Prevenção de Fraudes e Golpes Digitais em Meios de Pagamento Eletrônicos: mecanismos jurídico-regulatórios e proteção ao consumidor no Sistema Financeiro Nacional

DOI: https://doi.org/10.58766/rpgbcb.v20.1.1263

Danniel Pedro Lima de Araújo da Conceição*

Recebido/Received: 19/2/2026
Aprovado/Approved: 7/8/2026

Introdução. 1 A evolução do arcabouço regulatório de prevenção a fraudes. 1.1 O compartilhamento de dados e a Resolução Conjunta 6/2023. 1.2 Governança e cibersegurança (Resolução CMN 4.893/2021). 1.3 Novos paradigmas: criptoativos e Pix Automático. 2 O Pix e a resposta operacional: MED. 2.1 O funcionamento e os limites do MED. 2.2 Responsabilidade das instituições na detecção. 3 A responsabilidade civil e a proteção do consumidor na jurisprudência. 3.1 A Súmula 479 do STJ e a desconstrução da culpa do consumidor. 3.2 O "golpe da falsa central", a tecnologia de spoofing *e o* distinguishing *no STJ. 3.3 A atuação do TCU e a tutela coletiva dos hipervulneráveis. 4 A nova fronteira tecnológica e o* enforcement *estatal: Open Finance, inteligência artificial e o regime sancionador. 4.1 A integração do Open Finance na modelagem de risco (Resolução BCB 506/2025). 4.2 Inteligência artificial e auditoria algorítmica (Instrução Normativa BCB 587/2025). 4.3 O regime sancionador e a efetividade da norma (Resolução BCB 507/2025). Conclusão.*

Resumo

Este artigo analisa o marco jurídico-regulatório para prevenção de fraudes e golpes digitais no Sistema Financeiro Nacional (SFN), com ênfase em meios de pagamento eletrônicos, especialmente o Pix. O objetivo é avaliar a eficácia dos mecanismos de governança e segurança cibernética do Banco Central do Brasil (BC) e do Conselho Monetário Nacional (CMN) na proteção do consumidor financeiro. A metodologia adota a análise normativa de resoluções recentes, como a Resolução Conjunta 6/2023 e as atualizações do Regulamento do Pix referentes ao Mecanismo Especial de Devolução (MED), aliada à jurisprudência do Superior Tribunal de Justiça (STJ) e aos acórdãos do Tribunal de Contas da União (TCU). Os resultados revelam uma evolução regulatória focada no compartilhamento obrigatório de dados sobre fraudes e na responsabilidade objetiva dos prestadores de serviço por falhas de segurança ou engenharia social. Conclui-se pela necessidade de reforçar o monitoramento em tempo real e as tecnologias de detecção, transferindo o risco da fraude do consumidor vulnerável para as instituições, em consonância com a Lei 15.252, de 4 de novembro de 2025, e os princípios da cidadania financeira.

Palavras-chave: fraudes digitais; Pix; proteção do consumidor; governança bancária; cidadania financeira.

* Procurador Federal da Advocacia-Geral da União (AGU), atuando como Procurador-Chefe da Universidade Federal de Catalão/GO. Especialista em Direitos Humanos e Gestão Estratégica da Segurança Pública. https://orcid.org/0009-0002-8593-359X

Prevention of Digital Fraud and Scams in Electronic Payment Methods: legal-regulatory mechanisms and consumer protection in the National Financial System

Abstract

This article analyzes the legal-regulatory framework for the prevention of digital fraud and scams within the National Financial System (SFN), with emphasis on electronic payment methods, notably Pix. The objective is to evaluate the effectiveness of governance and cybersecurity mechanisms established by the Banco Central do Brasil (BCB) *and the National Monetary Council (CMN) regarding financial consumer protection. The methodology adopts a normative analysis of recent resolutions, such as Joint Resolution No. 6/2023 and updates to the Pix Regulation concerning the Special Return Mechanism (MED), combined with the jurisprudence of the Superior Court of Justice (STJ) and rulings of the Federal Court of Accounts (TCU). The results reveal a regulatory evolution based on the mandatory sharing of fraud data and the strict liability of service providers for security failures or social engineering. It is concluded that there is a need to reinforce real-time monitoring and detection technologies, shifting the fraud risk from the vulnerable consumer to the institutions, in line with Law No. 15.252/2025 and financial citizenship principles.*

