



Analisis Risiko Transformasi Digital pada Pengguna QRIS

Naila Aqila Salsabila^{1*}, Dodi Siswanto²

¹⁻² Universitas Al Ghifari, Indonesia

Email: naaqilaa22@gmail.com¹, siswantododi88@gmail.com²

*Penulis Korespondensi: naaqilaa22@gmail.com

Abstract. Post-pandemic digitalization has accelerated the adoption of cashless payment systems among Micro, Small, and Medium Enterprises (MSMEs) in Indonesia. One of Bank Indonesia's major innovations is the Quick Response Code Indonesian Standard (QRIS), which has enhanced financial inclusion, business competitiveness, transaction transparency, and economic efficiency. Despite these benefits, QRIS adoption also raises concerns regarding cybersecurity and operational reliability. This study aims to examine the advantages and potential risks associated with QRIS implementation. A Systematic Literature Review (SLR) was conducted using the PRISMA framework. Secondary data were collected from Scopus, Web of Science, Google Scholar, and official reports published within the last five years. The findings reveal two major challenges. First, cybersecurity risks include fraudulent QRIS stickers, QR code phishing (quishing), and malware embedded in malicious QR codes that threaten users' sensitive information. Second, operational constraints include input errors in static QRIS transactions, dependence on internet connectivity and server stability, synchronization failures, and transaction limits that reduce flexibility for large-scale payments. Overall, QRIS remains an efficient and secure digital payment system, but its sustainable implementation requires stronger digital literacy, improved cybersecurity awareness, and reliable supporting infrastructure.

Keywords: Cybersecurity Risk; Digital Payment; MSMEs; QRIS; Systematic Literature Review.

Abstrak. Digitalisasi pascapandemi telah mempercepat adopsi sistem pembayaran nontunai di kalangan Usaha Mikro, Kecil, dan Menengah (UMKM) di Indonesia. Salah satu inovasi utama Bank Indonesia adalah *Quick Response Code Indonesian Standard* (QRIS), yang telah meningkatkan inklusi keuangan, daya saing usaha, transparansi transaksi, dan efisiensi ekonomi. Meskipun memberikan berbagai manfaat, penerapan QRIS juga menimbulkan kekhawatiran terkait keamanan siber dan keandalan operasional. Penelitian ini bertujuan untuk mengkaji manfaat serta potensi risiko yang berkaitan dengan implementasi QRIS. Penelitian menggunakan metode *Systematic Literature Review* (SLR) dengan kerangka PRISMA. Data sekunder diperoleh dari Scopus, Web of Science, Google Scholar, serta laporan resmi yang diterbitkan dalam lima tahun terakhir. Hasil penelitian mengidentifikasi dua tantangan utama. Pertama, risiko keamanan siber meliputi pemalsuan stiker QRIS, *QR code phishing* (quishing), serta malware yang disisipkan pada kode QR berbahaya sehingga mengancam keamanan informasi sensitif pengguna. Kedua, kendala operasional mencakup kesalahan input nominal pada transaksi QRIS statis, ketergantungan pada koneksi internet dan stabilitas server, kegagalan sinkronisasi transaksi, serta batasan nominal transaksi yang mengurangi fleksibilitas pembayaran dalam skala besar. Secara keseluruhan, QRIS tetap menjadi sistem pembayaran digital yang efisien dan aman, namun implementasinya secara berkelanjutan memerlukan peningkatan literasi digital, kesadaran terhadap keamanan siber, serta dukungan infrastruktur yang andal.

Kata Kunci: Pembayaran Digital; QRIS; Risiko Keamanan Siber; *Systematic Literature Review*; UMKM.

1. PENDAHULUAN

Penggunaan uang untuk aktivitas ekonomi sehari-hari pasti akan terus ada, tetapi digitalisasi semakin muncul seiring waktu dan memudahkan masyarakat untuk membayar (Sriekaningsih, 2020). Masyarakat Indonesia menggunakan pembayaran digital sebagai gaya hidup, terutama setelah Pandemi COVID 19 melanda dunia. Usaha Mikro, Kecil, dan Menengah (UMKM) dapat menggunakan berbagai sistem pembayaran digital, tergantung pada wilayah dan preferensi mereka (Tarantang et al., 2019); (Saebah & Asikin, 2022). Namun, penggunaan sistem pembayaran digital menawarkan sejumlah keuntungan yang meningkatkan kenyamanan baik bagi pelanggan maupun bisnis. Sebagai bisnis di era modern, sangat penting

untuk memanfaatkan berbagai teknologi yang sudah berkembang, seperti metode pembayaran digital (Febriyantoro & Arisandi, 2018).

