Teaching and Learning Journal of Mandalika, Vol. 4, No. 2, e-ISSN: 2721-9666, p-ISSN: 2828-7126
Available online at: http://ojs.cahayamandalika.com/index.php/teacher
Akreditasi Sinta 5, SK. Nomor: 152/E/KPT/2023

TRANSAKSI KEUANGAN DIGITAL MENGGUNAKAN QRIS DITINJAU DARI ASPEK HUKUM

Fridayani[1], Benny Cuaca[2]
[1]Universitas Pamulang, Banten, [2]Universitas Pelita Harapan Surabaya, Indonesia
*Corresponding Author e-mail: dosen02918@unpam.ac.id, bennycuaca@yahoo.com

Article History
Received: April
Revised: May
Published: May

Key Words:
Legal Aspects, Financial Records, Digital, QRIS

Abstract: *One sector that is experiencing changes in the current digital era is the financial sector, where payment transactions are starting to be carried out through digital systems, some of which use the QRIS system. Payment transactions via QRIS can speed up transactions and reduce operational costs, especially for commercial players. However, the use of QRIS has clearly given rise to what is called digital crime, which can harm users (QRIS consumers) by destroying the QR code and "undoing" the actions carried out by the perpetrator. This research uses qualitative research with data collection techniques through library research which is analyzed qualitatively. The results of the first research concluded that legal protection for QRIS users based on current regulations includes PJSP having valid legal status, PJSP must create a financial innovation ecosystem with good digital credentials in the financial services sector and be registered with the Financial Services Authority. OJK and QRIS users (consumers) enjoy rights based on the provisions of the Consumer Protection Law and the ITE Law. Second, the legal consequences of misusing consumer data in digital transactions using QRIS make the perpetrator liable for professional misconduct. For losses incurred, QRIS users can file a civil lawsuit or compensation through PJSP, as stipulated in Article 12, paragraph 1, Law no. 27, 2022 on personal data protection.*

Kata Kunci:
Aspek Hukum, Catatan Keuangan, Digital, QRIS

Abstrack: Salah satu sektor yang mengalami perubahan di era digital saat ini adalah sektor keuangan, dimana transaksi pembayaran mulai dilakukan melalui sistem digital, beberapa di antaranya menggunakan sistem QRIS. Transaksi pembayaran melalui QRIS dapat mempercepat transaksi dan menekan biaya operasional, khususnya bagi pelaku komersial. Namun, penggunaan QRIS jelas telah memunculkan apa yang disebut kejahatan digital, yaitu dapat merugikan pengguna (konsumen QRIS) dengan menghancurkan kode QR dan "membatalkan" tindakan yang dilakukan oleh pelaku. Penelitian ini menggunakan penelitian kualitatif dengan teknik pengumpulan data melalui penelitian kepustakaan (library research) yang dianalisis secara kualitatif. Hasil riset pertama menyimpulkan bahwa perlindungan hukum bagi pengguna QRIS berdasarkan regulasi yang berlaku saat ini antara lain PJSP memiliki status hukum yang sah, PJSP harus menciptakan ekosistem inovasi keuangan dengan kredensial digital yang baik di sektor jasa keuangan dan terdaftar di Otoritas Jasa Keuangan. Pengguna OJK dan QRIS (konsumen) menikmati hak berdasarkan ketentuan UU Perlindungan Konsumen dan UU ITE. Kedua, akibat hukum penyalahgunaan data konsumen dalam transaksi digital menggunakan QRIS membuat pelaku bertanggung jawab atas kesalahan profesional. Atas kerugian yang terjadi, pengguna QRIS dapat mengajukan gugatan perdata atau ganti rugi melalui PJSP, sebagaimana diatur dalam Pasal 12 ayat 1 UU No. 27 Tahun 2022 tentang perlindungan data pribadi.

Pendahuluan

Ketika sekelompok pemuda kelahiran tahun 1980 memulai revolusi, era digital pun mulai berkembang. Munculnya digitalisasi menandai dimulainya era informasi digital, atau terciptanya teknologi baru yang lebih maju. Digitalisasi adalah istilah yang digunakan untuk menggambarkan modernisasi atau inovasi penggunaan teknologi. Hal ini sering dikaitkan

dengan keberadaan internet dan teknologi komputer sebagai alat yang mampu melakukan apa saja untuk memudahkan pekerjaan manusia (Setiawan, 2022).

