

ANALISIS DAMPAK CYBERCRIME DATA FORGERY DAN UU HUKUM PERLINDUNGAN KONSUMEN PADA METODE PEMBAYARAN BERBASIS DIGITAL QRIS

Roida Pakpahan

Program Studi Sistem Informasi
Universitas Bina Sarana Informatika

*Correspondent Author: roida.rkh@bsi.ac.id

Received: May 31, 2026. **Revised:** July 25, 2026. **Accepted:** July 28, 2026. **Issue Period:** Vol.10 No.3 (2026), Pp. 906-913

Abstrak: Era teknologi yang semakin canggih penggunaan metode pembayaran berbasis digital terutama Quick Response Code Indonesian Standard (QRIS) mengalami peningkatan yang sangat signifikan. Bank Indonesia dalam laporannya menyatakan tahun 2026 pengguna QRIS mencapai 63 Juta. QRIS sebagai standart pembayaran digital nasional menjadi tren pembayaran digital terutama dikalangan UMKM karena QRIS memberikan kemudahan dalam melakukan transaksi namun disisi lain aplikasi QRIS memunculkan tantangan baru dalam dunia siber yakni cybercrime data forgery, sebuah tindakan kejahatan siber melalui modus penipuan data. Tingginya tingkat kejahatan yang terjadi dalam sistem pembayaran QRIS membutuhkan perlindungan hukum bagi pengguna aplikasi. Penelitian ini bertujuan untuk mengeksplorasi dampak kejahatan siber data forgery pada sistem pembayaran berbasis QRIS serta menganalisis implementasi perlindungan hukum pada konsumen pengguna pembayaran digital berbasis QRIS. Penelitian ini menggunakan metode penelitian deskriptif dan yuridis normatif. Hasil penelitian menunjukkan data forgery sebagai kejahatan siber melakukan berbagai metode penipuan melalui penggunaan stiker QR code palsu, phishing melalui QR code, hingga penipuan data transaksi. Kejahatan siber melalui QRIS terjadi dengan memanfaatkan ketidaktahuan dan ketidak hati-hatian pengguna. Cybercrime data forgery pada transaksi QRIS tidak hanya menimbulkan kerugian finansial tetapi juga berdampak terhadap penurunan kepercayaan masyarakat terhadap sistem pembayaran digital. Undang-undang yang berlaku hingga saat ini belum mengatur secara spesifik terkait tindakan penipuan berbasis QRIS. Cybercrime data forgery menjadi tantang baru bagi regulator dan pemerintah dalam menjamin keamanan bertransaksi keuangan digital. Keberadaan undang-undang harus hadir memberikan perlindungan dan kepastian hukum bagi para pengguna Aplikasi QRIS untuk bebas dari kejahatan siber data forgery. Hukum sejatinya harus mampu mengimbangi perkembangan keuangan digital yang semakin inovatif.

Kata Kunci: Cybercrime, Data Forgery, Hukum, Perlindungan Konsumen



DOI: 10.52362/jisamar.v10i3.2573

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).

Abstract: *In the increasingly sophisticated technological era, the use of digital-based payment methods, especially the Quick Response Code Indonesian Standard (QRIS), has experienced a very significant increase. Bank Indonesia in its report stated that by 2026 QRIS users will reach 63 million. QRIS as a national digital payment standard has become a digital payment trend, especially among MSMEs because QRIS provides convenience in conducting transactions, but on the other hand, the QRIS application raises new challenges in the cyber world, namely cybercrime data forgery, an act of cybercrime through data fraud. The high level of crime that occurs in the QRIS payment system requires legal protection for application users. This study aims to explore the impact of data forgery cybercrime on QRIS-based payment systems and analyze the implementation of legal protection for consumers who use QRIS-based digital payments. This research uses descriptive and normative juridical research methods. The research results show that data forgery as a cybercrime carries out various fraud methods through the use of fake QR code stickers, phishing via QR codes, and transaction data fraud. Cybercrime through QRIS occurs by exploiting users' ignorance and carelessness. Cybercrime involving data forgery in QRIS transactions not only causes financial losses but also reduces public trust in digital payment systems. The current laws do not specifically regulate QRIS-based fraud. Cybercrime data forgery is a new challenge for regulators and governments in ensuring the security of digital financial transactions. Legislation must be in place to provide protection and legal certainty for QRIS app users, preventing data forgery cybercrime. The law must be able to keep pace with increasingly innovative digital financial developments.*

Keywords: *Cybercrime, Data Forgery, Law, Consumer Protection*

I. PENDAHULUAN

Teknologi yang serba canggih turut mempengaruhi perkembangan metode sistem keuangan khususnya transformasi dalam sistem pembayaran digital, salah satunya aplikasi QRIS. QRIS (Quick Response Code Indonesian Standard) merupakan satu kode QR yang disediakan untuk semua jenis transaksi pembayaran digital. QRIS menjadi salah satu strategi nasional dalam mempercepat digitalisasi keuangan di Indonesia.