Untuk bertransaksi dengan pelanggan, menggunakan metode pembayaran digital pasti akan lebih mudah karena prosesnya cepat dan transparan (Septianisya & Anggoro, 2024). Dengan berkembangnya teknologi informasi dan komunikasi, banyak sektor telah berubah, termasuk sistem pembayaran. Quick Response Code Indonesian Standard (QRIS) adalah salah satu inovasi penting dalam ekosistem pembayaran digital Indonesia. Dibat untuk menyederhanakan dan mengintegrasikan metode pembayaran berbasis kode QR, QRIS memungkinkan pelanggan untuk melakukan transaksi dengan cepat dan mudah hanya dengan memindai kode QR (Handayani & Soeparan, 2022, Asikin et al., 2024).

Namun, kekhawatiran tentang keamanan transaksi muncul seiring dengan adopsi luas QRIS. Meskipun QRIS mudah digunakan, masalah keamanan data dan kemungkinan penipuan masih menjadi masalah besar (Yudiana, 2023). Penelitian Rahardjo (2019) menekankan kebutuhan akan kebijakan yang lebih kuat untuk menangani ancaman keamanan digital dan kekurangan sistem perlindungan data. Sebagai contoh, pengguna QRIS terus menghadapi masalah seperti serangan phishing dan skimming.

Pembayaran digital adalah transaksi menggunakan uang elektronik melalui platform digital menggunakan metode transfer bank, scan QR, atau dompet elektronik tertentu (Napitupulu et al., 2020). Singkatnya, 'digital' berarti dilakukan melalui internet dan tanpa uang secara fisik. Pembayaran melalui internet lebih cepat, efisien, dan aman (Payamta, 2023).

Pembayaran digital di Indonesia juga kian berkembang. Dapat dilihat dari pengelolaan infrastruktur pembayaran yang terintegrasi serta kebijakan pemerintah sebagai contoh QRIS dan BI-FAST (Yadi et al., 2023). Bahkan, transportasi umum juga sangat memudahkan masyarakat untuk dapat membeli dan membayar tiket secara online, serta cukup melakukan 'tap' melalui barcode pada tiket elektronik di ponsel (Saebah & Asikin, 2022). Pembayaran digital sekarang dapat digunakan untuk berbagai hal, seperti membeli token listrik, pulsa internet, atau makanan dan minuman di restoran dan bahkan kedai. Pengisian saldo melalui platform online seperti mobile banking, transfer bank, atau bahkan beberapa situs e-commerce adalah bagian dari sistem pembayaran digital.

Sistem pembayaran Quick Response Indonesian Standard (QRIS), juga dikenal sebagai "Kris", dibuat oleh Bank Indonesia dan Asosiasi Sistem Pembayaran Indonesia (ASPI) untuk menetapkan standar untuk proses pembayaran elektronik di Indonesia. QRIS menyatukan berbagai sistem pembayaran elektronik di Indonesia dalam satu sistem QR Code. Pembayaran

melalui satu kode QRIS dapat dilakukan oleh pengguna dari berbagai sistem pembayaran elektronik dengan menggunakan ponsel berkamera yang

terhubung ke internet (Permatasari et al., 2022). Ketika melakukan pembayaran melalui QRIS, konsumen tidak dikenakan biaya tambahan. Namun, untuk merchant (pedagang), Bank Indonesia telah menetapkan skema dan biaya transaksi QRIS berdasarkan saran dari perwakilan penyedia sistem pembayaran elektronik.

Untuk memperoleh kode QRIS, penjual harus terlebih dahulu mendaftar dengan Penyedia Jasa Sistem Pembayaran (PJSP) yang berizin Bank Indonesia sebagai penyelenggara QRIS. PJSP ini dapat berupa bank maupun non-bank, seperti jasa dompet elektronik. situs web resmi QRIS berisi informasi tentang skema dan biaya transaksi QRIS (Nasution, 2020). Daftar lengkap PJSP yang berizin Bank Indonesia dapat ditemukan di situs web resmi Bank Indonesia.

