s.d. 395 KUHP. Penipuan, dalam pengertian yuridis, mencakup segala tindakan yang dilakukan dengan memberikan gambaran palsu atau menyesatkan dengan tujuan memperoleh keuntungan secara melawan hukum.

Menurut KBBI, penipuan adalah tindakan memperdaya, memberikan informasi palsu agar pihak lain dirugikan dan pelaku diuntungkan. Adapun Pasal 378 KUHP menyatakan: “Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu, sifat palsu atau tipu muslihat, maupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang, membuat utang, atau menghapuskan piutang, diancam dengan pidana penjara paling lama empat tahun.”

Dalam rincian Soesilo, penipuan terdiri dari unsur merayu atau membujuk dengan tujuan menguasai barang milik orang lain. Unsur diskriptif penipuan menurut Pasal 378 antara lain: memakai nama palsu, menggunakan kedudukan palsu, tipuan atau rangkaian kebohongan, penyerahan barang, pembentukan hutang/penghilangan hutang, dan adanya niat menguntungkan diri sendiri/ orang lain secara melawan hukum.

Unsur subjektifnya mencakup adanya tujuan tertentu dan niat mencoba atau berhasil mendapatkan keuntungan (profitable intent) melalui cara-cara yang tidak sah secara hukum. Bila alat penggerak adalah kebohongan, identitas palsu, atau rekayasa lain yang bertentangan dengan norma masyarakat umum, dan keuntungan yang didapat cacat hukum, maka tindakan tersebut dikualifikasikan sebagai penipuan.

Adapun Pasal 379 KUHP mengatur penipuan ringan, yakni penipuan berobjek barang (non-ternak) yang nilainya di bawah dua ratus lima puluh rupiah, diancam penjara tiga bulan atau denda tertentu.

Perlu diperhatikan bahwa KUHP memberikan ruang untuk pengaturan lebih lanjut dalam dua puluh pasal terkait penipuan, seperti Pasal 379a (gagal bayar saat pembelian), Pasal 380 ayat (1) (pemalsuan identitas, karya cipta), hingga Pasal 393bis (penipuan dalam konteks hukum/peran pengacara). Variasi penipuan lainnya termasuk penipuan asuransi (Pasal 381, 382), praktik

persaingan tidak sehat (Pasal 383bis), jual-beli barang palsu (Pasal 383), penipuan kontrak (Pasal 387), penipuan barang militer (Pasal 388), dan hoax (Pasal 390).

Dengan berkembangnya masyarakat dan semakin kompleksnya modus penipuan, pemerintah pun mengeluarkan payung hukum khusus melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), sebagai payung hukum bagi kejahatan siber dan penipuan berbasis teknologi. Inovasi ini menjawab kebutuhan hukum kontemporer, terutama dalam ranah transaksi dan pembayaran digital yang rentan memunculkan penipuan berbasis teknologi.

C. Metode Pembayaran Kode QR: Transformasi Transaksi Era Digital

Perkembangan teknologi membawa fenomena baru, yakni pembayaran berbasis kode QR (Quick Response code). Kode QR memudahkan transaksi dengan sistem pembayaran cashless, memanfaatkan perangkat telepon pintar sebagai alat autentikasi dan transfer dana.

Kode QR adalah kode batang dua dimensi yang dapat menyimpan informasi pembayaran, yang saat dipindai memungkinkan transaksi cepat tanpa perlu uang tunai atau kartu fisik. Dua bentuk utama penggunaan QR Code pada transaksi adalah Merchant-Presented Mode (merchant menampilkan QR, pelanggan memindai) dan Customer-Presented Mode (pelanggan menampilkan QR, merchant memindai). Keunggulan sistem pembayaran ini antara lain:

a) Kemudahan penggunaan
b) Aksesibilitas meluas, tidak memerlukan EDC mahal
c) Kecepatan transaksi, tidak memerlukan pertukaran fisik uang atau kartu
d) Keamanan lebih baik karena data tidak langsung terekspos
e) Dukungan autentikasi berlapis seperti fingerprint, face scan, atau kode OTP

Penetrasi pembayaran QR sangat masif di Tiongkok (Alipay, WeChat Pay) dan India (UPI), serta diadopsi secara strategis di Indonesia melalui standar QRIS (Quick Response Code Indonesian Standard) hasil kerja sama industri sistem pembayaran dan Bank Indonesia.