Perubahan metode transaksi dana tunai ke pembayaran digital lewat QR Code telah mempercepat inklusi keuangan dan efisiensi transaksi, terutama untuk para pelaku UMKM. QRIS banyak digunakan karena proses penggunaannya yang praktis dan efisien. QRIS memberikan kemudahan bagi pengguna untuk melakukan berbagai transaksi keuangan melalui pemindaan QR-Code.

QRIS turut berperan mendorong pertumbuhan usaha mikro, kecil, dan menengah. Bank Indonesia mencatat periode April 2026 terdapat 63 Juta (enam puluh tiga juta) pengguna QRIS, [1]. Namun disisi lain lajunya tingkat penggunaan pembayaran QRIS, memberikan tantangan baru terkait dengan cybercrime (kejahatan siber) data forgery (pemalsuan data) melalui pemindaan QR Code.

Penggunaan QRIS yang semakin tinggi turut meningkatkan risiko kejahatan siber dalam transaksi digital. Bentuk kejahatan siber yang sering terjadi antara lain pemalsuan data QR Code, phishing melalui tautan palsu, pencurian data pribadi, penyalahgunaan akun pembayaran digital hingga pengalihan dana ke rekening pelaku kejahatan tanpa persetujuan pengguna.

Data forgery (pemalsuan data) merupakan salah satu kejahatan siber yang sangat serius dalam pembayaran digital karena kejadian siber pemalsuan data akan menimbulkan kerugian pada individu maupun pelaku usaha baik kerugian finansial maupun penurunan tingkat kepercayaan publik terhadap penggunaan metode pembayaran QR Code.

Data forgery pada sistem pembayaran Quick Response (QR) Code dilakukan melalui modus QR tampering/switching (menempelkan stiker QR palsu) atau *quishing* (mengelabui pengguna agar memindai kode QR berbahaya). Kejahatan siber (cybercrime) data forgery (pemalsuan data) melalui pembayaran digital memberikan dampak yang sangat serius bagi pengguna aplikasi QRIS karena menimbulkan kerugian finansial



DOI: 10.52362/jisamar.v10i3.2573

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).

yang sangat besar. Otorisasi Jasa Keuangan (OJK) Tahun 2025 mencatat total kerugian terkait scam dan fraud termasuk QR fraud mencapai Rp 2,5 (dua setengah) triliun dari 155.000 (seratus lima puluh lima ribu) aduan antara tahun 2022 hingga kuartal I tahun 2024, hal tersebut membuktikan besarnya dampak kerugian ekonomi akibat kejahatan digital, [2]. Kejahatan siber data forgery akan berdampak terhadap dana konsumen, data pribadi, hingga peretasan perangkat pengguna.

Rendahnya tingkat literasi digital masyarakat terkait teknis pembayaran digital turut mempengaruhi terjadinya penipuan berbasis QRIS, banyak pengguna belum memahami cara mengenali penipuan digital dan menjaga kerahasiaan data pribadi maupun prosedur pelaporan apabila menjadi korban kejahatan siber. Di sisi lain, perkembangan modus kejahatan digital berlangsung sangat cepat sehingga sering kali melampaui kesiapan regulasi dan pengawasan yang berlaku, [3], [4].

Adanya kejahatan siber data forgery yang semakin tinggi yang dilakukan para pelaku kejahatan melalui metode pembayaran QRIS, membutuhkan perlindungan hukum. Keberadaan undang-undang dalam memberikan perlindungan hukum bagi konsumen pengguna QRIS merupakan kebutuhan yang bersifat urgensi mengingat perkembangan sistem keuangan digital yang semakin masif harus diimbangi dengan regulasi dan kepastian hukum sesuai dengan kondisi terkini.