Fenomena global revolusi digital telah banyak mengubah cara hidup dan interaksi masyarakat, khususnya di industri keuangan, di banyak negara, termasuk Indonesia. Penerapan pola kehidupan dan interaksi manusia dengan menggunakan berbagai versi basis ekonomi digital relatif mudah dan efisien. Bagi masyarakat yang biasanya terlibat dalam aktivitas ekonomi model relasional, hal ini menghadirkan peluang sekaligus tantangan, terutama bagi mereka yang terlibat dalam berbagai inkarnasi basis ekonomi digital, seperti pemilik modal, penyedia layanan platform, dan konsumen (BPHN, 2022).

Teknologi berkembang begitu pesat sehingga mengubah perilaku manusia dan menjadikan transaksi sepenuhnya digital. Mengadopsi teknologi digital bukan hanya sekedar cara untuk tetap mengikuti kemajuan informasi; yang lebih penting lagi, teknologi digital dapat membantu masyarakat dalam berbagai hal, termasuk dalam melakukan transaksi keuangan. Pembayaran terbatas dan layanan sistem keuangan, seperti transfer uang, penyimpanan sejumlah uang, dan transaksi pembayaran, menguntungkan penyedia layanan dan pelanggan ketika ditawarkan melalui sistem keuangan digital. Hal ini mengurangi bahaya kerugian bagi nasabah dan membuat transaksi keuangan menjadi cepat, aman, dan efisien (Setiawan, 2022).Dunia perbankan merupakan salah satu sektor yang membutuhkan transformasi digital. Setidaknya ada 3 (tiga) aspek utama yang mendorong perkembangan transformasi digital perbankan di Indonesia, yaitu peluang digital, perilaku digital, dan transaksi digital. Akselerasi perbankan digital di Indonesia ditandai dengan semakin meningkatnya penggunaan pembayaran digital melalui QRIS (Indonesian Standard for Quick Response Codes), (Saraswati, 2023).

Dilihat dari perspektif transaksi digital yang menjadi fokus kajian ini, Bank Indonesia (BI) mencatat hingga Oktober 2023, nominal transaksi QRIS akan meningkat sebesar 186,08% year-on-year (y-o-y) atau mencapai Rp 24,97 triliun (Irawati, 2023). Berdasarkan data Bank Indonesia, hingga 83% volume transaksi QRIS didominasi oleh usaha mikro, kecil, dan menengah (UMKM). Jumlah ini seharusnya meningkat dibandingkan tahun-tahun sebelumnya. Perdagangan melalui QRIS dapat mendorong pertumbuhan ekonomi Indonesia yang lebih efektif. Memang transaksi keuangan melalui QRIS memungkinkan transaksi menjadi lebih cepat dan dapat menekan biaya operasional. Menurut Profesor Dodi W. Irawanto, pakar UMKM dan SDM Universitas Brawijaya (UB), mengatakan sistem digitalisasi semakin memudahkan pelaku UMKM dalam meningkatkan efisiensi dan produktivitasnya. Dengan hadirnya QRIS, pelaku UMKM tidak perlu lagi membuat laporan

keuangan konvensional namun juga dapat terintegrasi dengan platform pelaporan keuangan yang prosesnya lebih sederhana. Selain itu, pencatatan laporan keuangan secara real time dapat memberikan peluang efisiensi dengan alokasi anggaran yang lebih akurat (Fizriyani, 2023).

Transaksi keuangan sistem digital menggunakan QRIS jelas tidak selalu memberikan dampak positif bagi konsumen keuangan digital, seperti disebutkan di atas. Memang QRIS jelas memiliki kelemahan yang bisa dimanfaatkan oleh pihak-pihak tertentu untuk mendapatkan keuntungan ilegal, sehingga berpotensi merugikan konsumen keuangan digital. Kondisi tersebut sejalan dengan kutipan voi.id bahwa penggunaan QRIS untuk transaksi pembayaran akan menghadapi ancaman kejahatan digital. Memang sangat sulit bagi mata manusia untuk membedakan kode QR asli dan palsu. Memang ternyata QR Code resmi asli penjual bisa dimodifikasi dan ditambah link virus dan malware yang mampu mencuri akun konsumen (Voi.id, 2023)