QRIS mengintegrasikan berbagai penyedia layanan pembayaran QR dan memastikan semua aplikasi pembayaran yang berlogo QRIS dapat diterima lintas merchant di Indonesia. Misalnya, pemilik warung di Banjarmasin cukup mengaktifkan akun di satu penyelenggara QRIS; masyarakat bisa membayar memakai aplikasi mana saja, meski penyelenggaranya berbeda.

Penerapan QRIS membawa manfaat berupa percepatan digitalisasi UMKM, kemudahan pembayaran di sektor informal, efisiensi, dan keamanan yang lebih baik. Namun tetap ada tantangan, misalnya ketergantungan pada koneksi internet dan risiko keamanan siber lewat duplikasi kode atau phishing. Secara keseluruhan, keberadaan QR code payment mempercepat transformasi sistem pembayaran nasional menuju transaksi nontunai berbasis digital, sejalan dengan kebijakan Bank Indonesia.

D. Transaksi Elektronik: Definisi, Skema, dan Perlindungan Hukumnya

Transaksi elektronik adalah proses transfer informasi, data, atau nilai ekonomi antar pihak melalui sarana elektronik atau internet, tanpa memerlukan interaksi fisik atau dokumen kertas. Bentuk transaksinya antara lain: e-commerce, transfer uang elektronik, pembayaran tagihan, e-banking, kartu kredit/debit, dompet digital, transfer bank online, hingga cryptocurrency.

Transaksi elektronik telah menjadi tulang punggung perekonomian digital dan bagian dari kehidupan sehari-hari masyarakat Indonesia. Penerapannya bisa ditemukan pada pembayaran toko online, pembayaran listrik melalui aplikasi, transfer dana via e-wallet, dan lain-lain.

Pengaturan transaksi elektronik di Indonesia diatur dalam Undang-Undang No. 11 Tahun 2008 yang kemudian diperbaharui menjadi Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE menetapkan asas-asas penting, yaitu:

a) Kepastian hukum: segala transaksi digital harus diakui dan dilindungi secara hukum,
b) Asas manfaat: teknologi digital dipakai untuk sebesar-besarnya kemaslahatan masyarakat,
c) Asas kehati-hatian: penggunaan teknologi harus penuh pertimbangan risiko
d) Asas iktikad baik: transaksi elektronik tidak boleh digunakan untuk merugikan pihak lain,
e) Asas kebebasan memilih teknologi: tidak membatasi penggunaan satu jenis teknologi saja,

Tujuan utama pengaturan ini antara lain untuk mencerdaskan kehidupan bangsa dalam sistem informasi global, mengembangkan perdagangan dan perekonomian nasional, meningkatkan efektivitas pelayanan publik, serta memberi rasa aman dan kepastian hukum bagi semua pihak yang bertransaksi secara elektronik.

Namun demikian, kemajuan transaksi elektronik memicu tantangan baru, mulai dari penyalahgunaan data pribadi dan maraknya penipuan siber, hingga kebutuhan pembuktian digital dalam proses penegakan hukum pidana. Dorongan penerapan prinsip-prinsip pertanggungjawaban pidana yang adaptif dan responsif pun makin mendesak diterapkan di era transaksi digital.

III. METODE PENELITIAN

A. Lokasi Penelitian

Penyusunan skripsi ini penulis memilih lokasi penelitian di Polres Kendari guna mendapatkan informasi mengenai pengaturan hukum transaksi elektronik.

B. Jenis dan Sumber Data

Dalam penelitian ini, materi yang dijadikan sumber informasi adalah data sekunder. Data sekunder merujuk pada informasi yang telah dikumpulkan dengan tujuan yang berbeda dari yang diperlukan untuk menyelesaikan permasalahan yang sedang dihadapi. Dalam penelitian ini, sumber data sekunder yang digunakan meliputi berbagai literatur, artikel, jurnal, serta situs web yang relevan dengan topik penelitian yang sedang dilaksanakan.