Penelitian ini bertujuan untuk mengidentifikasi dampak cybercrime (kejahatan siber) data forgery (pemalsuan data) serta menganalisis implementasi Undang – undang hukum perlindungan konsumen bagi para pengguna keuangan digital Aplikasi QRIS.

II. METODE DAN MATERI

2.1. Metode

Penelitian ini menggunakan metode penelitian deskriptif dan yuridis normatif. Pendekatan deskriptif untuk menjelaskan hal yang berkaitan dengan penggunaan aplikasi pembayaran digital khususnya QRIS. Tinjauan pustaka terstruktur, pengumpulan artikel, laporan Bank Indonesia dan Otoritas Jasa Keuangan, artikel jurnal tentang QRIS dan kejahatan siber. Teknik wawancara dengan pengelola UMKM dan para pengguna QRIS. Yuridis Normatif dilakukan untuk mengkaji norma hukum, asas hukum serta ketentuan peraturan perundang-undangan yang berkaitan dengan perlindungan hukum bagi pengguna QRIS.

2.2. Materi

A. Quick Response Indonesian Standard (QRIS)

QRIS (Quick Response Indonesian Standard) merupakan standar nasional kode QR yang dikembangkan untuk mempermudah transaksi pembayaran digital di Indonesia yang diprakarsai oleh Bank Indonesia. [5]



Gambar 1. Quick Response Indonesian Standard



DOI: 10.52362/jisamar.v10i3.2573

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).

Sumber: Bank Indonesia

QRIS (Quick Response Indonesian Standard) adalah instrumen pembayaran digital yang dirancang untuk menciptakan interoperabilitas antar penyedia jasa pembayaran sehingga masyarakat dapat melakukan transaksi secara lebih mudah, aman, dan terstandarisasi, [6].

B. Data Forgery

Data forgery atau pemalsuan data merupakan tindakan memodifikasi atau memanipulasi informasi dengan maksud menipu atau menyesatkan orang lain, [7].

C. Perlindungan Konsumen

Menurut Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, hukum perlindungan konsumen merupakan seperangkat peraturan yang bertujuan untuk menjaga serta menjamin hak dan kewajiban konsumen dalam melakukan transaksi dengan produsen atau penyedia jasa. Regulasi tersebut tidak hanya mengatur hak serta kewajiban konsumen, tetapi juga menetapkan ketentuan yang harus dipatuhi oleh para pelaku usaha. Perlindungan konsumen tidak hanya mencakup transaksi jual beli secara langsung tetapi juga yang sifatnya tidak secara langsung atau secara online, [8]

Perlindungan konsumen sebagai bagian dari undang-undang yang memuat asas-asas atau aturan-aturan yang bersifat mengatur dan berfungsi untuk melindungi kepentingan konsumen. Hak-hak konsumen didefinisikan sebagai semua prinsip dan aturan hukum yang berkaitan dengan hubungan dan permasalahan yang berkaitan dengan konsumsi barang dan/atau jasa dalam kehidupan bermasyarakat antara berbagai pihak dan satu sama lain, [9]. Konsumen menurut pasal 1 ayat 2 Undang-Undang Perlindungan Konsumen yaitu Konsumen merupakan setiap orang, pemakai barang dan/jasa yang tersedia dalam masyarakat baik bagi kepentingan diri sendiri, keluarga, maupun makhluk hidup lain dan tidak diperdagangkan.

Pelaku usaha berdasarkan Undang – undang Perlindungan Konsumen, Pasal 1 ayat 3 didefinisikan sebagai orang perseorangan atau badan usaha, berbentuk badan hukum maupun bukan badan hukum yang dibentuk dan berkedudukan atau melakukan kegiatan dalam wilayah hukum negara Republik Indonesia secara sendiri maupun bersama-sama melalui perjanjian menyelenggarakan kegiatan usaha dalam berbagai bidang ekonomi.

III. PEMBAHASA DAN HASIL

Perkembangan teknologi digital turut mempengaruhi metode sistem pembayaran digital di Indonesia salah satunya melalui pembayaran digital berbasis Quick Response Code Indonesian Standard (QRIS). QRIS merupakan sistem pembayaran digital nasional yang dibentuk Bank Indonesia berbasis QR Code.

QRIS (Quick Response Code Indonesian Standard) sebagai standar nasional kode QR yang dirancang untuk mendukung transaksi digital melalui aplikasi uang elektronik. QRIS bertujuan meningkatkan efisiensi pembayaran, memperluas inklusi keuangan, mendukung pertumbuhan UMKM serta mendorong pertumbuhan ekonomi nasional.