Bank Indonesia mendorong penggunaan QRIS dalam upaya mempercepat penerapan sistem pembayaran tanpa tunai di Indonesia melalui Cetak Biru Sistem Pembayaran Indonesia 2025. Sebab, sistem pembayaran cashless dinilai lebih praktis dan aman ketimbang transaksi uang tunai. Perekonomian "bawah tanah" sebelumnya tidak tercatat karena transaksi tanpa uang juga tercatat dengan baik. Dengan menggunakan QRIS, perekonomian Indonesia dapat melihat banyak peluang.

Pertama, QRIS meningkatkan inklusi keuangan: membuat pembayaran elektronik menjadi lebih mudah bagi orang-orang yang sebelumnya tidak memiliki rekening bank atau kartu kredit. Ini akan meningkatkan akses keuangan di Indonesia dan mendorong pertumbuhan ekonomi di berbagai sektor.

Kedua, QRIS meningkatkan daya saing bisnis, terutama usaha mikro, kecil dan menengah. Bisnis kecil dan menengah (UMKM) yang sebelumnya hanya dapat menerima pembayaran tunai sekarang dapat menerima pembayaran non-tunai dengan QRIS. Ini memungkinkan mereka untuk menjangkau lebih banyak pelanggan dan memperluas jangkauan bisnis mereka.

Ketiga, penggunaan QRIS meningkatkan transparansi, dan pengendalian transaksi keuangan. Karena QRIS memungkinkan pencatatan otomatis dan pemantauan transaksi secara real-time oleh Bank Indonesia dan penyedia jasa sistem pembayaran, transaksi menjadi lebih transparan dan terkontrol. QRIS juga dapat membantu mengurangi kemungkinan penipuan dan kecurangan dalam transaksi. Keempat, penggunaan QRIS meningkatkan efisiensi dan produktivitas perekonomian di Indonesia. Dengan menggunakan QRIS, transaksi keuangan menjadi lebih cepat dan efisien, sehingga mengurangi waktu transaksi dan biaya

administrasi. Ini akan meningkatkan efisiensi dan produktivitas di berbagai industri, terutama di sector ekonomi digital.

2. KAJIAN TEORITIS

Teori Transformasi Digital (*Digital Transformation Theory*)

Transformasi digital merupakan proses perubahan mendasar dari sistem konvensional menuju sistem berbasis teknologi digital yang memengaruhi berbagai aspek kehidupan, termasuk ekonomi dan perilaku masyarakat. Menurut perspektif teoretis, transformasi digital tidak hanya mencakup adopsi teknologi, tetapi juga perubahan pola pikir, budaya organisasi, serta model bisnis yang lebih adaptif terhadap perkembangan teknologi. Dalam konteks sistem pembayaran, transformasi ini terlihat dari pergeseran penggunaan uang tunai menuju transaksi digital yang lebih cepat dan efisien. QRIS sebagai salah satu inovasi digital payment menjadi representasi nyata dari transformasi tersebut di Indonesia. Oleh karena itu, pemahaman terhadap teori ini penting untuk melihat dinamika perubahan yang terjadi pada pengguna dan pelaku usaha. Namun demikian, transformasi digital juga menimbulkan berbagai risiko yang tidak dapat diabaikan.

Ketidaksiapan infrastruktur teknologi dan rendahnya literasi digital dapat menjadi hambatan dalam proses adaptasi masyarakat. Selain itu, perubahan yang cepat seringkali tidak diimbangi dengan kesiapan regulasi dan sistem pengawasan yang memadai. Dalam penggunaan QRIS, hal ini dapat memicu kesalahan penggunaan serta potensi penyalahgunaan teknologi. Risiko lain juga muncul dari ketergantungan terhadap sistem digital yang rentan terhadap gangguan teknis. Dengan demikian, teori transformasi digital tidak hanya menjelaskan peluang, tetapi juga tantangan yang harus diantisipasi.

Teori Risiko Teknologi (*Technology Risk Theory*)

Teori risiko teknologi menjelaskan bahwa setiap penggunaan teknologi informasi selalu diiringi dengan potensi risiko yang dapat berdampak pada individu maupun organisasi. Risiko tersebut dapat berupa kegagalan sistem, serangan siber, kebocoran data, hingga kesalahan manusia dalam pengoperasian teknologi. Dalam sistem pembayaran digital seperti QRIS, risiko ini menjadi semakin kompleks karena melibatkan data keuangan yang bersifat sensitif. Oleh sebab itu, penting untuk melakukan identifikasi dan analisis risiko secara komprehensif guna meminimalkan dampak yang ditimbulkan. Teori ini juga menekankan pentingnya manajemen risiko sebagai bagian dari implementasi teknologi yang aman dan berkelanjutan.