Metode baru kejahatan keuangan digital yang menggunakan sistem QRIS melalui kode QR disebut “quishing”, yaitu gabungan antara kode QR dan phishing, di mana pelaku “memikat” calon korban untuk mendapatkan informasi pribadi. Cara kerjanya, ketika korban memindai kode QR, akan muncul pesan teks sederhana, daftar aplikasi, bahkan alamat peta. Dengan kemampuan tersebut, calon korban akan diarahkan oleh pelaku ke website palsu yang sulit dideteksi. Pelaku kemudian mengelabui calon korban agar mengunduh sesuatu ke dalam perangkat yang justru merugikan perangkat calon korban. Selanjutnya, penyerang meminta calon korban untuk memasukkan beberapa detail login, yang kemudian diperoleh penyerang. Jenis kejahatan “quishing” ini semakin meningkat karena siapa pun yang tidak memiliki keahlian khusus dapat dengan mudah membuat kode QR (Nano, 2024).

Contoh kasus nyata adalah yang terjadi pada seorang ibu bernama Rani, seorang penjual tortilla pinggir jalan di wilayah Bekasi. Rani baru-baru ini menyadari bahwa pendapatan yang ia peroleh dari penjualannya sebenarnya terbatas, yang baru diketahui setahun kemudian. Dari hasil penelusuran, diketahui ada yang menempelkan QRIS palsu di keranjang belanjaannya. Akibat kejadian tersebut, masih belum jelas siapa pelaku pemasangan QRIS palsu tersebut. Kejadian ini dilaporkan ke polisi setempat oleh korban namun tidak dapat ditangani karena kesulitan dalam memberikan bukti. Korban kemudian bertanya kepada bank tempat dia menyimpan uang tersebut untuk membantu mengetahui identitas penerima uang dari salinan rekening korannya namun tidak berhasil. Sebab bank tidak bisa memberikan informasi rahasia perbankan kepada siapapun.

Berdasarkan permasalahan yang timbul dalam penggunaan QRIS sebagai sistem transaksi pembayaran digital di atas, setidaknya dapat diidentifikasi 2 (dua) Perma Alahan dari segi hukum. Pertama, konsumen yang menjadi korban penipuan QRIS berada pada posisi yang lemah sehingga pemerintah mempunyai kewajiban untuk memberikan perlindungan hukum kepada pengguna QRIS sebagai konsumen. Kedua, sistem QRIS sebagai alat transaksi pembayaran digital menimbulkan kejahatan digital dengan memanfaatkan kelemahan yang ada berupa QRIS palsu dan memusnahkannya sehingga dapat menimbulkan akibat hukum.

Metode Penelitian

Artikel penelitian ini berkonsultasi dengan Mamahit & Urumsah (2018) menggunakan metode kualitatif dengan pendekatan penelitian sastra, meliputi observasi dan telaah informasi terkait topik penelitian. Penulis kemudian menggabungkan metode tersebut dengan penelitian sebelumnya yang berkaitan dengan penelitian ini untuk menjelaskan suatu peristiwa yang akan datang (Arianto, 2021).

Makalah hukum primer dan sekunder berfungsi sebagai sumber data sekunder untuk pengumpulan data. Dokumen hukum utama yang dimaksud adalah: Peraturan Bank Indonesia Nomor 18/40/PBI/2016 tentang Pembayaran untuk Pemrosesan Transaksi; Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Peraturan Perbankan Indonesia No. 20/6/Pbi/2018 tentang Mata Uang Kripto; Peraturan Dewan Gubernur Nomor 21/18/Padg/2019 tentang Penerapan Kode Respon Cepat Standar Pembayaran Nasional; dan peraturan terkait lainnya yang berkaitan dengan hal ini. Meneliti. Penelitian dokumen digunakan untuk mengembangkan dokumen hukum sekunder. Mempelajari buku, makalah, jurnal penelitian, jurnal online, dan sumber literatur lain yang berkaitan dengan topik merupakan cara penelitian sastra dilakukan (Rinjani, 2022).