Keywords: *digital fraud; Pix; consumer protection; banking governance; financial citizenship.*

Introdução

A transformação digital do SFN alterou a dinâmica das relações de consumo bancário. Se, por um lado, a massificação dos meios de pagamento eletrônicos – notadamente o Pix – democratizou o acesso e conferiu celeridade às transações, por outro, ampliou a superfície de riscos de segurança. A digitalização, essencial para o exercício da cidadania, expôs o consumidor a vetores de ataque sofisticados, nos quais a tecnologia é instrumentalizada para a prática de engenharia social e ilícitos patrimoniais.

O aumento exponencial de fraudes e golpes digitais não é apenas uma estatística operacional, mas um problema estrutural de segurança pública. Relatórios setoriais apontam que as instituições financeiras investiram cerca de R$2,12 bilhões em 2023. Contudo, a astúcia dos fraudadores evolui em ritmo acelerado, demonstrando que a barreira tecnológica, por si só, é insuficiente se não estiver alicerçada em mecanismos robustos de governança e detecção comportamental (Brasil, 2023c).

Essa assimetria de forças coloca em xeque a relação entre o consumidor – muitas vezes hipossuficiente técnica e informacionalmente – e o dever de segurança das instituições. O STJ enfrentou essa tensão no Recurso Especial 2.222.059, consolidando o entendimento de que a falha na identificação de transações atípicas caracteriza defeito na prestação do serviço. A Corte firmou a responsabilidade objetiva das instituições, inclusive em casos de engenharia social, afastando a tese de culpa exclusiva da vítima quando o sistema bancário falha em seu dever de vigilância.

Na mesma linha de proteção, o TCU, por meio do Acórdão 2.875/2025, alertou para a hipervulnerabilidade de grupos específicos, como os idosos. A Corte de Contas determinou ações integradas entre órgãos de controle e o BC para mitigar os riscos decorrentes da exclusão digital e da sofisticação dos ardis criminosos.

O objetivo deste artigo, portanto, é analisar a eficácia do arcabouço jurídico-regulatório contemporâneo voltado à prevenção de fraudes, com ênfase na transição de um modelo reativo para uma governança preventiva e colaborativa. Serão examinados os impactos da Resolução Conjunta 6/2023, que instituiu o compartilhamento obrigatório de dados sobre fraudes (Brasil, 2023a), e as recentes alterações no Regulamento do Pix, como a Resolução BCB 501/2025, que impõe o bloqueio cautelar e a rejeição de transações para contas suspeitas (Brasil, 2025c).

A segurança cibernética, nessa perspectiva, transcende a categoria de requisito técnico operacional para se constituir em condição indispensável para a confiança no sistema financeiro e na própria cidadania. A confiança no sistema de pagamentos depende da capacidade regulatória e institucional de transferir o risco da tecnologia para quem a explora economicamente, garantindo que a inovação não signifique a precarização da proteção patrimonial do consumidor.

Nesse contexto, a análise aqui proposta dialoga diretamente com os avanços trazidos pela Lei 15.252/2025 (Brasil, 2025g). Examina-se como esse novo marco legal, ao lado das resoluções do BC e da jurisprudência do STJ, reconfigura o dever de monitoramento em tempo real, transformando a prevenção a fraudes de uma medida operacional em uma garantia legal de cidadania financeira, conforme preconizado pelo regulador.

1 A evolução do arcabouço regulatório de prevenção a fraudes

A estabilidade e a higidez do SFN dependem, contemporaneamente, da capacidade estatal e privada de mitigar riscos cibernéticos. O paradigma regulatório brasileiro, historicamente focado na solidez patrimonial das instituições, expandiu-se forçosamente para abarcar a segurança da informação e a prevenção a fraudes como pilares de sustentação da própria atividade bancária. Não se trata mais apenas de proteger o ativo da instituição, mas de salvaguardar a integridade do patrimônio do consumidor e a confiança pública no sistema de pagamentos.

