



Pertanggungjawaban Pidana terhadap Penggunaan Kode QR Palsu dalam Transaksi Elektronik di Indonesia

<u>INFO PENULIS</u>	<u>INFO ARTIKEL</u>
Niken Yulian Yusuf Universitas Sulawesi Tenggara nikenyyu@gmail.com Virya Suprayogi Yusuf Universitas Sulawesi Tenggara	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), 2924-2930.

Abstrak

Penggunaan *Quick Response Code* (QR Code) dalam transaksi elektronik, khususnya melalui *Quick Response Code Indonesian Standard* (QRIS), memberikan kemudahan, kecepatan, dan efisiensi bagi pelaku usaha maupun konsumen. Namun, perkembangan tersebut juga memunculkan modus kejahatan siber berupa penggunaan kode QR palsu. Modus tersebut antara lain dilakukan melalui penggantian kode QR asli milik merchant dengan kode QR pelaku, penyebaran aplikasi dompet digital palsu, phishing, dan penggunaan rekening atau akun pembayaran dengan identitas fiktif. Penelitian ini bertujuan menganalisis pertanggungjawaban pidana terhadap pelaku penggunaan kode QR palsu dalam transaksi elektronik di Indonesia. Penelitian menggunakan metode hukum empiris dengan pendekatan perundang-undangan dan pendekatan kasus. Data diperoleh melalui studi kepustakaan dan hasil wawancara dengan aparat kepolisian pada Polres Kendari, kemudian dianalisis secara deskriptif-kualitatif. Hasil penelitian menunjukkan bahwa pelaku dapat dimintai pertanggungjawaban pidana apabila terbukti melakukan perbuatan melawan hukum, mempunyai kemampuan bertanggung jawab, melakukan perbuatan dengan kesengajaan, serta tidak memiliki alasan penghapus pidana. Penggunaan QR Code palsu pada dasarnya dapat memenuhi unsur penipuan dan/atau manipulasi informasi atau dokumen elektronik. Bentuk pertanggungjawaban dapat berupa pidana penjara, pidana denda, serta pemulihan kerugian korban melalui restitusi sesuai ketentuan yang berlaku. Pembuktian perkara membutuhkan keterpaduan alat bukti konvensional dan bukti elektronik, seperti keterangan korban dan saksi, riwayat transaksi, identitas rekening penerima, rekaman kamera pengawas, serta pemeriksaan digital forensik. Hambatan utama penegakan hukum meliputi penggunaan identitas palsu, rekening penampung, lintas wilayah, cepatnya pemindahan dana, dan rendahnya kesadaran korban untuk segera melapor. Oleh karena itu, pertanggungjawaban pidana perlu didukung oleh penguatan kapasitas digital forensik, koordinasi antara aparat penegak hukum dan penyelenggara sistem pembayaran, serta edukasi publik mengenai verifikasi penerima transaksi.

Kata Kunci: Pertanggungjawaban Pidana, QR Code Palsu, Penipuan Digital, Transaksi Elektronik, QRIS.

Abstract

The use of Quick Response Codes (QR Codes) in electronic transactions, particularly through the Quick Response Code Indonesian Standard (QRIS), provides convenience, speed, and efficiency for merchants and consumers. However, this development has also created new forms of cybercrime involving fake QR Codes. Such schemes may include replacing a merchant's original QR Code with the offender's code, distributing fraudulent digital-wallet applications, phishing, and using payment accounts registered under false identities. This study examines criminal liability for the use of fake QR Codes in electronic transactions in Indonesia. It employs empirical legal research using statutory and case approaches. Data were collected through library research and interviews with police officers at Kendari Police Resort and were analyzed descriptively and qualitatively. The findings show that an offender may be held criminally liable when the unlawful act, criminal capacity, intentional fault, and the absence of grounds excluding punishment are established. The use of a fake QR Code may fulfil the elements of fraud and/or manipulation of electronic information or electronic documents. Criminal liability may take the form of imprisonment, fines, and victim recovery through restitution under the applicable legal framework. Establishing liability requires the integration of conventional and electronic evidence, including victim and witness statements, transaction histories, recipient-account identities, CCTV footage, and digital forensic examination. The principal enforcement challenges include false identities, mule accounts, cross-jurisdictional operations, rapid fund transfers, and delayed reporting by victims. Criminal liability must therefore be supported by strengthened digital-forensic capacity, coordination among law-enforcement agencies and payment-system providers, and public education regarding verification of transaction recipients.