Hasil dan Pembahasan

Perlindungan Hukum Bagi Pengguna QRIS

QRIS adalah format kode QR yang diciptakan untuk mempermudah transaksi pembayaran digital menggunakan aplikasi cryptocurrency, dompet digital, dan layanan mobile banking di Indonesia. Peraturan Anggota Dewan Gubernur Nomor 21/18/PADG/2019 tentang Penyelenggaraan Respon Cepat Nasional saat ini merupakan dasar hukum yang ditetapkan oleh Bank Indonesia untuk penggunaan QRIS sebagai sistem pembayaran digital di Indonesia. Kode standar adalah aturan yang harus diikuti dalam menulis kode. dalam hal pembayaran (PADG

nomor 21/18/2019). Penggunaan QRIS sebagai metode pembayaran digital melibatkan berbagai pihak, seperti Penyedia Jasa Sistem Pembayaran (PJSP), lembaga switching, pengumpul merchant, Arsip Perdagangan Nasional (NMR), penerbit, konsumen, penjual, dan pengguna QRIS.

QRIS, sebagai implementasi teknologi keuangan di Indonesia, memiliki hubungan erat dengan PBI Nomor 19/12/2017 yang mengatur pelaksanaan teknologi keuangan. PBI tersebut menjelaskan tujuan yang ingin dicapai. Pada awalnya, guna memperoleh kebutuhan yang bervariasi dari masyarakat termasuk membuka peluang akses terhadap layanan finansial dan proses transaksi. Selanjutnya, mengurangi kemungkinan terjadinya risiko terhadap sistem keuangan melalui langkah-langkah pengendalian. Ketiga, mendukung perkembangan yang berkelanjutan dan penggabungan ekonomi nasional dengan menciptakan stabilitas dalam mata uang, stabilitas dalam sistem keuangan, serta membangun kepercayaan pada sistem pembayaran yang efisien, tanpa hambatan, aman, dan terpercaya. Poin berikutnya adalah memastikan perlindungan konsumen saat menggunakan teknologi keuangan.

Pada saat mengadopsi QRIS sebagai metode pembayaran, konsumen yang menggunakan layanan ini perlu mendapatkan perlindungan hukum yang khusus. Peraturan Bank Indonesia tanggal 19 Desember 2017 menyatakan bahwa penyelenggara teknologi keuangan yang menggunakan QRIS harus mengimplementasikan prinsip-prinsip perlindungan konsumen dalam penggunaan QRIS. Prinsip-prinsip perlindungan konsumen dalam sektor jasa keuangan telah dijelaskan dalam Pasal 2 Peraturan Otoritas Jasa Keuangan Nomor: 1/POJK.07/2013 (POJK No. n Pada tanggal 1 Juli 2013, tiga prinsip utama telah diberlakukan, yaitu keterbukaan, penanganan yang adil, dan kepercayaan. Dalam rangka menjaga kerahasiaan dan keamanan data dan informasi konsumen, serta menangani keluhan dan memecahkan masalah konsumen dengan cara yang mudah, cepat, dan efektif. Dilihat dari contoh situasi penipuan yang disajikan pada awal tulisan, dapat dilihat dengan jelas bahwa perlunya perlindungan hukum bagi pengguna QRIS terkait dengan keamanan data dan informasi konsumen serta penanganan pengaduan dalam kasus keuangan yang merugikan konsumen. Jumlah uang yang diperoleh dari tindakan pemalsuan melalui QRIS, sebuah bentuk kejahatan digital, didapatkan.

Aspek keamanan penggunaan QRIS untuk transaksi digital harus dipenuhi oleh operator QRIS sebagai prasyarat utama bagi pengguna QRIS dari sisi keamanan. Bank Indonesia bertanggung jawab untuk memenuhi persyaratan yang telah ditetapkan dalam Peraturan Bank Indonesia No.18/40. Paragraf ini berbicara tentang Peraturan Bank Indonesia (PBI) tahun 2016 mengenai pelaksanaan pemrosesan transaksi pembayaran, yang ditunjukkan sebagai PBI Nomor. Untuk memastikan keamanan transaksi yang dilakukan melalui QRIS, terutama dalam

