Ar-Rasyid: Jurnal Publikasi Penelitian Ilmiah - ISSN:2348-8635
https://journal.sahakreasindo.co.id/index.php/ar-rasyid
Volume 1 Nomor 6 – Tahun 2025 - Halaman 797-805

KESADARAN KEAMANAN KONSUMEN DALAM PENGGUNAAN TRANSAKSI DIGITAL QRIS SEBAGAI PERLINDUNGAN KONSUMEN DIGITAL: STUDI KASUS PENIPUAN QRIS PADA PEDAGANG PAKAIAN DI KECAMATAN KIBIN, KABUPATEN SERANG

Sri Lidya Agustin[1], Anita Fitri[2], Franoto Siswantoro[3], Faizal Alpiansyah[4]
Jurusan Ilmu Hukum Fakultas Hukum, Universitas Pamulang PSDKU Serang [1-4]
Email: srilidya.law@gmail.com

ABSTRACT

The development of digital transactions through the Indonesian Standard Quick Response Code (QRIS) payment system has boosted transaction efficiency, particularly in the micro and small business sector. However, the increase in QRIS usage has also been accompanied by a rise in digital transaction fraud cases, which are generally carried out through social engineering. One such QRIS fraud case occurred in Kibin Subdistrict, Serang Regency, affecting merchants who were users of digital transaction services. This study aims to analyze the forms of QRIS fraud and examine consumer security awareness in the use of digital transactions as part of digital consumer protection. The research method used is normative-empirical legal research with a regulatory and case study approach, supported by primary data in the form of interviews with three merchants who were victims of QRIS fraud. The results of the study show that QRIS fraud occurs not because of system failure, but rather due to low consumer security awareness and understanding of digital transaction mechanisms. Digital consumer protection in Indonesia is still oriented towards system security and has not optimally accommodated the aspect of user vigilance. Therefore, it is necessary to strengthen digital consumer protection that is not only technological in nature, but also based on increasing public security awareness.

Keywords : *QRIS, Security Awareness, Digital Consumer Protection, Electronic Transaction Fraud.*

ABSTRAK

Perkembangan transaksi digital melalui sistem pembayaran Quick Response Code Indonesian Standard (QRIS) telah mendorong efisiensi transaksi, khususnya di

sektor usaha mikro dan kecil. Namun, peningkatan penggunaan QRIS juga diikuti dengan maraknya kasus penipuan transaksi digital yang umumnya dilakukan melalui modus rekayasa sosial (social engineering). Salah satu kasus penipuan QRIS terjadi di Kecamatan Kibin, Kabupaten Serang, yang menimpa pedagang sebagai pengguna layanan transaksi digital. Penelitian ini bertujuan untuk menganalisis bentuk penipuan QRIS serta mengkaji kesadaran keamanan konsumen dalam penggunaan transaksi digital sebagai bagian dari perlindungan konsumen digital. Metode penelitian yang digunakan adalah penelitian hukum normatif-empiris dengan pendekatan peraturan perundang-undangan dan studi kasus, yang didukung oleh data primer berupa wawancara terhadap tiga pedagang korban penipuan QRIS. Hasil penelitian menunjukkan bahwa penipuan QRIS terjadi bukan akibat kegagalan sistem, melainkan rendahnya kesadaran keamanan dan pemahaman konsumen terhadap mekanisme transaksi digital. Perlindungan konsumen digital di Indonesia masih berorientasi pada keamanan sistem dan belum secara optimal mengakomodasi aspek kewaspadaan pengguna. Oleh karena itu, diperlukan penguatan perlindungan konsumen digital yang tidak hanya bersifat teknologis, tetapi juga berbasis peningkatan kesadaran keamanan masyarakat.