Keywords: Criminal Liability, Fake QR Code, Digital Fraud, Electronic Transaction, QRIS.

A. Pendahuluan

Digitalisasi sistem pembayaran telah mengubah pola transaksi masyarakat dari penggunaan uang tunai menuju pembayaran elektronik. Salah satu instrumen yang berkembang pesat adalah penggunaan QR Code sebagai media pembayaran. Dalam sistem pembayaran Indonesia, QRIS menjadi standar QR Code pembayaran yang memungkinkan masyarakat melakukan transaksi lintas aplikasi pembayaran pada merchant yang telah terdaftar. Penggunaan QRIS memberi kemudahan karena konsumen cukup memindai kode yang tersedia, memasukkan nominal apabila diperlukan, dan mengonfirmasi transaksi melalui aplikasi pembayaran.

Di balik kemudahan tersebut, terdapat risiko penyalahgunaan teknologi. Salah satu modus yang berkembang ialah penggunaan kode QR palsu untuk mengalihkan dana transaksi ke rekening pelaku. Pelaku dapat mencetak dan menempelkan QR Code palsu di atas QRIS asli milik pedagang, tempat usaha, maupun tempat ibadah. Dalam bentuk lain, pelaku dapat menyebarkan tautan atau aplikasi palsu yang menyerupai aplikasi pembayaran resmi, lalu memperoleh akses terhadap data atau dana milik korban. Penipuan demikian tidak hanya merugikan konsumen dan merchant, tetapi juga mengganggu kepercayaan publik terhadap keamanan transaksi elektronik.

Persoalan penggunaan kode QR palsu tidak semata-mata berkaitan dengan ada atau tidaknya kerugian keuangan. Secara hukum pidana, persoalan utamanya adalah apakah perbuatan pelaku memenuhi rumusan tindak pidana dan apakah kesalahan atas perbuatan tersebut dapat dibebankan kepada pelaku. Pertanggungjawaban pidana tidak lahir hanya karena terdapat akibat yang merugikan korban. Pelaku harus terbukti melakukan perbuatan yang dilarang, memiliki kemampuan bertanggung jawab, melakukan perbuatan dengan bentuk kesalahan yang dipersyaratkan, serta tidak memiliki alasan pembeda atau alasan pemaaf.

Dalam penelitian pada Polres Kendari, modus yang diidentifikasi antara lain penggantian QR Code asli milik merchant dengan kode milik pelaku, penggunaan akun atau rekening dengan identitas yang sulit dilacak, serta penyebaran aplikasi atau tautan palsu yang menyerupai layanan pembayaran digital resmi. Penyidik menghadapi kesulitan karena pelaku dapat menggunakan rekening pihak lain, akun fiktif, atau memindahkan dana secara cepat setelah transaksi terjadi. Kondisi ini membuat proses identifikasi pelaku dan penelusuran aliran dana menjadi unsur penting dalam penegakan hukum.

Berdasarkan latar belakang tersebut, artikel ini membahas bentuk pertanggungjawaban pidana terhadap penggunaan kode QR palsu dalam transaksi elektronik, syarat pembebanannya kepada pelaku, kebutuhan pembuktiannya, serta kendala yang dihadapi dalam proses penegakan hukum.