hal perlindungan data pribadi pengguna QRIS yang dikelola oleh PJSP, langkah-langkah penting perlu diambil. Sertifikat PBI 18/40/2016 mencatat bahwa PJSP memiliki tanggung jawab untuk menjaga keamanan informasi penggunaan QRIS. Di samping itu, partisipasi PJSP dalam menyediakan dan mengatur fasilitas pembayaran melalui QRIS telah diatur oleh Bank Indonesia dengan tujuan menciptakan sistem pembayaran yang aman dan teratur, sesuai dengan semua aturan hukum yang berlaku di Indonesia serta memperoleh izin hukum. Pembenaran terhadap segala bentuk kecerobohan dan perilaku melanggar aturan. Sementara itu, posisi pelanggan dalam transaksi menggunakan QRIS sesuai dengan tanggung jawab dan peran PJSP. Pasal 4 Angka 1 dari Peraturan Undang-Undang Nomor 8 Tahun 1999 mengatur bahwa konsumen memiliki hak untuk memperoleh informasi yang benar dan memastikan keamanan mereka.

Dalam upaya untuk memperkuat kepercayaan masyarakat dan meningkatkan performa QRIS dalam sistem pembayaran digital, Otoritas Jasa Keuangan (OJK) menetapkan undang-undang yang mengatur keamanan penggunaan QRIS, selain tindakan yang telah dilakukan oleh Bank Indonesia. Dalam Pasal 37(1) Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor ..., dijelaskan bahwa... Sesuai dengan Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.02/2018 mengenai Inovasi Keuangan Digital di Sektor Jasa Keuangan, lembaga penyedia jasa pembayaran (PJSP) diharuskan bekerja sama untuk menyusun struktur kerja sama yang memungkinkan pengembangan ekosistem inovasi keuangan digital untuk diterapkan dalam sistem pembayaran yang digunakan oleh lembaga keuangan. Untuk melakukan fungsi dukungan keuangan digitalnya, PJSP harus melalui proses pendaftaran di OJK terlebih dahulu.

Kepentingan menjaga keamanan data pengguna QRIS sangat besar, oleh karena itu, pemerintah perlu melindungi data tersebut dengan mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pengamanan Data Pribadi yang di dalam Pasal 54 ayat (2) menguraikan tentang adanya pejabat dan agen yang bertujuan untuk memastikan keamanan data tersebut. Pertanyaan tentang transaksi QRIS yang diadakan oleh PSJP. Sesuai dengan aturan tersebut, PJSP harus menjaga keamanan informasi pelanggan terkait dengan penggunaan QRIS dalam proses pengolahan data pribadi. PJSP perlu menyadari adanya potensi risiko terhadap informasi pelanggan yang terkait dengan pengolahan transaksi menggunakan QRIS. PJSP juga melakukan pemeriksaan terhadap transaksi, termasuk apa yang terlibat dalam transaksi, data yang digunakan, konteks transaksi oleh pengguna QRIS, serta tujuan dari pemrosesan transaksi.

Terkait dengan penanganan pengaduan pengguna QRIS yang mengalami kerugian akibat pelanggaran QRIS, PJSP wajib memberikan pembinaan melalui sarana informasi yang tersedia mengenai pengaduan atau tata cara pengaduan yang dapat digunakan konsumen untuk menggunakan haknya yang dilindungi undang-undang. Upaya tersebut merujuk pada proses sosialisasi kembali proses penyelesaian permasalahan yang muncul pada sistem pembayaran menggunakan QRIS. Hal ini terkait dengan kasus yang terjadi di lokasi kejadian, dimana masih banyak masyarakat yang belum mengetahui cara menggunakan QRIS yang benar dan bingung apakah mereka tertipu oleh QRIS palsu atau tidak. Oleh karena itu, pengaduan mengenai permasalahan tersebut dapat disampaikan kepada PJSP sebagai penyedia layanan pembayaran menggunakan QRIS (Telkom, 2022).

Dari penjelasan sebelumnya dapat disimpulkan bahwa PBI No.18/40/2016 mengatur tentang persyaratan keamanan transaksi QRIS. Pengguna QRIS yang juga pelanggan layanan transaksi digital akan memiliki kepastian hukum selama memanfaatkan QRIS untuk membayar merchant berkat ketentuan hukum tersebut. Selain diatur dalam PBI Nomor 18/40/2016, persyaratan keamanan penggunaan QRIS sebagai sistem pembayaran juga sesuai dengan UUPK Nomor 8 Tahun 1999 yang mengatur tentang hak-hak konsumen, salah satunya adalah hak atas jaminan. —saat mengonsumsi produk atau layanan. Laporan audit sistem informasi dari auditor independen dengan menggunakan prosedur pengendalian keamanan menjadi bukti kesiapan PJSP dalam melakukan proses transaksi yang aman.