Penggunaan QRIS menghadirkan berbagai bentuk risiko teknologi yang nyata. Ancaman seperti quishing, manipulasi kode QR palsu, serta penyusupan malware menjadi isu utama dalam keamanan sistem pembayaran digital. Selain itu, gangguan jaringan internet dan server juga dapat menyebabkan kegagalan transaksi yang merugikan pengguna. Faktor human error, seperti kesalahan dalam memasukkan nominal transaksi, turut memperbesar potensi kerugian. Oleh karena itu, pendekatan berbasis teori risiko teknologi diperlukan untuk merumuskan strategi mitigasi yang efektif. Dengan demikian, keamanan dan keandalan sistem QRIS dapat terus ditingkatkan.

Teori Penerimaan Teknologi (Technology Acceptance Model / TAM)

Technology Acceptance Model (TAM) merupakan salah satu teori yang digunakan untuk menjelaskan bagaimana individu menerima dan menggunakan suatu teknologi. Model ini menekankan dua faktor utama, yaitu *perceived usefulness* (persepsi manfaat) dan *perceived ease of use* (persepsi kemudahan penggunaan). Kedua faktor tersebut memengaruhi sikap pengguna terhadap teknologi serta niat untuk menggunakannya secara berkelanjutan. Dalam konteks QRIS, kemudahan transaksi dan efisiensi waktu menjadi faktor utama yang mendorong adopsi oleh masyarakat dan pelaku UMKM. Oleh karena itu, TAM menjadi landasan penting dalam memahami tingkat penerimaan teknologi pembayaran digital. Meskipun demikian, persepsi risiko juga memiliki peran signifikan dalam memengaruhi penerimaan teknologi. Semakin tinggi tingkat risiko yang dirasakan, maka semakin rendah tingkat kepercayaan pengguna terhadap teknologi tersebut.

Dalam penggunaan QRIS, kekhawatiran terhadap keamanan data dan potensi penipuan dapat menghambat adopsi secara luas. Selain itu, pengalaman negatif pengguna akibat gangguan sistem juga dapat menurunkan minat penggunaan di masa depan. Oleh karena itu, penting untuk menyeimbangkan antara manfaat dan risiko dalam implementasi teknologi. Dengan demikian, tingkat penerimaan QRIS dapat ditingkatkan melalui peningkatan keamanan dan edukasi pengguna.

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yaitu metode studi literatur. Metode studi literatur atau dikenal juga dengan istilah studi kepustakaan adalah teknik pengumpulan data dan informasi dengan menelaah sumber-sumber tertulis seperti jurnal ilmiah, buku referensi, ensiklopedia, serta sumber-sumber lain yang terpercaya baik dalam bentuk tulisan atau dalam format digital yang relevan dan berhubungan dengan objek yang sedang diteliti. Ungkapan tersebut sejalan dengan yang dikemukakan oleh (Moh.Nazir, 201) yang mengatakan bahwa

studi literatur adalah teknik pengumpulan data dengan mengadakan studi penelaahan terhadap buku- buku, literatur-literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan. Pendapat tersebut juga didukung oleh pendapat (Prof. Dr. Suharsimi Arikunto, 2002) yang mengungkapkan bahwa studi pustaka adalah metode pengumpulan data dengan mencari informasi lewat buku, majalah, koran, dan literatur lainnya yang bertujuan untuk membentuk sebuah landasan teori.

4. HASIL DAN PEMBAHASAN

Analisis Risiko Keamanan Digital pada Pengguna QRIS

Transformasi digital dalam sistem pembayaran melalui QRIS telah membawa perubahan signifikan dalam pola transaksi masyarakat Indonesia. Penggunaan QR code sebagai media pembayaran mempercepat proses transaksi dan meningkatkan efisiensi ekonomi. Namun, di balik kemudahan tersebut terdapat berbagai risiko keamanan digital yang perlu dianalisis secara mendalam. Risiko ini muncul akibat sifat teknologi yang terbuka dan mudah diakses oleh berbagai pihak. Oleh karena itu, analisis terhadap risiko keamanan menjadi penting dalam memastikan keberlanjutan sistem pembayaran digital (Davis, 1989).

Salah satu risiko utama dalam penggunaan QRIS adalah manipulasi kode QR oleh pihak yang tidak bertanggung jawab. Penipu dapat mengganti kode QR asli dengan kode palsu yang terhubung ke rekening pribadi mereka. Hal ini sulit dideteksi oleh pengguna karena tampilan kode QR secara visual hampir identik. Dampak dari tindakan ini adalah kerugian finansial baik bagi konsumen maupun merchant. Fenomena ini menunjukkan adanya celah keamanan dalam implementasi teknologi QR (Baskara & Hariyadi, 2014).