B. Metodologi

Penelitian ini menggunakan metode penelitian hukum empiris dengan pendekatan perundang-undangan dan pendekatan kasus. Pendekatan perundang-undangan digunakan untuk menelaah ketentuan hukum pidana, hukum transaksi elektronik, dan ketentuan yang relevan terhadap perlindungan korban. Sementara itu, pendekatan kasus digunakan untuk memahami karakteristik dan praktik penanganan penipuan kode QR palsu dalam transaksi elektronik.

Lokasi penelitian berada pada Polres Kendari. Data primer diperoleh melalui wawancara dengan penyidik yang menangani perkara penipuan dan kejahatan berbasis teknologi. Data sekunder diperoleh melalui studi kepustakaan atas peraturan perundang-undangan, literatur hukum pidana, jurnal, serta dokumen yang berkaitan dengan sistem pembayaran elektronik dan penipuan digital.

Data dianalisis secara deskriptif-kualitatif. Analisis dilakukan dengan menghubungkan fakta mengenai modus penggunaan QR Code palsu dengan unsur-unsur pertanggungjawaban pidana, ketentuan pidana yang relevan, bentuk pembuktian elektronik, serta kendala penegakan hukum. Metode ini digunakan untuk memberikan gambaran yang sistematis tentang pembebanan pertanggungjawaban pidana kepada pelaku penipuan QR Code palsu.

C. Hasil dan Pembahasan

Konsep Pertanggungjawaban Pidana

Pertanggungjawaban pidana merupakan mekanisme hukum untuk meneruskan celaan atas suatu tindak pidana kepada subjek hukum yang melakukan perbuatan tersebut. Dalam doktrin hukum pidana, asas fundamental yang digunakan ialah *tiada pidana tanpa kesalahan* atau *nulla poena sine culpa*. Artinya, seseorang tidak dapat dipidana hanya karena suatu akibat pidana terjadi; harus dibuktikan pula adanya kesalahan yang dapat dicelakan kepadanya.

Pembebanan pertanggungjawaban pidana terhadap pelaku penggunaan kode QR palsu memerlukan beberapa unsur. Pertama, harus ada perbuatan yang memenuhi rumusan tindak pidana. Perbuatan tersebut dapat berupa membuat QR Code palsu, memanipulasi identitas merchant, mengganti QR Code asli dengan QR Code yang terhubung ke rekening pelaku, menyebarkan aplikasi pembayaran palsu, atau menggunakan sarana elektronik untuk mengarahkan dana korban kepada pelaku.

Kedua, pelaku harus mempunyai kemampuan bertanggung jawab. Secara umum, orang yang melakukan perbuatan harus mampu memahami sifat perbuatannya dan mampu menentukan kehendaknya sesuai pemahaman tersebut. Ketiga, harus terdapat kesalahan dalam bentuk kesengajaan atau, pada tindak pidana tertentu, kealpaan. Pada modus QR Code palsu, unsur kesengajaan pada umumnya terlihat dari rangkaian persiapan pelaku: membuat kode QR, menautkannya dengan rekening tertentu, mengganti QR Code yang sah, menyiapkan akun penampung, atau menyebarkan aplikasi dan tautan palsu.

Keempat, tidak terdapat alasan pembenar atau pemaaf. Penggantian kode pembayaran milik merchant dengan kode yang mengarahkan dana kepada pelaku tidak dapat dibenarkan dalam hubungan hukum yang sah. Perbuatan tersebut dilakukan tanpa hak dan bertentangan dengan kepentingan pemilik merchant, konsumen, serta sistem pembayaran elektronik. Dengan terpenuhinya unsur-unsur tersebut, pelaku dapat dibebani pertanggungjawaban pidana.

Bentuk Perbuatan dan Kesalahan Pelaku

Penggunaan QR Code palsu pada dasarnya merupakan modus penipuan yang memanfaatkan kepercayaan korban terhadap tampilan, nama merchant, atau sarana pembayaran digital. Korban memindai QR Code dengan keyakinan bahwa pembayaran diarahkan kepada merchant, sedangkan pelaku justru mengarahkan pembayaran itu kepada rekening atau akun yang dikuasainya.