C. Teknik Pengumpulan Data

Metode yang akan diterapkan untuk pengumpulan data adalah studi pustaka atau dokumentasi. Studi pustaka atau dokumentasi adalah metode pengumpulan data yang tidak dilakukan secara langsung terhadap subjek penelitian. Dokumen dan pustaka yang telah diteliti berfungsi sebagai sumber bahan hukum primer, sekunder, dan tersier. Sumber-sumber ini ditemukan di berbagai tempat, termasuk perpustakaan, laboratorium hukum, serta melalui pencarian di internet. Kemudian, tahap berikutnya adalah melakukan inversi terhadap dokumen-dokumen atau materi hukum yang relevan.

D. Analisis Data

Dalam penelitian ini, metode analisis data yang diterapkan adalah metode deskriptif-analitis. Informasi yang diperoleh melalui kajian literatur dikumpulkan, diorganisir, dan disusun dalam struktur yang teratur, kategori, serta satuan penjelasan dasar. Data yang diperoleh dari studi ini dianalisis dengan pendekatan deskriptif. Sementara itu, informasi yang telah diolah disajikan dalam bentuk kualitatif

E. Waktu Penelitian

Penelitian ini dilakukan penulis dalam pengumpulan data yang dibutuhkan guna mendukung pembahasan adalah selama 3 bulan yaitu : bulan Januari-Maret 2025 melakukan penelitian lapangan dan menganalisis data.

IV. PEMBAHASAN

A. Penipuan Kode QR Palsu dalam Transaksi Elektronik di Indonesia: Kajian Hukum dan Pertanggungjawaban Pidana

Perkembangan teknologi informasi dan komunikasi telah menghadirkan banyak terobosan dalam kehidupan masyarakat modern, khususnya dalam bidang keuangan. Salah satu inovasi yang mendominasi sistem pembayaran digital di Indonesia ialah penggunaan Quick Response Code Indonesian Standard (QRIS). QRIS dicanangkan Bank Indonesia sebagai integrasi berbagai sistem QR yang ada agar mempermudah, mempercepat, dan menstandardisasi proses pembayaran. Dengan kepraktisan, kemudahan, serta keamanannya, QRIS telah menjadi pilihan utama baik bagi masyarakat maupun pelaku usaha di berbagai sektor, mulai dari usaha kecil menengah hingga lembaga keagamaan.

Namun, keberhasilan inovasi ini justru diikuti oleh munculnya modus-modus kejahatan baru. Di antaranya adalah penipuan menggunakan QR Code palsu yang berkembang pesat beberapa tahun terakhir. Kasus yang sering dijumpai adalah penggantian QR Code asli milik merchant atau rumah ibadah dengan QR palsu milik pelaku, sehingga dana hasil pembayaran atau donasi berpindah ke rekening penipu. Fenomena ini tidak hanya mengakibatkan kerugian finansial, tetapi juga menimbulkan masalah kepercayaan masyarakat dalam menggunakan instrumen pembayaran digital.

Kejahatan semacam ini menimbulkan implikasi hukum yang tidak sederhana. Oleh karena itu, penting untuk menguraikan bagaimana regulasi hukum Indonesia dapat diterapkan terhadap pelaku penipuan QR Code palsu serta apa bentuk pertanggungjawaban pidana yang mungkin dikenakan. Kajian ini mengambil dasar aturan KUHP, UU ITE, serta regulasi Bank Indonesia, dilengkapi dengan data empiris berupa wawancara dari aparat penegak hukum di Polres Kendari.

B. Kerangka Hukum yang Mengatur Penipuan QR Code Palsu

Dalam sistem hukum Indonesia, berbagai perangkat regulasi dapat digunakan untuk menjerat pelaku kejahatan penipuan digital, termasuk yang menggunakan QR Code palsu.