Selain itu, praktik quishing menjadi ancaman serius dalam ekosistem pembayaran digital. Teknik ini memanfaatkan kode QR untuk mengarahkan pengguna ke situs palsu yang menyerupai layanan resmi. Pengguna yang tidak waspada dapat dengan mudah memasukkan data sensitif seperti PIN atau password. Data tersebut kemudian dimanfaatkan oleh pelaku untuk melakukan kejahatan finansial. Hal ini menunjukkan pentingnya literasi digital dalam menghadapi ancaman siber (Adiyanti & Pudjihardjo, 2014). Ancaman malware juga menjadi bagian dari risiko keamanan QRIS yang tidak dapat diabaikan. Kode QR dapat digunakan untuk menyisipkan tautan berbahaya yang mengunduh aplikasi ilegal ke perangkat pengguna.

Malware tersebut dapat mencuri data pribadi hingga mengakses aplikasi perbankan. Risiko ini semakin tinggi ketika pengguna memindai kode QR dari sumber yang tidak terpercaya. Oleh karena itu, edukasi pengguna menjadi faktor kunci dalam mitigasi risiko (Febriyantoro & Arisandi, 2018). Dalam perspektif teori risiko teknologi, setiap inovasi digital

selalu diiringi dengan potensi kerentanan sistem. QRIS sebagai teknologi pembayaran tidak terlepas dari kemungkinan eksploitasi oleh pelaku kejahatan siber. Risiko ini mencakup aspek teknis maupun perilaku pengguna yang kurang waspada. Oleh karena itu, diperlukan pendekatan manajemen risiko yang komprehensif. Hal ini bertujuan untuk meminimalkan dampak negatif dari penggunaan teknologi (Davis, 1989).

Persepsi risiko juga memengaruhi tingkat kepercayaan pengguna terhadap QRIS. Semakin tinggi risiko yang dirasakan, maka semakin rendah tingkat adopsi teknologi tersebut. Hal ini sejalan dengan teori Technology Acceptance Model yang menekankan pentingnya persepsi dalam penggunaan teknologi. Pengguna cenderung menghindari sistem yang dianggap tidak aman. Oleh karena itu, peningkatan keamanan menjadi faktor penting dalam meningkatkan kepercayaan (Adiyanti & Pudjihardjo, 2014).

Keamanan data menjadi isu krusial dalam penggunaan QRIS. Transaksi digital melibatkan pertukaran data yang bersifat sensitif dan harus dilindungi dengan baik. Kebocoran data dapat menyebabkan kerugian besar bagi pengguna. Oleh karena itu, sistem keamanan harus terus diperbarui mengikuti perkembangan teknologi. Hal ini menjadi tantangan bagi penyedia layanan keuangan digital (Baskara & Hariyadi, 2014). Selain aspek teknis, faktor manusia juga berperan besar dalam risiko keamanan.

Kurangnya pemahaman pengguna terhadap cara kerja QRIS dapat meningkatkan potensi kesalahan. Pengguna seringkali tidak memverifikasi sumber kode QR sebelum melakukan transaksi. Hal ini membuka peluang terjadinya penipuan. Oleh karena itu, edukasi menjadi solusi utama dalam mengurangi risiko (Febriyantoro & Arisandi, 2018). Perkembangan teknologi digital yang cepat seringkali tidak diimbangi dengan kesiapan regulasi. Hal ini menyebabkan adanya celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan. Regulasi yang adaptif sangat diperlukan untuk mengatur penggunaan QRIS secara aman. Pemerintah dan lembaga terkait harus berperan aktif dalam hal ini. Dengan demikian, keamanan sistem dapat lebih terjamin (Davis, 1989).

Implementasi sistem keamanan berlapis menjadi solusi dalam mengatasi risiko digital. Penggunaan autentikasi ganda dan enkripsi data dapat meningkatkan perlindungan pengguna. Selain itu, sistem monitoring transaksi juga perlu diperkuat. Hal ini bertujuan untuk mendeteksi aktivitas mencurigakan secara dini. Dengan demikian, risiko dapat diminimalkan secara efektif (Adiyanti & Pudjihardjo, 2014). Kesadaran pengguna terhadap risiko digital masih tergolong rendah di beberapa wilayah. Hal ini dipengaruhi oleh tingkat pendidikan dan akses informasi. Pengguna yang kurang teredukasi lebih rentan terhadap kejahatan siber. Oleh karena itu,

program literasi digital harus diperluas. Edukasi ini penting untuk meningkatkan keamanan transaksi (Febriyantoro & Arisandi, 2018).