Unsur kesengajaan dapat dilihat dari tujuan dan pola tindakan pelaku. Apabila pelaku membuat QR Code yang terhubung ke rekening pribadi atau rekening penampung, kemudian menempelkannya di atas QR Code asli, tindakan tersebut menunjukkan adanya kehendak untuk memperoleh keuntungan secara melawan hukum. Kesengajaan juga dapat terlihat dari penggunaan identitas palsu, rekening pihak ketiga, perangkat komunikasi tertentu, aplikasi tidak resmi, atau metode pemindahan dana yang ditujukan untuk menyulitkan pelacakan.

Dalam konteks tindak pidana penipuan, penggunaan QR Code palsu dapat dipahami sebagai alat atau tipu muslihat untuk menggerakkan korban melakukan pembayaran. Korban menyerahkan uang secara sukarela dalam arti fisik, tetapi persetujuan tersebut diperoleh karena

adanya keadaan yang menyesatkan. Dengan demikian, kerugian korban lahir dari hubungan sebab akibat antara tindakan manipulatif pelaku dan pembayaran yang dilakukan korban.

Selain penipuan, manipulasi QR Code dapat berkaitan dengan perbuatan membuat, mengubah, merusak, menghilangkan, menyembunyikan, atau menyebarkan informasi elektronik maupun dokumen elektronik secara melawan hukum. Penentuan pasal yang diterapkan perlu disesuaikan dengan fakta perkara. Apabila modus hanya berupa penggantian stiker QRIS secara fisik, penyidik tetap harus membuktikan keterhubungan antara QR Code palsu, akun penerima dana, dan pelaku. Jika modus melibatkan aplikasi palsu, phishing, akses tanpa hak, atau pengambilalihan akun, maka pemeriksaan digital forensik dan analisis sistem elektronik menjadi semakin menentukan.

Dasar Pertanggungjawaban Pidana

Dasar pertanggungjawaban pidana terhadap pelaku tidak dapat ditentukan hanya berdasarkan label “penipuan QRIS”. Penegak hukum harus menguraikan secara konkret perbuatan pelaku, alat yang dipakai, akibat yang timbul, bentuk kesalahan, dan hubungan kausal antara perbuatan dengan kerugian korban.

Ketentuan yang dipandang relevan meliputi tindak pidana penipuan dalam KUHP serta ketentuan mengenai manipulasi informasi atau dokumen elektronik dalam UU ITE. Pasal penipuan digunakan apabila terdapat maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan penggunaan nama palsu, keadaan palsu, tipu muslihat, atau rangkaian kebohongan yang menyebabkan pihak lain menyerahkan uang atau barang. Sementara itu, ketentuan UU ITE relevan apabila pelaku melakukan manipulasi, penciptaan, perubahan, atau penggunaan informasi dan/atau dokumen elektronik untuk tujuan menipu atau merugikan pihak lain.

Penerapan dasar hukum perlu dilakukan secara hati-hati berdasarkan prinsip legalitas dan larangan pemidanaan ganda terhadap perbuatan yang sama. Apabila satu rangkaian perbuatan memenuhi unsur beberapa ketentuan pidana, penuntut umum harus merumuskan konstruksi dakwaan secara tepat, termasuk menilai kemungkinan dakwaan alternatif, subsidiar, atau kumulatif sesuai karakter fakta perkaranya.