A regulação infralegal, capitaneada pelo CMN e pelo BC, evoluiu de diretrizes principiológicas para imposições técnicas cogentes. Observa-se uma transição do modelo de "segurança de perímetro" (focado na proteção individual de cada banco) para um modelo de "inteligência colaborativa", em que a troca de informações e a governança robusta de dados tornam-se compulsórias.

1.1 O compartilhamento de dados e a Resolução Conjunta 6/2023

A assimetria informacional sempre constituiu a principal vantagem tática das organizações criminosas. A fragmentação dos dados permitia que fraudadores migrassem de uma instituição para outra, perpetuando a prática ilícita sem que o novo prestador tivesse ciência do histórico de risco.

Para sanar essa lacuna, a Resolução Conjunta 6, de 23 de maio de 2023, impôs a obrigatoriedade de compartilhamento de dados e informações sobre indícios de fraudes (Brasil, 2023a). Conforme a exposição de motivos do regulador, a medida visa aprimorar a visibilidade sistêmica dos riscos, exigindo a implementação de sistemas eletrônicos interoperáveis para registro e consulta de ocorrências, harmonizando o dever de segurança com o sigilo bancário ao legitimar o tratamento de dados para a proteção do crédito e a prevenção a ilícitos (Brasil, 2023b).

CC BY NC SA

O normativo exige a implementação de sistemas eletrônicos interoperáveis que permitam o registro e a consulta de dados sobre tentativas ou ocorrências de fraudes, identificando não apenas a descrição do *modus operandi*, mas também os dados das contas destinatárias e de seus titulares (Brasil, 2023a; Finsiders Brasil, 2023). Essa medida visa desarticular o uso de "contas-laranjas", essenciais para a pulverização do produto do crime, permitindo que as instituições bloqueiem preventivamente a abertura de contas ou transações para indivíduos já sinalizados no sistema compartilhado.

Juridicamente, a norma harmoniza o dever de segurança com o sigilo bancário e a Lei Geral de Proteção de Dados (LGPD), ao exigir o consentimento prévio do cliente em cláusula contratual de destaque, legitimando o tratamento de dados para fins de prevenção à fraude, conforme o legítimo interesse e a proteção do crédito.

1.2 Governança e cibersegurança (Resolução CMN 4.893/2021)

A segurança cibernética deixou de ser uma questão de suporte tecnológico para se tornar uma obrigação de governança corporativa. A Resolução CMN 4.893, de 26 de fevereiro de 2021, alterada recentemente pela Resolução CMN 5.274, de 18 de dezembro de 2025, consolidou a exigência de uma política de segurança cibernética robusta, que deve contemplar, no mínimo, procedimentos de autenticação, criptografia, prevenção de intrusão e rastreabilidade (Brasil, 2025f).

A regulação impõe que tais controles não sejam meras opções gerenciais, mas requisitos mandatórios para o funcionamento da instituição. Destaca-se a obrigatoriedade de realização de testes de intrusão com periodicidade mínima anual e a vedação expressa de que empresas prestadoras de serviços a terceiros tenham acesso às chaves privadas associadas a certificados digitais utilizados pela instituição.

Tais medidas, introduzidas na regulação de cibersegurança, visam reforçar a blindagem do núcleo crítico do sistema bancário e garantir a integridade fim a fim das transações (Brasil, 2025c).

1.3 Novos paradigmas: criptoativos e Pix Automático

A inovação financeira traz consigo a necessidade de atualização constante do perímetro regulatório. A Lei 14.478, de 21 de dezembro de 2022, conhecida como o Marco Legal dos Criptoativos, inseriu as prestadoras de serviços de ativos virtuais no rol de instituições supervisionadas, sujeitando-as às normas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (Brasil, 2022). A lei criminalizou a fraude com a utilização de ativos virtuais (art. 171-A do Código Penal), reconhecendo a necessidade de tutela penal específica para um mercado que, pela sua natureza descentralizada e transnacional, atrai vetores de risco para a poupança popular.