Pertama, Kitab Undang-Undang Hukum Pidana (KUHP) menjadi dasar utama. Pasal 378 KUHP dengan tegas mengatur bahwa siapa pun yang dengan maksud menguntungkan diri atau orang lain secara melawan hukum, menggunakan tipu muslihat, identitas palsu, atau rangkaian kebohongan untuk menggerakkan orang lain menyerahkan barang atau pembayaran, dapat dipidana penjara paling lama empat tahun. Rumusan pasal ini jelas relevan dengan modus penggantian QR Code atau manipulasi digital yang menyesatkan korban untuk menyerahkan uangnya. Selain itu, Pasal 362 KUHP tentang pencurian juga dapat menjerat pelaku jika tindakannya dikategorikan sebagai pengalihan dana secara tidak sah, dengan ancaman hukuman maksimal lima tahun.

Kedua, Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE), yaitu UU Nomor 11 Tahun 2008 yang telah diperbarui melalui UU Nomor 1 Tahun 2024, juga menjadi instrumen penting. Pasal 35 juncto Pasal 51 ayat (1) UU ITE mengatur bahwa setiap orang yang dengan sengaja memanipulasi, membuat, atau menyebarkan informasi elektronik palsu dengan tujuan menipu atau merugikan orang lain dapat dipidana dengan penjara maksimal 12 tahun dan/atau denda hingga

Rp12 miliar. Lebih lanjut, Pasal 28 ayat (1) UU ITE menegaskan larangan penyebaran informasi bohong dan menyesatkan yang berpotensi merugikan konsumen dalam transaksi elektronik.

Ketiga, Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Standar QRIS juga berperan fundamental. Regulasi ini menegaskan kewajiban penyelenggara jasa sistem pembayaran untuk mematuhi standar keamanan QRIS. Jika terjadi penyalahgunaan, bukan hanya pelaku individu yang dapat dituntut pidana, melainkan juga penyelenggara sistem bisa terancam sanksi administratif apabila terbukti lalai menjaga keamanan sistemnya.

Dengan tiga dasar hukum ini, sebenarnya perangkat regulasi yang ada dianggap cukup memadai untuk menjerat pelaku. Namun, dari hasil wawancara dengan penyidik kepolisian di Kendari, implementasinya masih menghadapi berbagai kendala.

C. Modus Kejahatan QR Code Palsu: Studi Kasus Lapangan

Berdasarkan wawancara dengan penyidik kriminal Polres Kendari, Aiptu Arif Setiawan, terdapat modus-modus populer yang digunakan para pelaku. Salah satu yang paling umum ialah penggantian QR Code asli dengan yang palsu. Pelaku mencetak QR modifikasi, lalu menempelkannya langsung menutupi kode asli pedagang, kafe, atau bahkan tempat ibadah. Hal ini tampak sederhana, namun sangat efektif dalam menipu korban. Seorang pemilik kafe di Kendari, misalnya, baru menyadari penipuan setelah dua hari tidak menerima pemasukan digital, padahal banyak pelanggan sudah membayar melalui QRIS. Setelah diperiksa, ternyata kode pembayaran telah diganti oleh pelaku. Kasus serupa juga terjadi di sejumlah masjid dengan tujuan pengalihan dana donasi.

Selain modus fisik, terdapat pula metode phishing melalui aplikasi palsu. Pelaku menyebarkan tautan aplikasi yang menyerupai dompet digital resmi. Sejumlah korban yang tertipu diarahkan mengunduh aplikasi tersebut. Setelah akun terhubung, pelaku bisa mengakses saldo dan mencuri dana secara langsung. Modus ini lebih berbahaya karena selain menimbulkan kerugian finansial, juga menyebabkan kebocoran data pribadi yang berharga.

Metode lain adalah penipuan berkedok investasi digital. Di sini, pelaku menjanjikan keuntungan tinggi dengan mengarahkan korban untuk melakukan transfer melalui QR Code tertentu. Namun setelah pembayaran dilakukan, korban tidak pernah menerima hasil investasi seperti yang dijanjikan.

D. Tantangan Penegakan Hukum

Meskipun regulasi sudah cukup jelas, pelaksanaannya menghadapi tantangan nyata di lapangan. *Pertama*, masyarakat masih kurang memahami cara memverifikasi QRIS. Banyak konsumen yang langsung memindai dan membayar tanpa meneliti apakah nama penerima sudah sesuai dengan merchant yang dituju.