Aspek	Penipuan melalui QR Code palsu	Manipulasi informasi/dokumen elektronik
Inti perbuatan	Menggunakan QR Code palsu atau modus menyesatkan untuk mendorong korban membayar	Membuat, mengubah, memanipulasi, atau menggunakan informasi/dokumen elektronik secara melawan hukum
Tujuan pelaku	Memperoleh keuntungan bagi diri sendiri atau pihak lain secara melawan hukum	Menipu, menimbulkan kerugian, atau menghasilkan informasi/dokumen elektronik yang diperlakukan seolah-olah autentik
Fokus pembuktian	Tipu muslihat, kesesatan korban, pembayaran atau penyerahan dana, serta kerugian	Proses manipulasi digital, asal-usul QR Code, keterhubungan akun, jejak elektronik, dan tujuan pelaku
Bukti penting	Keterangan korban, bukti pembayaran, rekaman kamera pengawas, saksi merchant	Log transaksi, metadata, perangkat digital, akun penerima, alamat IP jika tersedia, dan pemeriksaan forensik digital

Tabel tersebut menunjukkan bahwa penggunaan QR Code palsu dapat beririsan dengan lebih dari satu konstruksi tindak pidana. Penentuan pasal harus dilakukan berdasarkan karakter konkret perbuatannya, bukan sekadar berdasarkan sarana yang dipakai.

Bentuk Sanksi dan Pemulihan Korban

Bentuk pertanggungjawaban utama bagi pelaku adalah pidana penjara dan/atau pidana denda sesuai ketentuan yang terbukti diterapkan. Pidana berfungsi sebagai reaksi negara terhadap perbuatan yang melanggar hukum sekaligus sarana pencegahan terhadap pengulangan tindak pidana. Dalam kasus penipuan digital, pemidanaan perlu memperhatikan tingkat kesengajaan, perencanaan, jumlah korban, nilai kerugian, penggunaan identitas palsu, peran

pelaku dalam jaringan, serta dampak terhadap kepercayaan masyarakat pada sistem pembayaran elektronik.

Selain pemidanaan, perlindungan korban merupakan bagian penting dari penanganan perkara. Korban dapat mengalami kerugian material akibat dana yang masuk ke rekening pelaku. Karena itu, pemulihan kerugian dapat ditempuh melalui mekanisme restitusi sesuai peraturan perundang-undangan. Restitusi tidak identik dengan pidana denda. Denda dibayarkan kepada negara sebagai sanksi pidana, sedangkan restitusi berorientasi pada pemulihan kerugian yang diderita korban.

Pemulihan efektif sangat bergantung pada kecepatan pelaporan dan kemampuan menelusuri aliran dana. Apabila laporan disampaikan segera setelah diketahui adanya transaksi mencurigakan, peluang pemblokiran rekening atau akun penerima dana menjadi lebih besar. Sebaliknya, keterlambatan pelaporan memungkinkan pelaku menarik, memindahkan, atau menyamarkan dana hasil kejahatan. Dalam penelitian di Polres Kendari, koordinasi dengan bank, penyedia layanan pembayaran, dan otoritas terkait dipandang penting untuk menelusuri transaksi dan mencegah dana hasil penipuan segera dicairkan oleh pelaku.

Pembuktian dalam Perkara QR Code Palsu

Pembuktian menjadi tahap yang menentukan karena tindak pidana ini dilakukan dengan kombinasi tindakan fisik dan elektronik. Tindakan fisik dapat berupa pembuatan serta pemasangan stiker QR Code palsu, sedangkan tindakan elektronik muncul dalam bentuk pembentukan QR Code, penggunaan akun pembayaran, penerimaan dana, dan pemindahan dana ke rekening lain.

Penyidik perlu mengumpulkan bukti yang membangun hubungan antara pelaku, QR Code palsu, rekening penerima, dan kerugian korban. Bukti yang relevan antara lain:

- Keterangan korban, merchant, saksi di lokasi, serta pihak yang mengetahui penggantian QR Code.
- Bukti transaksi dari aplikasi pembayaran, mutasi rekening, bukti pemindaian, dan notifikasi pembayaran.
- QR Code yang dipalsukan, stiker atau media fisik yang digunakan, serta QR Code asli milik merchant sebagai pembandingan.
- Rekaman CCTV di lokasi pemasangan atau penggantian QR Code.
- Data pemilik rekening, akun dompet digital, dan riwayat perpindahan dana.
- Barang bukti elektronik berupa telepon seluler, komputer, akun, aplikasi, atau pesan komunikasi yang diduga berkaitan dengan perencanaan dan pelaksanaan tindak pidana.
- Hasil pemeriksaan digital forensik untuk menelusuri asal-usul kode, koneksi akun, jejak transaksi, serta aktivitas pada perangkat elektronik.