Simultaneamente, a evolução do Pix para modelos de recorrência, como o Pix Automático, exigiu reforço das camadas de segurança. A Resolução BCB 402, de 22 de julho de 2024, estabeleceu regras rígidas para essa modalidade, impondo limites de valor e, principalmente, mecanismos de monitoramento sobre os usuários recebedores (Brasil, 2024). A norma determina que as instituições devem possuir ferramentas para identificar e agir contra recebedores que enviem instruções de pagamento indevidas ou ofertas excessivas, mitigando o risco de golpes em massa que exploram a automatização dos débitos (Brasil, 2024).

2 O Pix e a resposta operacional: MED

A arquitetura do arranjo de pagamentos instantâneos brasileiro (Pix) foi concebida sob o primado da eficiência e da velocidade. Contudo, a celeridade que beneficia a economia também instrumentaliza a expropriação patrimonial em casos de fraudes e engenharia social. Nesse cenário, o MED atua não apenas como uma ferramenta operacional, mas como a principal resposta regulatória para a recomposição do patrimônio do consumidor lesado, operacionalizando a responsabilidade civil das instituições no ambiente digital.

2.1 O funcionamento e os limites do MED

Instituído para conferir maior segurança jurídica às transações, o MED constitui um conjunto de regras e procedimentos operacionais que obriga as instituições participantes a efetivarem a devolução de valores em hipóteses estritas: fundada suspeita de fraude, golpes de engenharia social ou falha operacional nos sistemas das instituições (Infomoney, 2023). O mecanismo, contudo, não se aplica a desacordos comerciais ou erros de digitação do próprio usuário, situações que demandam resolução pela via judicial ou composição amigável (Infomoney, 2023).

O procedimento padrão impõe que, ao receber a notificação de infração, que deve ser aberta em até 80 dias da transação, a instituição detentora da conta recebedora proceda ao bloqueio cautelar dos recursos. Caso a fraude seja confirmada após análise (com prazo de até sete dias), a devolução deve ocorrer em até 96 horas (Infomoney, 2023).

Entretanto, a eficácia do MED enfrentou, em seus primeiros anos, um obstáculo estrutural: a pulverização rápida dos ativos. Estatísticas indicam que, em 2022, apenas 6% do montante total de R$3,1 bilhões em solicitações via MED foi efetivamente devolvido às vítimas (Infomoney, 2023). A baixa efetividade é agravada pelo fato de que, mesmo quando aceitas, dois terços das devoluções ocorrem de forma apenas parcial, devido ao rápido esvaziamento das contas pelos fraudadores, o que impôs a necessidade de atualizações regulatórias para permitir o bloqueio de recursos em camadas subsequentes de triangulação financeira.

Para mitigar essa limitação, o BC promoveu atualizações regulatórias robustas, vigentes a partir de 2026, que transformam a lógica do MED. A nova sistemática permite o rastreamento do caminho do dinheiro (*follow the money*), autorizando o bloqueio de recursos não apenas na primeira conta recebedora, mas em camadas subsequentes de triangulação financeira (Brasil, 2025a). Essa alteração normativa visa desarticular a lógica das "contas-laranjas", permitindo que o sistema alcance o ativo ilícito mesmo após sucessivas transferências, ampliando a probabilidade de ressarcimento integral ao consumidor (Brasil, 2025a).

2.2 Responsabilidade das instituições na detecção

A evolução normativa recente deslocou o eixo da responsabilidade bancária da simples reação para a prevenção compulsória. Não basta mais acolher a notificação de fraude; exige-se que a instituição atue ativamente para impedir que a transação fraudulenta ingresse no sistema.

CC BY NC SA

Como resposta a essa demanda de governança, a Resolução BCB 501, de 11 de setembro de 2025, impõe às instituições financeiras e de pagamento o dever de rejeitar transações – sejam Pix, TED ou boletos – destinadas a contas com "fundada suspeita de envolvimento em fraudes" (Brasil, 2025c). A norma estabelece que a avaliação de suspeita deve considerar informações constantes em bancos de dados compartilhados, sistemas eletrônicos públicos ou privados e, crucialmente, o perfil comportamental da conta destinatária, criando uma barreira de entrada preventiva para ilícitos no ecossistema de pagamentos (Brasil, 2025c).