Kedua, ada persoalan kesulitan penelusuran pelaku, terutama karena mereka sering memakai rekening atau identitas palsu. Kadang-kadang wilayah operasi pelaku lintas provinsi bahkan lintas negara, sehingga menyulitkan proses penyidikan. Dalam kasus tertentu, polisi tidak segera bisa mengikuti aliran dana, sebab rekening yang dipakai sering kali atas nama pihak ketiga yang tidak teridentifikasi.

Ketiga, belum ada regulasi yang spesifik mengenai QR Code palsu. Memang benar bahwa KUHP dan UU ITE sudah menyediakan dasar hukum yang relevan, tetapi karakteristik unik kejahatan QR Code memerlukan pasal khusus agar lebih jelas dan memberikan kepastian.

E. Pertanggungjawaban Pidana Pelaku Penipuan QR Code Palsu

Dalam hukum pidana, pertanggungjawaban berarti bahwa seseorang hanya dapat dihukum jika perbuatannya memenuhi unsur pidana, yakni adanya mens rea (niat jahat) serta actus reus (tindakan konkret). Dalam konteks QR Code palsu, unsur tersebut terpenuhi ketika pelaku secara sengaja memanipulasi kode atau aplikasi untuk menipu korban.

Dari sisi ancaman sanksi, bentuk pertanggungjawaban pidana yang melekat antara lain:

1. Pidana Penjara. Pasal 378 KUHP memberikan ancaman maksimal empat tahun. Pasal 35 jo. Pasal 51 ayat (1) UU ITE memungkinkan hukuman maksimal 12 tahun. Jika pelaku secara ilegal mengakses sistem elektronik, Pasal 30 UU ITE juga dapat digunakan dengan ancaman enam tahun.
2. Pidana Denda. Selain hukuman fisik, UU ITE juga memberi ruang penjatuhan denda hingga Rp12 miliar.
3. Restitusi atau ganti rugi kepada korban sebagaimana diatur dalam UU No. 31 Tahun 2014 tentang Perlindungan Saksi dan Korban. Kendati demikian, realisasi ganti rugi sering sulit karena pelaku kadang tidak punya aset yang bisa disita.

Faktor-faktor yang memengaruhi berat ringannya hukuman antara lain jumlah kerugian korban, peran pelaku (apakah sebagai aktor utama atau hanya perantara), serta ada tidaknya upaya pengembalian dana. Pelaku yang mengembalikan kerugian korban dapat memperoleh keringanan. Sebaliknya, jika pelaku bertindak sebagai otak skema penipuan, hukumannya lebih berat.

F. Hambatan Implementasi dan Upaya Pencegahan

Kendala besar dalam praktik hukum ialah kesulitan melacak pelaku yang menggunakan identitas fiktif dan rekening bengkok. Sebagian bahkan memakai dompet digital yang tidak memerlukan sistem verifikasi KYC (Know Your Customer). Selain itu, modus penipuan terus berkembang, misalnya malware yang bisa memodifikasi kode. Aparat penegak hukum harus selalu meningkatkan kemampuan digital forensik mereka agar bisa mengejar perkembangan tersebut.

Tidak kalah penting adalah masalah kesadaran masyarakat. Sebagian besar korban baru menyadari menjadi sasaran penipuan beberapa hari setelah transaksi, sehingga peluang pelaku melarikan dana semakin besar. Sebagai langkah pencegahan, Bank Indonesia dan Polres Kendari telah menggalakkan sosialisasi. Edukasi kepada pengguna QRIS untuk selalu memeriksa nama penerima sebelum konfirmasi pembayaran menjadi poin penting. Polisi Kendari juga mengimbau masyarakat untuk segera melapor jika menemukan kejanggalan. Selain itu, solusi yang dibutuhkan mencakup:

a) Peningkatan sistem keamanan digital dengan teknologi deteksi anomali.
b) Penguatan kerja sama antar lembaga seperti kepolisian, Otoritas Jasa Keuangan, Bank Indonesia, serta sektor perbankan.
c) Revisi regulasi agar mencantumkan norma khusus tentang kejahatan QR Code.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

1. Penipuan menggunakan kode QR palsu merupakan bentuk kejahatan siber yang semakin marak seiring dengan meningkatnya penggunaan metode pembayaran berbasis QRIS. Regulasi hukum di Indonesia telah mengatur tindakan ini melalui berbagai undang-undang, Meskipun regulasi yang ada cukup jelas, tantangan dalam penegakan hukum masih ditemukan, terutama dalam aspek identifikasi pelaku dan pelacakan transaksi yang dilakukan melalui rekening fiktif. Oleh karena itu, upaya pencegahan melalui edukasi masyarakat dan penguatan sistem keamanan digital menjadi hal yang sangat penting.