Kata Kunci : *QRIS, Kesadaran Keamanan, Perlindungan Konsumen Digital, Penipuan Transaksi Elektronik.*

PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam sistem pembayaran di Indonesia. Salah satu bentuk inovasi di bidang sistem pembayaran adalah hadirnya Quick Response Code Indonesian Standard (QRIS) yang bertujuan untuk menyederhanakan transaksi non-tunai dan mendorong inklusi keuangan, khususnya bagi pelaku usaha mikro, kecil, dan menengah. Pembayaran digital menggunakan uang elektronik melalui platform digital menggunakan metode ransfer bank, scan QR, atau dompet elektronik tertentu. Pembayaran melalui internet lebih cepat, efisien, dan aman. Pembayaran digital di Indonesia juga kian berkembang.

Dapat dilihat dari pengelolaan infrastruktur pembayaran yang terintegrasi serta kebijakan pemerintah sebagai contoh QRIS dan BI-FAST. 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. 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. 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.[1] Penggunaan QRIS yang semakin masif telah menjadikan transaksi digital sebagai bagian dari aktivitas ekonomi sehari-hari masyarakat. Namun demikian, di balik kemudahan yang ditawarkan, transaksi digital juga membuka ruang bagi munculnya berbagai bentuk kejahatan berbasis teknologi informasi.[2] Dalam praktiknya, kejahatan transaksi digital tidak selalu dilakukan melalui peretasan sistem (hacking), melainkan kerap memanfaatkan kelemahan pada aspek manusia sebagai pengguna sistem. Modus kejahatan yang umum digunakan adalah rekayasa sosial (social engineering), yakni teknik manipulasi psikologis yang bertujuan untuk mengecoh korban agar secara sukarela melakukan tindakan yang merugikan dirinya sendiri.

Fenomena tersebut tercermin dalam kasus penipuan QRIS yang terjadi di Kecamatan Kibin, Kabupaten Serang. Berdasarkan hasil wawancara terhadap pedagang pakaian yang menjadi korban, penipuan dilakukan dengan modus pelaku berpura-pura sebagai konsumen yang hendak melakukan transaksi belanja secara daring. Pelaku kemudian mengarahkan korban untuk memindai kode QRIS dengan dalih sebagai proses pembayaran dari pihak pelaku. Ketidaktahuan korban mengenai mekanisme kerja QRIS menyebabkan korban mengikuti instruksi tersebut, yang pada akhirnya justru mengakibatkan saldo rekening korban terdebit dan berpindah ke rekening pelaku. Setelah transaksi berhasil, pelaku memutus komunikasi dan tidak dapat dihubungi kembali.

Kasus tersebut menunjukkan bahwa kerugian konsumen tidak selalu disebabkan oleh kegagalan sistem pembayaran atau kelalaian penyedia jasa, melainkan oleh rendahnya kesadaran keamanan dan pemahaman pengguna terhadap cara kerja transaksi digital. Dalam konteks ini, konsumen khususnya pedagang kecil berada pada posisi yang rentan sebagai pihak yang kurang memiliki literasi dan kewaspadaan terhadap risiko transaksi elektronik.

Di sisi lain, kerangka hukum perlindungan konsumen digital di Indonesia, baik

[1] Kristanty, Desy Natalia. "Tren dan tantangan keamanan bertransaksi dengan qris dalam era transformasi sistem pembayaran digital." *Jurnal Syntax Admiration* 5.10 (2024): 3923-3933.
[2] Ma'arif, M. Fadhli, et al. "Security Risk Analysis of QRIS Implementation in Public Locations Using ISO 31000: 2018 Framework." *Journal of Applied Informatics and Computing* 9.4 (2025): 1670-1680.

melalui Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Konsumen, maupun regulasi di bidang sistem pembayaran, masih cenderung menitikberatkan pada aspek keamanan sistem dan tanggung jawab penyelenggara jasa. Aspek kesadaran keamanan pengguna sebagai bagian dari perlindungan konsumen belum mendapatkan perhatian yang memadai dalam pengaturan maupun implementasi kebijakan.