Sebagai pengatur sistem pembayaran, Bank Indonesia bertanggung jawab mengawasi implementasi layanan sistem pembayaran dan perubahan dalam fungsi organisasi untuk melindungi nasabah QRIS secara hukum. Dalam rangka mendorong pertumbuhan ekonomi dan memastikan kebijakan yang terstruktur, Bank Indonesia sedang melakukan pengawasan terhadap transaksi digital melalui QRIS dengan menyediakan sistem pembayaran yang terintegrasi dan kerangka kebijakan untuk mengatur penggunaan uang rupiah. Untuk memastikan ketahanan serta memberikan perlindungan hukum terhadap pengguna QRIS, terdapat dua jenis pengawasan yang diterapkan, yaitu pengawasan secara langsung dan pengawasan tidak langsung. Inspeksi rutin (pengamatan di lapangan) yang dilakukan oleh Bank Indonesia adalah salah satu elemen pengawasan langsung. Contoh pemantauan tidak langsung adalah ketika kita meminta data, laporan, dokumentasi, dan informasi penjelasan tentang proses transaksi QRIS. Monitoring merupakan indikator utama untuk menentukan kesuksesan operasional perusahaan. Di samping itu, pemanfaatan QRIS Bank Indonesia juga memberikan manfaat dalam hal pengawasan terhadap perlindungan konsumen serta kejelasan dalam hal hukum.

Penyalahgunaan Data Konsumen dalam Bertransaksi Menggunakan QRIS

Perkembangan teknologi informasi dalam kehidupan saat ini tidak dapat dielakkan, karena perkembangan teknologi informasi akan mengikuti kemajuan ilmu pengetahuan. Setiap perkembangan baru yang dimunculkan bertujuan untuk memberikan dampak positif kepada kehidupan manusia. Tidak selamanya perkembangan teknologi informasi memberikan dampak positif kepada masyarakat, terutama bagi entitas ekonomi yang menggunakan sistem digital dalam melakukan transaksi keuangan. Sebagai respons, penjahat digital berusaha beradaptasi dengan evolusi teknologi ini untuk menemukan celah dalam sistem pembayaran digital. Quishing adalah salah satu bentuk kejahatan digital yang semakin marak dalam beberapa waktu terakhir. Kejahatan ini dilakukan melalui Quick Response Codes (QR Codes) dengan tujuan untuk merampas data pribadi para pengguna QRIS. Penting untuk menjaga kerahasiaan data pribadi serta keamanan dana agar terhindar dari ancaman ini. Teks ini merujuk pada penyimpanan data di Bank pengguna QRIS.

Penyalahgunaan data pribadi dapat dilakukan oleh perorangan maupun oleh PJSP sendiri karena terkait dengan data pribadi konsumen yang dikelolanya. Oleh karena itu, berdasarkan Pasal 40 ayat (2) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), PJSP wajib menciptakan kondisi yang menguntungkan bagi transaksi keuangan melalui QRIS untuk melindungi pengguna QRIS. Data adalah konsumen yang menggunakan QRIS sesuai dengan hukum.

Munculnya kasus kejahatan digital dengan istilah "quishing" yang disebutkan di pendahuluan terjadi karena adanya penyalahgunaan data pribadi pengguna QRIS. Hal ini secara tegas dilarang oleh undang-undang ITE yang melarang akses ilegal terhadap data orang lain melalui sistem elektronik untuk mendapatkan informasi secara melanggar. Untuk mengungkapkan kembali isi teks ini, kita dapat menyampaikannya dengan cara berikut: Satu-satunya teks di sini adalah "n". sistem keamanan yang dimaksud dalam Pasal 46 ayat (2) UU ITE. Di samping itu, terdapat ketentuan yang jelas dalam UU ITE yang menyatakan bahwa mencuri data pengguna QRIS dilarang, kecuali jika dilakukan oleh pihak yang berwenang melalui proses hukum yang sah. Individu yang mengalami kerugian akibat melanggar hukum, berhak untuk mengajukan tuntutan ganti rugi, sementara pelaku pelanggaran harus bertanggung jawab atas tindakannya. Setiap tindakan melanggar privasi data Pengguna QRIS dapat dianggap sebagai tindakan mencuri identitas. Pencurian identitas merujuk pada tindakan