2. Pelaku penipuan kode QR palsu dapat dimintai pertanggungjawaban pidana berdasarkan hukum yang berlaku. Bentuk pertanggungjawaban pidana yang dapat dikenakan terhadap pelaku meliputi: Pidana Penjara, Pidana Denda, dan Restitusi kepada Korban, sebagai bentuk pemulihan kerugian akibat penipuan. Faktor yang mempengaruhi pertanggungjawaban pidana meliputi unsur kesengajaan pelaku, jumlah kerugian yang ditimbulkan, serta peran pelaku dalam kejahatan tersebut. Selain itu, tantangan utama dalam penegakan hukum adalah kesulitan dalam pelacakan identitas pelaku dan kurangnya kesadaran masyarakat dalam mengenali modus penipuan yang berkembang.

B. Saran

1. Pemerintah perlu mempertimbangkan penyusunan regulasi khusus yang lebih spesifik mengenai penipuan berbasis QR Code, mengingat metode pembayaran digital terus berkembang. Aparat penegak hukum perlu meningkatkan kemampuan digital forensik dalam menangani kasus kejahatan siber agar lebih efektif dalam mengidentifikasi dan menangkap pelaku. Selain itu Bank Indonesia dan OJK harus meningkatkan pengawasan terhadap transaksi yang mencurigakan serta memperketat kebijakan verifikasi akun pembayaran digital untuk mencegah penggunaan rekening fiktif oleh pelaku kejahatan.
2. Masyarakat perlu diberikan sosialisasi dan edukasi secara masif mengenai modus-modus penipuan QR Code palsu dan cara menghindarinya. Pengguna QRIS harus selalu memeriksa nama penerima transaksi sebelum melakukan pembayaran untuk memastikan dana dikirimkan ke rekening yang benar. Serta Pedagang dan pemilik usaha yang menggunakan QRIS harus rutin memeriksa kode QR yang dipasang di tempat usaha mereka untuk menghindari kemungkinan penggantian dengan QR Code palsu.

DAFTAR PUSTAKA

Atmasasmita, R. (2013). Sistem peradilan pidana kontemporer (Cet. 3). Jakarta: Kencana.

Chabris, C., & Simons, D. (2011). The invisible gorilla. HarperCollins.

Chabris, C., & Simons, D. (2011). The invisible gorilla. HarperCollins.

Hazewinkel, Suringa, D. (1953). Inleiding tot de studie van het Nederlandse strafrecht. Haarlem: H. D. Tjeenk Willink & Zoon N.V.

Lim, J. A. (2014). Pompe disease: from pathophysiology to therapy and back again. Orphanet Journal of Rare Diseases, 9, 85. https://doi.org/10.1186/s13023-014-0085-9

Mertokusumo, S. (2016). Teori hukum (Ed. revisi, Cet. 6). Yogyakarta: Cahaya Atma Pustaka.

Moeljatno, P. (2009). KUHP: Kitab Undang-Undang Hukum Pidana (Cetakan ke-28). Jakarta: Bumi Aksara.

Soesilo, R. (1995). Kitab undang-undang hukum pidana (KUHP): Bogor: Politeia.

Van Hamel, A. G. (1972). Sedjarah ilmu bahasa. Flores: Nusa Indah.

Peraturan Perundang-Undangan:

Indonesia, Kitab Undang-Undang Hukum Pidana

Indonesia, Kitab Hukum Acara Pidana

Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905

Bank Indonesia. (2020). Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Standar QRIS [Peraturan]. Jakarta: Bank Indonesia.

Republik Indonesia. (2014). Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 293. Jakarta: Sekretariat Negara.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 35 dan Pasal 51 ayat (1)