Bagi pelaku Usaha Mikro, Kecil dan Menengah (UMKM) integrasi pembayaran melalui QRIS menjadi strategi penting untuk meningkatkan efisiensi pembayaran dan mempercepat transaksi, serta mendorong pertumbuhan usaha yang berkelanjutan. Melalui skema Merchant Presented Mode, QRIS memungkinkan merchant menampilkan satu kode QR universal yang dapat dipindai sebagai metode pembayaran.

QRIS menghubungkan berbagai aplikasi pembayaran dalam satu kode standar nasional sehingga pengguna dapat melakukan pembayaran dalam satu platform tertentu. Kondisi tersebut membuktikan bahwa QRIS telah menjadi bagian penting dalam mendorong transformasi ekonomi digital dan inklusi keuangan nasional. Namun disamping itu peningkatan penggunaan QRIS yang berlangsung secara cepat turut memunculkan tantangan baru dalam siber salah satunya kejahatan siber data forgery (pemalsuan data). Sistem pembayaran berbasis QRIS rentan terhadap berbagai penipuan QR code yang dapat dimanfaatkan oleh pelaku kejahatan siber. Berbagai modus penipuan QR code dilakukan dengan mengganti QR code merchant dengan QR palsu, quishing yang mengalihkan transfer dana ke rekening yang tidak sah, [10].



DOI: 10.52362/jisamar.v10i3.2573

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).

Bank Indonesia dan Otorisasi Jasa Keuangan dalam laporannya menyatakan kejahatan siber data forgery mengalami peningkatan yang sangat tajam, insiden penipuan QR code melonjak hingga 160% dalam 2 tahun terakhir terdapat 356.786 (tiga ratus lima puluh enam ribu tujuh ratus delapan puluh enam) kasus phishing terkait pembayaran digital. Data Kaspersky menunjukkan serangan phishing menggunakan kode QR meningkat tajam pada paruh kedua 2025 dengan jumlah deteksi melonjak hingga lima kali lipat dibandingkan periode tahun sebelumnya, [2]. Data tersebut menunjukkan bahwa pelaku kejahatan semakin cerdik menyasar celah keamanan dalam pembayaran digital. Data forgery melalui QR code palsu memiliki risiko yang tinggi yang berpotensi merugikan konsumen pengguna QRIS secara financial. Kejahatan siber data forgery akan mengakibatkan dana konsumen salah tujuan transfer, penyalahgunaan data pribadi, hingga peretasan perangkat, [11].

Maraknya modus kejahatan siber dataforgery dipengaruhi berbagai faktor diantaranya dari sisi teknis, penggunaan QR Code yang bersifat statis dan minim perlindungan keamanan dan QR code tanpa dukungan mekanisme kriptografi meningkatkan risiko terjadinya pemalsuan data, [12]. Penyebab utama terjadinya penipuan QR Code adalah lemahnya perlindungan data pada QR Code itu sendiri. QR code yang bersifat statis dan tidak dilengkapi sistem pengamanan tambahan cenderung mudah disalin atau dimodifikasi.

Selain faktor teknis, rendahnya literasi pengguna dalam menggunakan QRIS menjadi salah satu faktor penyebab terjadinya penipuan melalui QRIS. Kebiasaan pengguna yang cenderung mengutamakan kecepatan transaksi sering kali membuat proses verifikasi diabaikan. Situasi tersebut dimanfaatkan oleh pelaku kejahatan melalui teknik rekayasa sosial dengan menampilkan QR palsu yang tampak sah dan sulit dibedakan dari QR asli. Kasus penipuan seperti penggantian QR asli dengan QR palsu atau quishing terjadi karena pengguna langsung memindai QR tanpa memastikan keaslian merchant atau tujuan pembayaran, sehingga pelaku kejahatan dengan mudah mengalihkan dana ke rekening pelaku, [13].