Peran lembaga keuangan sangat penting dalam menjaga keamanan QRIS. Mereka harus memastikan bahwa sistem yang digunakan telah memenuhi standar keamanan internasional. Selain itu, pelayanan pengaduan juga harus responsif terhadap keluhan pengguna. Hal ini penting untuk menjaga kepercayaan masyarakat. Dengan demikian, ekosistem digital dapat berkembang secara sehat (Baskara & Hariyadi, 2014). Keamanan QRIS juga dipengaruhi oleh kualitas teknologi yang digunakan. Sistem yang tidak stabil dapat meningkatkan risiko kegagalan transaksi.

Hal ini dapat menimbulkan kerugian dan ketidakpercayaan pengguna. Oleh karena itu, peningkatan kualitas teknologi menjadi prioritas utama. Investasi dalam infrastruktur digital sangat diperlukan (Davis, 1989). Pengawasan terhadap penggunaan QRIS harus dilakukan secara berkelanjutan. Hal ini untuk memastikan bahwa sistem tetap aman dan bebas dari penyalahgunaan. Pengawasan dapat dilakukan melalui audit sistem dan evaluasi berkala. Dengan demikian, potensi risiko dapat diidentifikasi lebih awal. Langkah ini penting dalam menjaga stabilitas sistem pembayaran digital (Adiyanti & Pudjihardjo, 2014).

Risiko keamanan digital dalam penggunaan QRIS merupakan tantangan yang kompleks. Risiko ini mencakup aspek teknis, perilaku, dan regulasi yang saling berkaitan. Oleh karena itu, pendekatan yang holistik diperlukan dalam mengatasinya. Kolaborasi antara pemerintah, penyedia layanan, dan masyarakat menjadi kunci utama. Dengan demikian, keamanan QRIS dapat terus ditingkatkan secara berkelanjutan (Febriyantoro & Arisandi, 2018).

Analisis Risiko Operasional dan Infrastruktur dalam Penggunaan QRIS

Penggunaan QRIS juga menghadapi tantangan dari sisi operasional dan infrastruktur. Sistem pembayaran digital sangat bergantung pada teknologi dan jaringan yang stabil. Ketergantungan ini menjadi kelemahan ketika terjadi gangguan teknis. Oleh karena itu, analisis terhadap risiko operasional menjadi penting. Hal ini bertujuan untuk memastikan kelancaran transaksi digital (Davis, 1989). Salah satu risiko operasional yang sering terjadi adalah human error dalam penggunaan QRIS statis. Pengguna harus memasukkan nominal transaksi secara manual. Kesalahan dalam memasukkan angka dapat menyebabkan kerugian finansial. Proses pengembalian dana juga tidak selalu mudah dan cepat. Hal ini menunjukkan perlunya peningkatan sistem otomatisasi (Adiyanti & Pudjihardjo, 2014). Ketergantungan terhadap jaringan internet menjadi tantangan utama dalam penggunaan QRIS.

Transaksi tidak dapat dilakukan tanpa koneksi yang stabil. Di daerah dengan akses internet terbatas, penggunaan QRIS menjadi kurang efektif. Hal ini menghambat inklusi keuangan digital. Oleh karena itu, pemerataan infrastruktur menjadi sangat penting (Febriyantoro & Arisandi, 2018). Gangguan pada server juga dapat menyebabkan kegagalan transaksi. Fenomena saldo terpotong tetapi transaksi tidak tercatat sering terjadi. Hal ini menimbulkan konflik antara pembeli dan penjual. Sistem harus mampu mengatasi masalah ini dengan cepat. Oleh karena itu, peningkatan kapasitas server menjadi kebutuhan utama (Baskara & Hariyadi, 2014).