A celeridade na contestação também foi elevada a requisito regulatório. Reconhecendo que cada minuto é crucial na recuperação de ativos digitais, o regulador determinou a implementação de funcionalidades de "autoatendimento" nos aplicativos bancários. Desde outubro de 2025, os participantes do Pix devem disponibilizar canal direto para que o usuário conteste a transação e acione o MED sem a necessidade de trâmites burocráticos via *call center* (Brasil, 2025a). Essa medida reduz o tempo de resposta entre a percepção do golpe e o bloqueio cautelar, aumentando substancialmente a efetividade da medida administrativa.

3 A responsabilidade civil e a proteção do consumidor na jurisprudência

A judicialização das fraudes bancárias digitais no Brasil atingiu um ponto de inflexão. O Poder Judiciário, instado a resolver litígios de massa decorrentes da digitalização compulsória dos serviços financeiros, tem reconfigurado os dogmas da responsabilidade civil. A análise da jurisprudência recente, especialmente do STJ e do TCU, revela o abandono progressivo da tese da "culpa exclusiva da vítima" em favor de uma doutrina que privilegia o "dever de segurança" e a integridade do perfil do consumidor como bens jurídicos tutelados.

3.1 A Súmula 479 do STJ e a desconstrução da culpa do consumidor

A base da responsabilidade bancária reside na Súmula 479 do STJ. Contudo, a aplicação desse verbete vinha encontrando resistência em casos de engenharia social. Recentemente, no julgamento do Recurso Especial 2.220.333/DF, a Corte Superior refinou esse entendimento ao afastar a tese de culpa concorrente do consumidor em casos de "golpe da mão fantasma" (acesso remoto). O Tribunal assentou que não é razoável exigir do consumidor médio que pressuponha o risco de dano ao seguir orientações de suposto funcionário do banco, consolidando que a falha nos mecanismos de segurança da instituição prepondera sobre a vulnerabilidade da vítima (Brasil, 2025h).

Essa evolução jurisprudencial, que migrou da culpa exclusiva da vítima para o dever de segurança intrínseco à atividade, encontra agora respaldo legislativo expresso. A responsabilidade objetiva das instituições ganha novos contornos com a Lei 15.252/2025 (Brasil, 2025g), que dispõe sobre os direitos da pessoa natural usuária de serviços financeiros. Ao positivar a segurança digital não apenas como requisito técnico, mas como garantia fundamental do usuário, o novo diploma legal reforça a tese do STJ de que a falha nos mecanismos de monitoramento constitui, por si só, violação de direito básico, esvaziando alegações de culpa concorrente em cenários de engenharia social complexa.

A doutrina contemporânea e a jurisprudência mais recente do STJ têm criticado a exigência de um "consumidor perfeito": um indivíduo hipervigilante, detentor de conhecimentos técnicos de cibersegurança e imune a manipulações psicológicas. Essa construção idealizada servia como um atalho argumentativo para a "racionalização da culpa", deslocando o foco da falha sistêmica de segurança para o comportamento da parte hipossuficiente.

O entendimento atual rechaça essa lógica. O risco da atividade bancária digital não se limita à invasão de *hackers* aos servidores do banco (falha de segurança clássica), mas abrange também a falha na detecção de transações que destoam do perfil de consumo do cliente. Se o sistema antifraude da instituição permite que um idoso, acostumado a transações de baixo valor, realize múltiplas transferências vultosas em curto lapso temporal para contas desconhecidas, houve falha na prestação do serviço por inobservância do dever de vigilância, caracterizando o defeito do serviço nos moldes do art. 14, § 1º, do Código de Defesa do Consumidor (CDC) (Brasil, 2025i).

3.2 O "golpe da falsa central", a tecnologia de *spoofing* e o *distinguishing* no STJ

A complexidade das fraudes atuais exige uma análise fática detalhada. No julgamento paradigmático do Recurso Especial 2.222.059/SP (Brasil, 2025i), a Terceira Turma do STJ analisou o "golpe da falsa central", no qual criminosos utilizam a tecnologia de *spoofing* para mascarar o número telefônico e simular a central oficial do banco. O Ministro Relator Ricardo Villas Bôas Cueva destacou que a instituição financeira tem o dever de identificar transações que fogem ao padrão de consumo do correntista.