Widjanarko [14] menjelaskan bahwa masih banyak pengguna dan pelaku UMKM yang belum memahami risiko keamanan dalam transaksi digital QRIS. Kurangnya pengetahuan membuat para pengguna mudah tertipu melalui modus rekayasa sosial QR palsu atau menyamar sebagai merchant resmi yang tampak meyakinkan. Kejahatan siber dalam sistem pembayaran digital tidak hanya terjadi karena kelemahan teknologi, tetapi juga karena pelaku memanfaatkan kelengahan pengguna. Kasus penipuan QR merupakan bagian dari kejahatan siber yang mengandalkan kombinasi antara celah sistem dan manipulasi perilaku manusia. Proses pelaporan yang rumit dan lambat sering kali membuat korban terlambat menyadari kerugian, sehingga dana yang sudah berpindah sulit untuk ditelusuri kembali.

Berbagai masalah yang timbul dalam penggunaan metode pembayar digital berbasis QRIS membutuhkan keamanan secara teknis dalam melakukan transaksi serta perlindungan hukum dan regulasi yang tepat guna melindungi para pengguna dari berbagai penipuan dari tindak kejahatan siber data forgery.

Upaya mencegah kejahatan Siber data forgery secara teknis dapat dilakukan dengan menerapkan cyber security. Cyber security merupakan sekumpulan instrumen, strategi, prinsip keamanan, langkah perlindungan, panduan, metode pengelolaan risiko yang dapat digunakan untuk melindungi pengguna QRIS dari berbagai metode penipuan QR Code. Cyber security memiliki berbagai keunggulan dan berperan penting dalam melindungi keamanan sistem digital. Salah satu manfaat utamanya adalah kemampuan untuk mendeteksi dan mencegah serangan secara cepat melalui teknologi seperti IDS dan IPS, sehingga ancaman dapat segera ditangani sebelum menimbulkan kerugian. Cyber security juga dapat diintegrasikan dengan teknologi canggih seperti Artificial Intelligence (AI) dan Machine Learning (ML) yang memungkinkan sistem mempelajari pola serangan sebelumnya dan memberikan respons yang lebih cepat serta akurat terhadap ancaman baru.

Cyber security merupakan serangkaian praktik dan pendekatan teknis yang bertujuan untuk melindungi sistem informasi dari ancaman akses yang tidak sah, sabotase digital serta pencurian data. Cyber security digunakan untuk pengamanan jaringan, perlindungan data pribadi, penerapan autentikasi berlapis, serta pemantauan aktivitas transaksi secara real-time untuk mendeteksi potensi ancaman. Cyber security (keamanan siber) memiliki sejumlah peran fundamental yang menjadi landasan utama dalam melindungi sistem dan informasi digital diantaranya;

- a. Confidentiality berfokus pada upaya menjaga informasi agar hanya dapat diakses oleh pihak yang memiliki kewenangan.
- b. Integrity bertujuan memastikan bahwa data, baik yang disimpan maupun yang dikirimkan, tetap utuh dan tidak mengalami perubahan tanpa izin.



- c. Availability berkaitan dengan jaminan bahwa sistem dan data selalu siap digunakan serta dapat diakses oleh pengguna yang berhak ketika diperlukan.
- d. Authentication berfungsi untuk memastikan keaslian identitas pengguna atau sistem yang mengakses informasi.
- e. Non-repudiation berperan dalam mencegah terjadinya penyangkalan dari pihak pengirim maupun penerima terhadap aktivitas atau transaksi data yang telah dilakukan.

Penerapan keamanan yang baik dengan mengaplikasikan cyber security akan meningkatkan kepercayaan pengguna karena data transaksi terlindungi dengan baik. Selain peningkatan keamanan dalam siber aspek undang-undang hukum perlindungan konsumen merupakan salah satu faktor utama yang sangat dibutuhkan untuk mengantisipasi berbagai kerugian yang dialami konsumen pengguna QRIS.

Perlindungan konsumen memiliki peranan penting dalam sistem Undang-undang yang memperkuat hubungan antara konsumen dan pelaku usaha, guna melindungi hak-hak konsumen dalam kegiatan konsumsi barang dan jasa. Peraturan Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Lembaga Perlindungan Konsumen di Indonesia berperan dalam menjaga hak-hak konsumen dari ketidakadilan dalam transaksi barang dan jasa.

Undang-undang hukum perlindungan konsumen menjadi faktor penting dalam penggunaan QRIS sebagai layanan pembayaran digital. Pada dasarnya pengguna memiliki hak atas keamanan, kenyamanan, informasi yang benar serta hak memperoleh kompensasi apabila mengalami kerugian akibat sistem yang bermasalah atau kelalaian penyelenggara. Merchant dan penyedia jasa pembayaran berkewajiban memastikan transaksi berjalan aman, transparan dan dapat dipertanggungjawabkan. Terjadinya kesalahan transaksi, kegagalan sistem, atau penipuan yang disebabkan lemahnya pengawasan maka pengguna berhak melakukan pengaduan dan menuntut penyelesaian sesuai ketentuan hukum.