yang melibatkan pengambilan data pribadi seseorang secara ilegal dan menggunakan informasi tersebut untuk keuntungan pribadi atau kepentingan orang lain. Pentingnya keamanan data pribadi semakin dipertanyakan karena hampir semua informasi pengguna QRIS tersimpan secara daring, yang membuat pencurian data menjadi lebih mudah dilakukan. Pencurian informasi pribadi individu adalah salah satu bentuk tindakan ilegal (Hartadi, 2020).

Selain kasus kejahatan digital, contoh dalam kasus ini adalah model "quishing", yaitu pemalsuan QRIS yang dilakukan seseorang dengan tujuan mengalihkan transfer dana yang diterima ke rekening pelaku. Dengan memalsukan QRIS, penulis telah melanggar ketentuan Pasal 31 UU ITE yang mengatur tentang pemalsuan informasi elektronik dan/atau dokumen elektronik dengan risiko sanksi pidana berdasarkan UU ITE, apabila terbukti membuktikan bahwa penulis melakukan pemalsuan penggunaannya. . oleh QRIS. QRIS. Selain itu, pemalsuan QRIS dikenakan sanksi pidana karena melanggar Pasal 49 Undang-Undang Nomor 10 Tahun 1998 tentang Industri Perbankan terkait dengan tindak pidana di bidang sistem pembayaran.

Kejadian penyalahgunaan data pribadi konsumen saat bertransaksi digital melalui QRIS dan tindakan pemalsuan QRIS menghasilkan dampak hukum sebagai tanggapan terhadap praktek tersebut. Konsekuensi hukum yang timbul adalah tugas hukum yang harus ditanggung oleh mereka yang melakukan penyalahgunaan data. Tanggung jawab yang diterapkan merupakan konsekuensi dari kesalahan yang dilakukan atau sebagai respons terhadap prinsip-prinsip yang telah ditetapkan, terutama berdasarkan unsur kesalahan. Menurut prinsip ini, ada kebutuhan untuk memberi pertanggungjawaban kepada individu atau kelompok yang berada di bawah pengawasan hanya jika terdapat bukti kesalahan yang dilakukan oleh mereka (Umboh, 2018). Dalam tindakan memikul tanggung jawab ini, pengguna data wajib menanggung kerugian yang disebabkan oleh kelalaian mereka. Bukti bahwa pihak yang menggunakan data tersebut secara tidak benar harus dikemukakan oleh korban yang merugi. Tugas ini secara khusus berfokus pada pihak yang melakukan kesalahan dengan melanggar data konsumen dalam transaksi QRIS. Menurut Shidarta (2000), prinsip ini mengemukakan bahwa seseorang hanya dapat dipertanggungjawabkan jika ada bukti kesalahannya.

Konsekuensi legal bagi orang perorangan atau bisnis kecil yang mengambil keuntungan dari informasi konsumen dalam QRIS meliputi pembayaran kompensasi dan proses hukum sesuai dengan Pasal 12 ayat (1) dari Undang-Undang Nomor 1 Tahun 27 Januari 2017 tentang Perlindungan Hak Data Pribadi. Pengajuan gugatan yang dilakukan oleh seseorang yang merasa mengalami kerugian tidak dapat dinyatakan sah. Ayat pertama dan ayat ketiga dari Pasal 67 Undang-Undang Perlindungan Data Pribadi (PDP) mengatur adanya konsekuensi

hukum tambahan selain proses pengadilan dan kompensasi finansial. Tindak pidana tambahan adalah istilah yang digunakan untuk menggambarkan pengambilan uang atau harta benda yang diperoleh melalui kegiatan kriminal dan pembayaran kompensasi (Oktavira, 2022).

Faktanya, siapapun yang merasa dirugikan akibat penyalahgunaan data akan terkena dampak hukum tersebut. Sebagai pelanggan QRIS, setiap orang berhak menjamin keamanan hukum posisinya dan menjaga datanya. Pengajuan gugatan terhadap suatu perbuatan melawan hukum dilakukan melalui Pengadilan Negeri, dan pihak yang merasa dirugikan dapat mengajukan pengaduan untuk mendapatkan ganti rugi. Sebelum menyampaikan laporan pengaduan ke Bank Indonesia, nasabah terlebih dahulu menyampaikan ke PJSP.