Penelitian terdahulu oleh Hilery (2024) di era pembayaran digital, memastikan keamanan transaksi merupakan hal yang krusial. Penelitian ini bertujuan untuk memastikan keamanan transaksi dalam era pembayaran digital, khususnya pada metode QRIS. Metode yang digunakan adalah metode yuridis normatif dengan pendekatan konseptual dan statute. Data yang digunakan berasal dari sumber sekunder, yaitu literatur dan referensi terkait. Analisis yang digunakan adalah deskriptif kualitatif dengan metode berpikir deduktif. Berdasarkan temuan penelitian, direkomendasikan langkah-langkah untuk meningkatkan keamanan transaksi QRIS, seperti metode otentikasi yang lebih kuat, protokol enkripsi yang kuat, pemantauan terus menerus, dan sistem deteksi penipuan secara *real-time*.[3]

Penelitian ini berbeda dari studi sebelumnya dengan fokus pada pemahaman yang

lebih mendalam tentang kesadaran keamanan konsumen dalam penggunaan transaksi digital QRIS sebagai instrumen perlindungan konsumen digital dan bagaimana bentuk kejahatan penipuan untuk mencegah pengulangan kasus yang sama. Penelitian ini diharapkan dapat memberikan kontribusi dalam memahami bahwa perlindungan konsumen digital tidak hanya bersifat teknis dan normatif, tetapi juga harus memperhatikan faktor manusia sebagai subjek utama dalam transaksi elektronik.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif-empiris. Pendekatan normatif digunakan untuk mengkaji dan menganalisis ketentuan peraturan perundang-undangan yang berkaitan dengan transaksi elektronik, sistem pembayaran QRIS, dan perlindungan konsumen digital. Pendekatan empiris digunakan untuk melihat bagaimana ketentuan hukum tersebut bekerja dalam praktik, khususnya dalam kasus penipuan QRIS yang terjadi di Kecamatan Kibin, Kabupaten Serang.

Sumber data dalam penelitian ini terdiri atas data Primer, yaitu data yang diperoleh secara langsung dari lapangan melalui wawancara dengan pedagang pakaian di Kecamatan Kibin, Kabupaten Serang, yang mengalami penipuan QRIS.

[3] Hilery, P. M., Latuconsina, M. B., Kristanty, D. N., Renhoran, M. I., Saputra, B. A., & Tilaar, R. M. A. (2024). "Tren dan Tantangan: Keamanan Bertransaksi Dengan Qris Dalam Era Transformasi Sistem Pembayaran Digital". *Jurnal Kajian Ilmiah Multidisipliner*, 8(7).

Wawancara dilakukan secara semi terstruktur untuk menggali pemahaman korban mengenai penggunaan QRIS, kronologi kejadian, serta persepsi korban terhadap risiko transaksi digital. Data Sekunder, yaitu data yang diperoleh dari peraturan perundang-undangan terkait transaksi elektronik dan perlindungan konsumen;

Pendekatan normatif dalam penelitian ini menggunakan pendekatan perundang-undangan (statute approach), yaitu dengan menelaah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta peraturan Bank Indonesia dan Otoritas Jasa Keuangan yang mengatur sistem pembayaran dan perlindungan konsumen.

Pendekatan empiris dilakukan melalui studi kasus, dengan mengkaji secara langsung pengalaman pedagang yang menjadi korban penipuan QRIS untuk memperoleh gambaran faktual mengenai tingkat kesadaran keamanan dalam penggunaan transaksi digital. Data yang diperoleh dianalisis secara kualitatif dengan metode deskriptif-analitis. Analisis dilakukan dengan cara mengaitkan temuan empiris dari lapangan dengan ketentuan hukum yang berlaku, sehingga dapat diketahui kesenjangan antara norma hukum (das sollen) dan praktik yang terjadi (das sein) dalam perlindungan konsumen digital.