Secara umum perlindungan hukum dalam penggunaan QRIS masih menggunakan Undang - Undang Transaksi Elektronik Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen serta PP Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Perlindungan hukum yang digunakan terkait transaksi digital melalui sistem QRIS masih dalam tahapan perlindungan hukum preventif yakni dengan memberikan pemahaman dan penyadaran bagi masyarakat terkait tata cara menggunakan sistem QRIS dalam bertransaksi serta potensi tindak pidana. Pengguna diberikan informasi tentang bagaimana cara melaporkan adanya potensi tindak pidana sebagai implikasi sistem QRIS. Perlindungan hukum represif dilakukan aparat penegak hukum yang ada dengan peningkatan kapasitas serta sarana dan prasarana.

Implementasi undang-undang untuk menjamin perlindungan hukum terkait tindakan penipuan melalui kode QR palsu masih menggunakan Pasal 35 jo. Pasal 51 ayat (1) UU ITE Tahun 2016 yang berbunyi melarang individu membuat, mendistribusikan, atau menggunakan informasi elektronik dan/atau dokumen elektronik yang tidak sah dengan niat menipu atau merugikan pihak lain dengan pidana penjara hingga 12 tahun dan/atau denda maksimal Rp. 12.000.000.000 (dua belas miliar) dan penerapan Pasal 378 jo Pasal 492 dalam Kitab Undang-Undang Hukum Pidana (KUHP) Tahun 2023 yang mengatur tindak pidana penipuan dengan ancaman hukuman penjara hingga empat tahun. Tindak pidana terhadap pelaku pemalsuan QR code QRIS dijerat melalui kombinasi instrumen hukum yang berlaku dengan UU ITE maupun KUHP.

Hingga saat ini upaya penegakan hukum melalui undang-undang terkait sistem pembayaran digital melalui QRIS belum diatur secara spesifik. Oleh karena itu diperlukan penguatan perlindungan hukum yang adaptif, efektif, dan berkelanjutan agar masyarakat pengguna aplikasi QRIS memperoleh rasa aman dalam bertransaksi digital. Hukum harus hadir untuk melindungi kepentingan konsumen agar tidak dirugikan oleh penyalahgunaan sistem keuangan digital. Perlindungan hukum bukan hanya bersifat reaktif, tetapi juga harus mampu bersikap antisipatif dan prediktif terhadap kemungkinan munculnya kejahatan siber di masa depan. Hukum harus siap menghadapi berbagai persoalan ditengah perkembangan keuangan digital yang semakin inovatif.

IV. KESIMPULAN

Berdasarkan pembahasan diatas dapat diberikan beberapa kesimpulan diantaranya:

1. Transaksi keuangan digital berbasis QRIS memberikan kemudahan dalam bertransaksi serta meningkatkan inklusi keuangan namun QRIS juga menimbulkan tantangan baru terkait maraknya kejahatan siber data forgery. Data forgery merupakan kejahatan serius dalam metode pembayaran digital melalui metode QR code palsu. Pemalsuan



DOI: 10.52362/jisamar.v10i3.2573

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).

data akan menimbulkan kerugian finansial. Disisilain cybercrime data forgery akan memberikan dampak negatif bagi para pelaku usaha khususnya UMKM yang paling banyak menggunakan QRIS. Kejahatan siber data forgery mempengaruhi kepercayaan konsumen dalam melakukan transaksi digital dan akan mengurangi tingkat penjualan UMKM akibat adanya penipuan lewat pembayaran QRIS pada merchant.