Bukti elektronik mempunyai fungsi penting karena dapat menjelaskan bagaimana QR Code dibuat, kepada rekening siapa pembayaran dialihkan, kapan dana diterima, serta ke mana dana tersebut dipindahkan. Namun, bukti elektronik perlu diperoleh dan dipelihara melalui prosedur yang menjamin autentisitas, integritas, dan relevansinya agar dapat digunakan secara sah dalam proses peradilan.

Hambatan Penegakan Hukum

Penelitian menunjukkan beberapa hambatan utama dalam membebaskan pertanggungjawaban pidana kepada pelaku QR Code palsu. Pertama, pelaku sering memakai rekening atau akun atas nama orang lain. Rekening demikian dapat diperoleh melalui pinjaman identitas, pembukaan akun dengan data yang tidak valid, atau penggunaan pihak ketiga sebagai penampung dana. Keadaan ini membuat nama pemilik rekening tidak selalu identik dengan pelaku utama.

Kedua, tindak pidana dapat dilakukan lintas wilayah. Pelaku dapat memasang QR Code palsu di satu daerah, menggunakan rekening yang dibuka di daerah lain, lalu mengakses atau memindahkan dana dari lokasi berbeda. Kondisi ini membutuhkan koordinasi antarsatuan kepolisian, penyedia jasa sistem pembayaran, perbankan, dan pihak lain yang berwenang.

Ketiga, karakter transaksi elektronik memungkinkan dana berpindah dalam waktu singkat. Semakin lama korban mengetahui adanya penipuan, semakin sulit dana ditelusuri dan diamankan. Karena itu, kecepatan pelaporan dari korban dan respons awal penyidik merupakan faktor penting.

Keempat, rendahnya literasi keamanan digital masyarakat meningkatkan risiko korban. Tidak semua pengguna memeriksa nama penerima yang muncul dalam aplikasi pembayaran sebelum mengonfirmasi transaksi. Dalam kasus QRIS milik merchant, konsumen perlu

memastikan bahwa nama penerima sesuai dengan nama usaha, sedangkan merchant perlu secara berkala memeriksa kondisi fisik QR Code yang dipasang di tempat usaha. Temuan penelitian menekankan pentingnya verifikasi penerima dan pengawasan rutin terhadap QR Code untuk mencegah penggantian secara fisik.

Penguatan Pertanggungjawaban Pidana

Pertanggungjawaban pidana akan lebih efektif jika didukung kebijakan pencegahan dan penegakan hukum yang terpadu. Pertama, aparat penegak hukum perlu meningkatkan kapasitas investigasi siber dan digital forensik, terutama untuk mengamankan, membaca, dan menghubungkan data transaksi elektronik dengan identitas pelaku.

Kedua, koordinasi kelembagaan harus diperkuat. Kepolisian, perbankan, penyelenggara dompet digital, penyelenggara jasa sistem pembayaran, Bank Indonesia, dan otoritas pengawas sektor keuangan perlu mempunyai prosedur respons yang cepat terhadap laporan transaksi mencurigakan. Prosedur ini mencakup pengamanan data, penelusuran transaksi, pemblokiran sementara berdasarkan dasar hukum yang sah, dan penyampaian informasi untuk kepentingan penyidikan.

Ketiga, penyedia layanan pembayaran perlu membangun sistem deteksi anomali transaksi. Sistem ini dapat membantu mengidentifikasi pola transaksi yang tidak lazim, akun yang menerima dana dalam jumlah besar dari banyak pihak dalam waktu singkat, atau aktivitas yang memiliki indikator risiko penipuan.