A decisão estabeleceu que a validação de operações suspeitas, atípicas e sequenciais deixa à mostra a existência de defeito na prestação do serviço, ensejando a responsabilização objetiva da instituição por falha no dever de segurança e vigilância, independentemente da entrega de dados pela vítima ludibriada (Brasil, 2025i).

O STJ estabeleceu critérios objetivos para a identificação da responsabilidade da instituição, afastando a culpa exclusiva ou concorrente do consumidor quando presentes os seguintes elementos:

- Quebra de perfil: realização de transações atípicas em horários, locais ou valores destoantes do histórico do usuário.
- Sequencialidade: intervalos curtos entre múltiplas operações (transferências em série).
- Vazamento de dados: o fato de o fraudador possuir dados sigilosos do cliente (nome completo, CPF, agência) antes mesmo do contato induz à presunção de falha na custódia de dados, atraindo a incidência da LGPD em diálogo com o CDC.

Ademais, em casos envolvendo o "golpe da mão fantasma" (acesso remoto ao dispositivo), a jurisprudência, exemplificada pelo REsp 2.220.333/DF, firmou-se no sentido de que a adesão aos canais digitais não pode ser interpretada como assunção de risco pelo consumidor. Se o banco falha em detectar a instalação de *software* malicioso ou a realização de empréstimos seguidos de transferências imediatas (o que contraria a lógica econômica racional), deve responder integralmente pelos prejuízos, sendo incabível a divisão proporcional de culpa (Brasil, 2025h).

3.3 A atuação do TCU e a tutela coletiva dos hipervulneráveis

Enquanto o Judiciário atua na reparação do dano individual, o TCU assumiu o protagonismo na exigência de políticas públicas preventivas, especialmente voltadas aos grupos hipervulneráveis. No Acórdão 2.875/2025 – Plenário, a Corte de Contas realizou uma auditoria operacional que identificou falhas estruturais na proteção da pessoa idosa contra fraudes digitais (Brasil, 2025j).

CC BY NC SA

O relatório apontou três fragilidades sistêmicas que facilitam a engenharia social:

- telecomunicações: a facilidade na obtenção de linhas telefônicas com cadastros precários permite o anonimato dos fraudadores;
- educação financeira: a ausência de campanhas contínuas e adaptadas à linguagem do público idoso;
- ineficácia do bloqueio: a demora das instituições financeiras em aplicar mecanismos como o bloqueio cautelar e o MED de forma uniforme (Brasil, 2025).

O Ministro Relator Augusto Nardes foi enfático ao declarar que "quem ainda não é idoso vai chegar lá", determinando uma atuação interministerial (Justiça, Direitos Humanos, Banco Central e Anatel) para combater a raiz do problema. Entre as determinações, destaca-se a exigência de aprimoramento da rastreabilidade de chamadas para combater o *spoofing* e o uso indevido de nomes de instituições oficiais – inclusive do próprio TCU – por criminosos (Brasil, 2025).

Essa abordagem sistêmica do TCU reforça a tese de que a segurança no ecossistema de pagamentos é um bem público, cuja garantia não pode depender apenas da diligência individual de consumidores vulneráveis, mas de uma arquitetura regulatória e tecnológica robusta, capaz de antecipar e neutralizar vetores de ataque.

4 A nova fronteira tecnológica e o *enforcement* estatal: Open Finance, inteligência artificial e o regime sancionador

A complexidade das fraudes financeiras contemporâneas, caracterizadas pela velocidade e pela transnacionalidade, impôs ao regulador o desafio de transitar de um modelo de supervisão baseada em conformidade documental para uma supervisão baseada em risco e tecnologia. Nesse cenário, o arcabouço normativo do SFN sofreu, ao longo de 2025, uma atualização estrutural, consolidando a premissa de que a inovação trazida pelo Open Finance e pela Inteligência Artificial (IA) não deve servir apenas à eficiência comercial, mas precipuamente à higidez do sistema. Paralelamente, o recrudescimento do regime sancionador sinaliza uma postura de "tolerância zero" com a negligência institucional na prevenção à lavagem de dinheiro e às fraudes digitais.