HASIL DAN PEMBAHASAN

QRIS merupakan standar nasional pembayaran berbasis kode QR yang berfungsi sebagai sarana transaksi elektronik. Dalam konteks hukum, QRIS termasuk bagian dari sistem elektronik sebagaimana dimaksud dalam Undang-Undang Informasi dan Transaksi Elektronik. Oleh karena itu, segala bentuk penyalahgunaan QRIS yang menimbulkan kerugian dapat dikualifikasikan sebagai kejahatan transaksi elektronik.

Penipuan QRIS yang terjadi di Kecamatan Kibin tidak dilakukan melalui peretasan sistem, melainkan melalui rekayasa sosial (social engineering). Pelaku memanfaatkan ketidaktahuan korban terhadap mekanisme transaksi QRIS dengan menyampaikan informasi yang tidak benar dan menyesatkan. Modus ini menunjukkan bahwa kejahatan transaksi digital tidak selalu bersifat teknis, tetapi juga dapat bersumber dari manipulasi perilaku pengguna.

Secara yuridis, perbuatan tersebut memenuhi unsur penipuan sebagaimana diatur dalam Pasal 378 KUHP, serta dapat dikualifikasikan sebagai penyebaran informasi bohong yang mengakibatkan kerugian konsumen dalam transaksi elektronik sebagaimana diatur dalam Pasal 28 ayat (1) Undang-Undang ITE.

Berdasarkan hasil wawancara terhadap pedagang pakaian yang menjadi korban penipuan QRIS, ditemukan pola modus yang kreati. Pelaku menghubungi korban melalui sambungan telepon dan mengaku sebagai konsumen yang hendak

melakukan pembelian secara daring. Dalam komunikasi tersebut, pelaku memberikan instruksi kepada korban untuk memindai kode QRIS bayar yang dibuat pelaku dengan alasan sebagai proses penerimaan pembayaran.

Korban yang tidak memahami bahwa pemindaian QRIS bayar justru merupakan tindakan melakukan pembayaran, mengikuti instruksi pelaku tanpa kecurigaan. Setelah korban melakukan pemindaian, saldo rekening korban secara otomatis terdebit dan berpindah ke rekening pelaku. Setelah transaksi berhasil, pelaku segera memutus komunikasi dan tidak dapat dihubungi kembali. Korban menyatakan bahwa banyak pedagang di Kecamatan Kibin yang mengalami kejadian serupa, hal tersebut dikarenakan pemahaman tentang penggunaan QRIS bayar dan QRIS transfer belum disosialisasikan dari pihak penyedia layanan.

Korban sudah melakukan upaya dengan mendatangi cabang bank layanan tempat korban menggunakan transaksi penjualannya. Pihak perbankan akan melakukan proses pelaporan terlebih dahulu dan proses investigasi aliran dana dalam upaya mengetahui pelaku dan dapat melakukan proses pemblokiran. Terkait proses pelaporan tersebut, korban juga menyatakan bahwa pihak perbankan membutuhkan dokumen pendukung seperti surat laporan kepolisian yang menyatakan terjadi transaksi penipuan pada korban, surat keterangan dan surat permohonan pemblokiran yang ditanda tangani di atas meterai.

Kasus tersebut menunjukkan bahwa penipuan QRIS bukan merupakan peristiwa insidental, melainkan mencerminkan adanya celah struktural dalam pemahaman dan kewaspadaan pengguna QRIS, khususnya di kalangan pedagang kecil. Kesadaran keamanan *(security awareness*) merupakan kemampuan pengguna untuk memahami risiko serta bertindak secara hati-hati dalam menggunakan teknologi digital. Dalam kasus penipuan QRIS di Kecamatan Kibin, hasil wawancara menunjukkan bahwa para korban memiliki pemahaman yang sangat terbatas mengenai mekanisme transaksi QRIS.

Para pedagang umumnya hanya memahami QRIS sebagai alat untuk mempermudah pembayaran, tanpa mengetahui perbedaan mendasar antara menerima pembayaran dan melakukan pembayaran. Ketergantungan pada komunikasi verbal dan kepercayaan terhadap pihak yang mengaku sebagai konsumen memperbesar peluang terjadinya penipuan.