Keempat, edukasi masyarakat harus ditempatkan sebagai bagian dari kebijakan pencegahan. Pengguna perlu membiasakan diri memeriksa nama penerima sebelum menekan tombol konfirmasi pembayaran. Merchant harus memastikan QR Code dipasang di tempat yang mudah diawasi, tidak tertutup stiker lain, dan diperiksa secara rutin. Langkah sederhana tersebut tidak menggantikan tanggung jawab negara dan penyelenggara sistem pembayaran, tetapi dapat mengurangi peluang keberhasilan modus penipuan.

D. Kesimpulan

Penggunaan kode QR palsu dalam transaksi elektronik dapat menimbulkan pertanggungjawaban pidana apabila pelaku terbukti melakukan perbuatan yang memenuhi unsur tindak pidana, memiliki kemampuan bertanggung jawab, bertindak dengan kesengajaan atau kesalahan yang dipersyaratkan, serta tidak mempunyai alasan pembenar atau pemaaf. Penggantian QR Code asli dengan QR Code palsu, pembuatan kode yang mengarahkan dana ke rekening pelaku, penyebaran aplikasi pembayaran palsu, dan penggunaan identitas transaksi fiktif pada prinsipnya menunjukkan adanya tindakan manipulatif yang ditujukan untuk memperoleh keuntungan secara melawan hukum.

Konstruksi pertanggungjawaban dapat dikaitkan dengan ketentuan penipuan dalam KUHP dan ketentuan pidana dalam UU ITE terkait manipulasi informasi atau dokumen elektronik, sepanjang unsur deliknya terbukti. Bentuk pertanggungjawaban dapat berupa pidana penjara, pidana denda, dan upaya pemulihan kerugian korban melalui restitusi. Pemilihan dan penerapan ketentuan pidana harus didasarkan pada uraian faktual mengenai cara kerja modus, bentuk manipulasi, hubungan kausal dengan kerugian korban, serta peran masing-masing pelaku.

Penegakan hukum terhadap tindak pidana QR Code palsu menghadapi kendala berupa penggunaan rekening penampung, identitas palsu, lintas yurisdiksi, pemindahan dana yang cepat, dan keterlambatan korban dalam melapor. Oleh sebab itu, penguatan pertanggungjawaban pidana harus diikuti peningkatan kemampuan digital forensik, koordinasi yang cepat antara aparat penegak hukum dan penyelenggara sistem pembayaran, mekanisme pemblokiran atau pelacakan dana yang sesuai hukum, serta peningkatan literasi keamanan digital bagi masyarakat dan merchant.

E. Referensi

- Ali, Z. (2017). *Metode penelitian hukum*. Sinar Grafika.
- Atmasasmita, R. (2017). *Rekonstruksi asas tiada pidana tanpa kesalahan*. Gramedia Pustaka Utama.
- Bank Indonesia. (2020). *Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang perlindungan konsumen Bank Indonesia*.
- Hendarsyah, D. (2018). Penggunaan uang elektronik dan uang virtual sebagai pengganti uang tunai di Indonesia. *Jurnal Ilmiah Ekonomi Bisnis*, 23(1), 1–15.

- Moeljatno. (2008). *Asas-asas hukum pidana*. Rineka Cipta.
- Muladi, & Arief, B. N. (2010). *Teori-teori dan kebijakan pidana*. Alumni.
- Prodjodikoro, W. (2014). *Asas-asas hukum pidana di Indonesia*. Refika Aditama.
- Soesilo, R. (1995). *Kitab Undang-Undang Hukum Pidana serta komentar-komentarnya lengkap pasal demi pasal*. Politeia.
- Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Wawancara dengan Aiptu Arif Setiawan, Penyidik Unit Reserse Kriminal Polres Kendari, sebagaimana dikutip dalam naskah penelitian mengenai penipuan kode QR palsu dalam transaksi elektronik.