2. Dalam konteks pemalsuan data (data forgery), keamanan dan keaslian data menjadi hal sangat krusial. Diperlukan upaya pencegahan yang efektif, antara lain dengan memperkuat sistem keamanan digital untuk mengantisipasi dan meminimalkan risiko kejahatan siber data forgery secara teknis dapat dilakukan dengan menerapkan cyber security dan menggunakan payload QR code yang dinamis.
3. Peran regulator dalam menetapkan standar keamanan sangat diperlukan untuk mendorong penerapan sistem verifikasi yang lebih kuat pada aplikasi QRIS serta mekanisme pelaporan dan respons yang cepat dari para pihak terkait untuk menekan dampak kerugian akibat penipuan keuangan digital.
4. Para pengguna QRIS harus menerapkan prinsip kehati-hatian dalam melakukan transaksi dengan memeriksa kembali QR code tujuan transfer atau pembayaran.
5. Hingga saat ini belum ada aturan spesifik yang mengatur secara terperinci tentang tindak pidana kejahatan siber data forgery penggunaan QR code palsu dalam transaksi berbasis QRIS. Dibutuhkan Undang-undang hukum perlindungan konsumen untuk menciptakan kepastian hukum bagi para pengguna QRIS.

REFERENASI

- [1]https://www.viva.co.id/bisnis/1902881-tembus-63-juta-pengguna-per-april-2026-qr-is-digunakan-45-juta-merchant-mayoritas-umkm#google_vignette
- [2]<https://qris.interactive.co.id/homepage/blog-detail.php?lang=en&page=MTc5-statistik-penipuan-qr-code-di-indonesia.-fakta-mengejutkan-danamp;-cara-menghindarinya>
- [3] Bodhi, S., & Tan, D. (2022). Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan (Cybercrime). *UNES Law Review*, 4(3).
- [4] Ayuningtyas, A., Adinugraha, H. H., & Sulthoni, M. (2024). Quick Response Code Indonesian Standard as a Digital Payment Solution to Increase the Turnover and Reduce the Circulation of Counterfeit Money. *Journal of Education and Computer Applications*, 1 (1).
- [5][https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/ritel/kanal-layanan/qris/default.aspx#:~:text=QRIS%20\(Quick%20Response%20Code%20Indonesian,%2C%20dan%20Andal%20\(CEMUMUAH\)](https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/ritel/kanal-layanan/qris/default.aspx#:~:text=QRIS%20(Quick%20Response%20Code%20Indonesian,%2C%20dan%20Andal%20(CEMUMUAH)).
- [6] Choirida, N. (2023). Analisis Faktor-Faktor Yang Mempengaruhi Keputusan Penggunaan QR Code Indonesian Standar (QRIS) Sebagai Sistem Pembayaran (Studi Kasus Generasi Z Kecamatan Ngaliyan) . Skripsi. UIN Walisongo Semarang.
- [7] Yusuf DM. 2022. Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber (Cyber Crime). *Jurnal Pendidikan dan Konseling*. Vol 4 No. 6.
- [8] <https://jdih.kemendag.go.id/peraturan/undang-undang-nomor-8-tahun-1999-tentang-perlindungan-konsumen>
- [9] Utama,B.S.,Citra,H.,&Sommaliagustina,D.(2023). Perlindungan Konsumen Terhadap Pengguna Produk Makanan Kemasan Cepat Saji Kedaluwarsa Di Kota Padang. *Judakum: Jurnal Dedikasi Hukum*, 2(3).
- [10] Ajhari, A. A. (2024). Security Analysis of Quick Response Code Indonesian Standard (QRIS) Digital Payment System. *Jurnal Info Kripto*, 18(3), 119–125.
- [11] <https://inet.detik.com/security/d-8516714/modus-baru-penipuan-online-pelaku-ubah-qr-code-dari-karakter-teks>



- [12] Dani Saputro, M., Wicaksana, B., & Zayid, F. (2023). Penerapan Algoritma AES 256 Pada Qr Code Untuk Sistem Registrasi Event Sepeda. TeknoIS: Jurnal Ilmiah Teknologi Informasi Dan Sains, 13(2).
- [13] Kristanty, D. N. (2024). Tren dan Tantangan Keamanan Bertransaksi dengan Qris dalam Era Transformasi Sistem Pembayaran Digital. Jurnal Syntax Admiration, 5(10).
- [14] Widjanarko, W. (2025). A review on the role of QRIS and digital wallets in facilitating MSME transactions in Indonesia. Annals of Human Resource Management Research, 5(1).
- [15] Pattynama, F. M., Santoso, H. A., Miarsa, F. R. D., & Pribadi, T. (2024). Legal Problems for Quick Response Code Indonesian Standard (Qris) Users in Online Payment Transactions. ANAYASA : Journal of Legal Studies, 2(1).
- [16] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal 35 dan Pasal 51 ayat (1)



DOI: 10.52362/jisamar.v10i3.2573

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).