4.1 A integração do Open Finance na modelagem de risco (Resolução BCB 506/2025)

O Sistema Financeiro Aberto (Open Finance) transcendeu sua vocação inicial de portabilidade e competitividade para se converter em um instrumento vital de segurança sistêmica. A Resolução BCB 506, de 26 de setembro de 2025, representa um marco regulatório ao disciplinar o uso de dados compartilhados especificamente para a prevenção de fraudes e a gestão de riscos. A norma faculta às instituições participantes a utilização do histórico comportamental compartilhado para refinar seus modelos de *scoring*, permitindo uma análise preditiva mais robusta sobre o perfil do usuário (Brasil, 2025d).

Inova-se, ainda, com a introdução da figura da "marcação de fraude transacional". Por meio desse mecanismo, o Prestador de Serviços de Pagamento (PSP) deve identificar e marcar, em sua própria base, transações ou usuários com fundada suspeita de ilicitude. O efeito jurídico dessa marcação é imediato e sistêmico: uma vez efetivada a notificação de infração ou a marcação, determina-se o bloqueio de novas transações (exceto devoluções) e vedam-se expressamente a portabilidade e a reivindicação de chaves Pix pelo usuário marcado, impedindo a migração da fraude para outras instituições (Brasil, 2025d).

Sob a ótica jurídica, essa medida mitiga a assimetria informacional que historicamente beneficiava estelionatários, que exploravam a falta de comunicação entre os agentes do mercado. A integração de dados cadastrais e transacionais ergue uma barreira de entrada operacional, impedindo que a fragmentação do sistema financeiro seja utilizada como vetor para a pulverização e ocultação de ativos ilícitos (Brasil, 2025d).

4.2 Inteligência artificial e auditoria algorítmica (Instrução Normativa BCB 587/2025)

A automação da detecção de fraudes deixou de ser uma faculdade de gestão para se tornar um requisito técnico auditável e cogente. A Instrução Normativa BCB 587, de 31 de janeiro de 2025, estabeleceu os requisitos técnicos e operacionais para o uso de inteligência artificial e *machine learning* nos processos de prevenção a fraudes (Brasil, 2025b).

O normativo impõe um dever de *accountability* (prestação de contas) sobre os algoritmos. Não basta que a IA bloqueie uma transação suspeita; a instituição deve garantir que a decisão automatizada seja passível de auditoria, assegurando a transparência e a "explicabilidade" das decisões. Essa exigência dialoga diretamente com os princípios da LGPD e do Código de Defesa do Consumidor, visando evitar o "viés algorítmico" e garantir que o bloqueio cautelar não se convole em negativa injustificada de prestação de serviço (Brasil, 2025d).

Ademais, a regulação exige que os sistemas antifraude passem por auditorias, com documentação rigorosa de regras, parâmetros e justificativas para os alertas gerados. Essa "auditoria algorítmica" visa assegurar que a tecnologia atue dentro dos limites da legalidade, prevenindo abusos na gestão automatizada de riscos e garantindo a confiabilidade dos mecanismos de bloqueio (Brasil, 2025d).

4.3 O regime sancionador e a efetividade da norma (Resolução BCB 507/2025)

A eficácia da norma jurídica depende, em *ultima ratio*, da credibilidade de sua sanção. Reconhecendo a necessidade de *enforcement* rigoroso, o BC editou a Resolução BCB 507, de 26 de setembro de 2025, que aprovou o novo Manual de Penalidades do Pix, revogando a anterior Resolução BCB 177/2021 (Brasil, 2025e).

O novo diploma inova ao tipificar a "reincidência específica" como agravante severa e ao estabelecer multas que podem atingir o patamar de R$1.000.000,00 (um milhão de reais), multiplicadas por fatores de ponderação baseados no porte da instituição (Ativos Totais) (Brasil, 2025e). A norma prevê sanções específicas para falhas na rejeição de transações suspeitas, inobservância das regras de bloqueio cautelar e omissão no uso do MED (Brasil, 2025e).