Rendahnya kesadaran keamanan ini menempatkan konsumen pada posisi yang sangat rentan. Dalam perspektif hukum perlindungan konsumen, kondisi tersebut menunjukkan bahwa konsumen belum sepenuhnya mampu menjalankan perannya sebagai subjek hukum yang sadar akan hak dan kewajibannya dalam transaksi digital.

Perlindungan konsumen digital di Indonesia pada dasarnya telah diatur melalui berbagai peraturan perundang-undangan. Namun, perlindungan tersebut masih lebih berfokus pada aspek keamanan sistem dan tanggung jawab

penyelenggara jasa. Dalam kasus penipuan QRIS, sistem pembayaran berfungsi sebagaimana mestinya dan tidak mengalami gangguan teknis.

Kondisi ini menunjukkan bahwa kerugian konsumen tidak selalu dapat diatasi melalui mekanisme perlindungan sistemik. Perlindungan represif melalui penegakan hukum sering kali mengalami kendala, seperti sulitnya pelacakan pelaku dan pengembalian dana. Akibatnya, konsumen tetap menanggung kerugian meskipun secara hukum berstatus sebagai korban. Hal ini mengindikasikan bahwa perlindungan konsumen digital yang ada belum sepenuhnya efektif dalam menghadapi kejahatan berbasis rekayasa sosial.

Berdasarkan temuan penelitian, perlindungan konsumen digital perlu direkonstruksi dengan menempatkan kesadaran keamanan pengguna sebagai elemen utama. Perlindungan tidak cukup hanya mengandalkan keamanan sistem, tetapi juga harus mendorong peningkatan literasi dan kewaspadaan konsumen.

Upaya tersebut dapat dilakukan melalui kewajiban edukasi aktif bagi penyedia QRIS, penyampaian peringatan risiko yang lebih eksplisit dalam aplikasi pembayaran, serta pelibatan pemerintah daerah dalam program literasi digital bagi pelaku usaha kecil. Dengan demikian, perlindungan konsumen digital dapat bersifat lebih substantif dan preventif dalam mencegah terjadinya penipuan transaksi elektronik.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat disimpulkan bahwa penipuan QRIS yang terjadi di Kecamatan Kibin, Kabupaten Serang merupakan bentuk kejahatan transaksi digital yang dilakukan melalui modus rekayasa sosial (*social engineering*). Penipuan tersebut tidak disebabkan oleh kegagalan atau kelemahan sistem pembayaran QRIS, melainkan oleh penyalahgunaan kepercayaan dan rendahnya pemahaman pengguna terhadap mekanisme transaksi digital.

Hasil wawancara terhadap pedagang korban menunjukkan bahwa tingkat kesadaran keamanan dalam penggunaan QRIS masih rendah. Para pedagang belum memahami secara memadai perbedaan antara tindakan menerima pembayaran dan melakukan pembayaran melalui QRIS, sehingga mudah dipengaruhi oleh informasi menyesatkan yang disampaikan pelaku. Kondisi ini menempatkan konsumen pada posisi rentan sebagai pihak yang lemah dalam transaksi digital.

Selain itu, penelitian ini menemukan bahwa perlindungan konsumen digital di Indonesia masih berorientasi pada aspek keamanan sistem dan tanggung jawab penyelenggara jasa pembayaran. Perlindungan yang bersifat preventif dan represif belum sepenuhnya menjangkau aspek kesadaran keamanan pengguna sebagai subjek utama transaksi elektronik. Akibatnya, meskipun konsumen secara hukum berstatus sebagai korban, pemulihan kerugian akibat penipuan QRIS masih sulit

direalisasikan.