Kesimpulan

1. Perlindungan hukum yang diberikan negara kepada pengguna QRIS berdasarkan peraturan yang berlaku, antara lain PJSP mempunyai status hukum yang sah, PJSP wajib menciptakan ekosistem inovasi keuangan digital baik di sektor jasa keuangan dan terdaftar di OJK, pengguna QRIS . (konsumen) berhak menikmati haknya berdasarkan ketentuan UU Perlindungan Konsumen dan UU ITE

2. Pelaku malapraktik menghadapi dampak hukum jika data konsumennya disalahgunakan dalam transaksi digital melalui QRIS. Pengguna QRIS dapat menuntut ganti rugi melalui PJSP atau mengajukan gugatan perdata atas kerugian yang diderita, sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya Pasal 12 ayat 1.

Referensi

BPHN. (2022). Laporan Akhir Analisis Dan Evaluasi Hukum Keuangan Digital. Jakarta: Kementerian Hukum dan HAM RI.

Fizriyani, W. (2023). Retrieved Januari 10, 2024, from https://ekonomi.republika.co.id/berita/rykauh502/83-persen-transaksi-qris-didominasi-pelaku-umkm.

Gufran, dkk., M. (2023). Determinan Tingkat Penggunaan Quick Response Indonesian Standard Di Kota Kendari, Value Added. Majalah Ekonomi Dan Bisnis, Volume 19, Nomor 2, 91.

Hartadi, R. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik, 285-299, hlm. 293. Jurnal HAM, Volume 11 Nomor 2.

Kerja, K. (2022). Laporan Akhir Analisis Dan Evaluasi Hukum Keuangan Digital. Jakarta: Pusat Analisis Dan Evaluasi Hukum Nasional Badan Pembinaan Hukum Nasional Kementerian Hukum dan HAM RI.

Nano , V. (2024). Modus Penipuan Pakai Kode QR di HP, Rekening Auto Ludes. Retrieved Januari 16, 2024, from https://www.cnbcindonesia.com/tech/20240203192826-37-511477/modus-penipuan-pakai-kode-qr-di-hp-rekening-auto-ludes

Nurohman, dkk., Y. (2022). Pembayaran Digital Sebagai Solusi Transaksi Di Masa Pandemi Covid 19: Studi Masyrakat Muslim Solo Raya). Among Makarti, Vol. 15 No. 2 (Edisi Khusus Dies Natalis ke-38) .

Oktavira, B. (2022). Terjadi Pencurian Data Pribadi (Identity Theft)?Tempuh langkah ini. Retrieved Februari 6, 2024, from https://www.hukumonline.com/klinik/a/terjadi-pencurian-data-pribadi-tempuh-langkah-inilt5d904597bfa6e/

Putra, I. P. (2022). Kertha Wicaksana: Sarana Komunikasi Dosen dan Mahasiswa Volume 16, Nomor 2., 99.

Ramli, T. (2020). Aspek Hukum Platform E-Commerce Dalam Era Transformasi Digital. Jurnal Studi Komunikasi dan Media.

Rinjani. (2022). Peran Auditor Internal Dan Auditor Eksternal Dalam Upaya Pemberantasan Korupsi Di Indonesia. E-Jurnal Akuntansi TSM, Vol. 2, No. 2, 1083-1098.

Saraswati, A. (2023, Februari 2). Peta Persaingan Bank Menuju Digital. Retrieved Januari 15, 2023, from https://infobanknews.com/peta-persaingan-bank-menuju-digital/.

Setiawan, H. (2022). Masa Depan Uang Digital di Indonesia Pasca KTT G.20. Pekalongan: Nasya Expanding Management.

Sinaga, d. I. (2023). Analisis Manajemen Resiko Penggunaan Digital Payment: (Studi Kasus Pada PT. Bank Syariah Indonesia, Tbk KC Medan S. Parman). Jurnal Ilmu Komputer, Ekonomi dan Manajemen, Volume 3 Nomor 1, 647-685.