Dalam perspektif transformasi digital, kesiapan infrastruktur menjadi faktor kunci keberhasilan. Tanpa dukungan infrastruktur yang memadai, teknologi tidak dapat berfungsi secara optimal. QRIS membutuhkan sistem yang terintegrasi dengan berbagai lembaga keuangan. Hal ini menambah kompleksitas sistem. Oleh karena itu, koordinasi antar lembaga menjadi penting (Davis, 1989). Batasan nominal transaksi juga menjadi kendala dalam penggunaan QRIS. Regulasi yang membatasi jumlah transaksi dapat menghambat fleksibilitas bisnis. Hal ini terutama dirasakan oleh pelaku usaha skala besar. QRIS lebih cocok untuk transaksi kecil hingga menengah. Oleh karena itu, diperlukan penyesuaian kebijakan (Adiyanti & Pudjihardjo, 2014).

Ketidaksiapan merchant dalam menggunakan teknologi juga menjadi masalah. Tidak semua pelaku usaha memiliki kemampuan digital yang memadai. Hal ini dapat menyebabkan kesalahan dalam pengelolaan transaksi. Pelatihan dan pendampingan menjadi solusi yang diperlukan. Dengan demikian, penggunaan QRIS dapat lebih optimal (Febriyantoro & Arisandi, 2018). Ketersediaan listrik juga memengaruhi operasional QRIS. Tanpa listrik, perangkat tidak dapat digunakan untuk transaksi. Hal ini menjadi kendala di daerah tertentu. Oleh karena itu, diperlukan solusi alternatif seperti sistem offline. Inovasi ini dapat meningkatkan ketahanan sistem (Baskara & Hariyadi, 2014).

Integrasi sistem antar bank dan penyedia layanan juga menjadi tantangan. Perbedaan sistem dapat menyebabkan keterlambatan transaksi. Hal ini dapat mengurangi kepercayaan pengguna. Oleh karena itu, standarisasi sistem menjadi penting. QRIS hadir sebagai solusi, namun masih perlu penyempurnaan (Davis, 1989). Biaya operasional juga menjadi pertimbangan dalam penggunaan QRIS. Merchant harus menanggung biaya layanan tertentu. Hal ini dapat memengaruhi keuntungan usaha. Oleh karena itu, kebijakan biaya harus disesuaikan. Tujuannya agar tetap mendorong adopsi teknologi (Adiyanti & Pudjihardjo, 2014). Kualitas layanan juga memengaruhi pengalaman pengguna. Sistem yang lambat atau sering error dapat menurunkan kepuasan. Hal ini berdampak pada loyalitas pengguna. Oleh

karena itu, peningkatan kualitas layanan menjadi prioritas. Hal ini penting untuk keberlanjutan sistem (Febriyantoro & Arisandi, 2018). Pengelolaan data transaksi juga menjadi tantangan operasional. Data yang tidak terkelola dengan baik dapat menimbulkan masalah. Oleh karena itu, sistem manajemen data harus diperkuat. Hal ini penting untuk mendukung analisis dan pengambilan keputusan. Dengan demikian, sistem dapat berjalan lebih efisien (Baskara & Hariyadi, 2014).

Koordinasi antar pihak menjadi kunci dalam mengatasi risiko operasional. Pemerintah, bank, dan penyedia layanan harus bekerja sama. Hal ini untuk memastikan sistem berjalan dengan baik. Kolaborasi ini penting dalam ekosistem digital. Dengan demikian, risiko dapat diminimalkan (Davis, 1989). Inovasi teknologi terus berkembang untuk mengatasi berbagai kendala. Pengembangan QRIS dinamis menjadi salah satu solusi. Sistem ini dapat mengurangi risiko human error. Selain itu, fitur keamanan juga terus ditingkatkan. Hal ini menunjukkan komitmen dalam meningkatkan kualitas layanan (Adiyanti & Pudjihardjo, 2014).

Risiko operasional dan infrastruktur dalam penggunaan QRIS merupakan tantangan yang kompleks. Risiko ini memerlukan penanganan yang terintegrasi dan berkelanjutan. Peningkatan infrastruktur, regulasi, dan literasi menjadi kunci utama. Dengan demikian, transformasi digital dapat berjalan dengan optimal. QRIS dapat menjadi solusi pembayaran yang andal di masa depan.