Dengan demikian, kesadaran keamanan konsumen merupakan elemen penting yang tidak terpisahkan dari konsep perlindungan konsumen digital. Tanpa adanya peningkatan kesadaran dan kewaspadaan pengguna, perlindungan hukum yang bersifat normatif berpotensi menjadi tidak efektif dalam mencegah terjadinya penipuan transaksi digital.

Saran

Berdasarkan hasil penelitian ini, diperlukan penguatan perlindungan konsumen digital yang tidak hanya berfokus pada aspek keamanan sistem pembayaran, tetapi juga pada peningkatan kesadaran keamanan pengguna transaksi digital. Pemerintah dan regulator diharapkan dapat merumuskan kebijakan yang secara eksplisit menempatkan edukasi dan literasi keamanan transaksi digital sebagai bagian integral dari perlindungan konsumen, khususnya bagi pelaku usaha mikro dan kecil yang menjadi pengguna utama QRIS. Upaya tersebut dapat dilakukan melalui program sosialisasi yang berkelanjutan dan mudah diakses oleh masyarakat.

Selain itu, penyelenggara jasa pembayaran dan perbankan perlu meningkatkan peran aktif dalam memberikan edukasi kepada pengguna QRIS mengenai mekanisme transaksi dan potensi risiko penipuan. Edukasi tersebut tidak hanya disampaikan pada tahap awal penggunaan layanan, tetapi juga melalui peringatan risiko yang jelas dan mudah dipahami dalam aplikasi pembayaran digital. Dengan demikian, pengguna diharapkan dapat lebih waspada terhadap instruksi transaksi yang tidak lazim dan berpotensi merugikan.

Di sisi lain, konsumen atau pedagang sebagai pengguna transaksi digital juga perlu meningkatkan kewaspadaan dan pemahaman dasar mengenai cara kerja QRIS. Sikap kehati-hatian dalam menerima informasi atau instruksi transaksi dari pihak yang tidak dikenal menjadi penting untuk meminimalkan risiko penipuan. Kesadaran bahwa tidak semua kemudahan transaksi digital bebas dari risiko merupakan langkah awal dalam membangun perlindungan konsumen yang lebih efektif.

Penelitian selanjutnya diharapkan dapat memperluas cakupan wilayah dan jumlah responden agar memperoleh gambaran yang lebih komprehensif mengenai tingkat kesadaran keamanan konsumen dalam transaksi digital. Pendekatan empiris yang lebih luas diharapkan mampu memberikan rekomendasi kebijakan yang lebih aplikatif dalam rangka memperkuat perlindungan konsumen digital di Indonesia.

DAFTAR PUSTAKA

Apriansyah, N., “Perlindungan Konsumen dalam Transaksi Elektronik di Indonesia,” *Jurnal Hukum dan Pembangunan*, Vol. 49 No. 2, 2019.

Kristanty, Desy Natalia. "Tren dan tantangan keamanan bertransaksi dengan qris

dalam era transformasi sistem pembayaran digital." *Jurnal Syntax Admiration* 5.10 (2024).

Ma'arif, M. Fadhli, et al. "Security Risk Analysis of QRIS Implementation in Public Locations Using ISO 31000: 2018 Framework." *Journal of Applied Informatics and Computing* 9.4 (2025).

P. M., Hilery, Latuconsina, M. B., Kristanty, D. N., Renhoran, M. I., Saputra, B. A., & Tilaar, R. M. A. (2024). "Tren dan Tantangan: Keamanan Bertransaksi Dengan Qris Dalam Era Transformasi Sistem Pembayaran Digital". *Jurnal Kajian Ilmiah Multidisipliner*, 8(7).

Pratama, R. A., "Kejahatan Siber Berbasis Rekayasa Sosial dalam Transaksi Digital," *Jurnal Ilmu Hukum*, Vol. 15 No. 1, 2021.

Sutedi, Adrian. "Perlindungan Konsumen Digital dalam Sistem Pembayaran Non-Tunai," *Jurnal Legislasi Indonesia*, Vol. 18 No. 3, 2021.