5. KESIMPULAN

Quick Response Code Indonesian Standard (QRIS) merupakan inovasi standar nasional yang sukses memberikan lompatan besar dalam mempermudah dan meningkatkan keamanan ekosistem pembayaran digital di Indonesia. Dengan menyatukan berbagai metode pembayaran ke dalam satu sistem terstandardisasi, QRIS mampu memberikan perlindungan data yang lebih terintegrasi bagi para penggunanya. Kendati demikian, adopsi teknologi ini tidak luput dari berbagai risiko nyata yang wajib diwaspadai, baik oleh pembeli maupun penjual. Tantangan utama dalam penggunaan QRIS bersumber dari dua faktor, yaitu celah kejahatan siber dan ketergantungan pada infrastruktur teknis. Dari sisi keamanan, pelaku kejahatan kerap memanfaatkan kemiripan visual kode QR untuk melakukan penipuan, seperti menempelkan stiker QRIS palsu di tempat umum, melakukan *quishing* (pancingan situs web tiruan untuk menguras saldo), hingga menyisipkan *malware* berbahaya untuk meretas data perbankan di ponsel pintar pengguna.

Sementara dari sisi operasional dan teknis, model QRIS statis masih rentan terhadap kesalahan manusia (*human error*) akibat salah input nominal yang berujung pada rumitnya proses pengembalian dana (*refund*). Selain itu, sistem ini menuntut ketergantungan mutlak pada stabilitas jaringan internet dan server. Gangguan pada salah satu jalur komunikasi atau server perbankan dapat melumpuhkan transaksi seketika atau memicu ketidaksesuaian data, seperti saldo konsumen yang sudah terpotong namun belum terdata di pihak penjual. Di sisi lain, kebijakan regulasi mengenai batasan limit nominal juga membuat QRIS kurang fleksibel untuk mengakomodasi transaksi bisnis berskala besar. Meskipun QRIS menawarkan efisiensi yang sangat tinggi sebagai alat pembayaran non-tunai modern, pemanfaatannya harus tetap diiringi dengan kehati-hatian, ketelitian tinggi sebelum menyetujui transaksi, serta kesadaran untuk selalu menyiapkan uang tunai darurat ketika sistem digital mengalami kendala di lapangan.

REFERENSI

- Adiyanti, A. I., & Pudjihardjo, M. (2014). Pengaruh pendapatan, manfaat, kemudahan penggunaan, daya tarik promosi, dan kepercayaan terhadap minat menggunakan layanan *e-money*. *Jurnal Ilmiah Mahasiswa FEB*, 3(1).
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Alsyukri, M. R. (2021). *Pengaruh kemudahan, gaya hidup dan perilaku konsumtif terhadap keputusan penggunaan e-wallet selama masa pandemi COVID-19* (Skripsi). STIE Malangkucecwara.
- Bank Indonesia. (2020). *Blueprint Sistem Pembayaran Indonesia 2025: Menavigasi sistem pembayaran nasional di era digital*. Bank Indonesia.
- Bank Indonesia. (2021). *QR Code Indonesian Standard (QRIS): Satu QR Code untuk semua pembayaran*. Bank Indonesia.
- Baskara, I. P., & Hariyadi, G. T. (2014). *Analisis pengaruh kepercayaan, keamanan, kualitas pelayanan, dan persepsi akan risiko terhadap keputusan pembelian melalui situs jejaring sosial (social networking websites)* (Skripsi). Universitas Dian Nuswantoro.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482. <https://doi.org/10.25300/MISQ/2013/37:2.3>
- Chaney, D. (2003). *Lifestyle: Suatu pengantar komprehensif*. Jelasutra.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- Febriyantoro, M. T., & Arisandi, D. (2018). Pemanfaatan digital marketing bagi usaha mikro, kecil dan menengah pada era Masyarakat Ekonomi ASEAN. *JMD: Jurnal Riset Manajemen & Bisnis Dewantara*, 1(2), 61–76. <https://doi.org/10.26533/jmd.v1i2.175>

- Jogiyanto, H. M. (2007). *Sistem informasi keperilakuan*. Andi.
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544–564. <https://doi.org/10.1016/j.dss.2007.07.001>
- Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, 61, 404–414. <https://doi.org/10.1016/j.chb.2016.03.030>
- Otoritas Jasa Keuangan. (2022). *Perkembangan fintech dan transformasi digital sektor jasa keuangan di Indonesia*. Otoritas Jasa Keuangan.
- Parasuraman, A. (2000). Technology readiness index (TRI): A multiple-item scale to measure readiness to embrace new technologies. *Journal of Service Research*, 2(4), 307–320. <https://doi.org/10.1177/109467050024001>
- Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom. *International Journal of Information Management*, 35(6), 860–873. <https://doi.org/10.1016/j.ijinfomgt.2015.08.009>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. <https://doi.org/10.2307/30036540>
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157–178. <https://doi.org/10.2307/41410412>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- World Bank. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank. <https://doi.org/10.1596/978-1-4648-1897-4>