Além da sanção pecuniária, o regulamento prevê a penalidade capital de exclusão do Pix para participantes que não cessarem práticas de risco ou que atuarem com negligência contumaz na gestão de "contas-laranjas". Essa postura regulatória alinha-se ao entendimento do TCU, que, no Acórdão 168/2026 – Plenário, determinou a inabilitação de empregados de instituições financeiras envolvidos em fraudes na concessão de crédito, reforçando que a responsabilidade alcança não apenas a pessoa jurídica, mas também os agentes que concorrem para o ilícito com dolo ou erro grosseiro (Brasil, 2026).

Portanto, o novo regime sancionador consolida uma política de responsabilização objetiva e tempestiva, transferindo o risco da operação para quem tem o dever de vigiá-la, em consonância com a jurisprudência do STJ sobre o fortuito interno.

CC BY NC SA

Conclusão

O percurso analítico trilhado neste estudo permite concluir que a segurança cibernética no SFN transcendeu a natureza de requisito operacional para se consolidar como um elemento central da estabilidade financeira e da cidadania. A digitalização acelerada dos meios de pagamento, simbolizada pelo Pix, trouxe inegáveis ganhos de eficiência, mas expôs o consumidor a um cenário de vulnerabilidade agravada, no qual a sofisticação da engenharia social exige uma resposta estatal enérgica e coordenada.

A evolução do arcabouço regulatório, capitaneada pelo CMN e pelo BC, demonstra uma acertada mudança de paradigma: abandona-se a lógica da "segurança de perímetro" individualizada em favor de um sistema de "inteligência colaborativa". A Resolução Conjunta 6/2023 é o marco dessa transição, ao impor o compartilhamento de dados sobre fraudes como dever jurídico, mitigando a assimetria informacional que historicamente favorecia a impunidade e a reiteração criminosa por meio de "contas-laranjas" (Brasil, 2023b; Finsiders Brasil, 2023).

No âmbito da responsabilidade civil, a jurisprudência do STJ, notadamente no julgamento do REsp 2.222.059, reafirmou a teoria do risco do empreendimento. Ao reconhecer que falhas na detecção de transações atípicas – que fogem ao perfil do usuário – configuram fortuito interno, a Corte Superior afastou a aplicação automática da culpa exclusiva da vítima em casos de golpes como o da "falsa central". Consolida-se, assim, o entendimento de que o dever de segurança das instituições financeiras engloba não apenas a blindagem contra invasões externas (*hackers*), mas também o monitoramento comportamental ativo capaz de interceptar movimentações suspeitas, ainda que autorizadas pelo consumidor ludibriado (Brasil, 2025i).

A tutela dos hipervulneráveis, por sua vez, ganhou relevo na atuação do Tribunal de Contas da União (TCU). O Acórdão 2.875/2025 evidenciou que a exclusão digital e a fragilidade de grupos como os idosos demandam políticas públicas integradas, envolvendo não apenas o regulador financeiro, mas também a Anatel e o Ministério da Justiça, para combater a raiz tecnológica dos golpes, como o *spoofing* e a concessão indiscriminada de linhas telefônicas (Brasil, 2025j). Ademais, a postura sancionadora do TCU, exemplificada no Acórdão 168/2026, ao inabilitar gestores por fraudes em operações de crédito, reforça a necessidade de *accountability* e integridade na condução dos processos internos das instituições (Brasil, 2026).

Do ponto de vista instrumental, o aprimoramento do MED e as novas regras do Pix, que autorizam o bloqueio cautelar e a rejeição de transações para contas marcadas, conferiram maior efetividade à recuperação de ativos (Brasil, 2025a). A integração dessas ferramentas com o Open Finance e a Inteligência Artificial, sob a égide da Lei 15.252/2025 e das normas de auditoria algorítmica, promete refinar a modelagem de risco, reduzindo falsos positivos e garantindo a explicabilidade dos bloqueios.

Por fim, a cooperação interinstitucional, materializada na parceria entre a Advocacia-Geral da União (AGU) e o BC no âmbito do Programa Nacional de Enfrentamento à Desinformação (PNDD), fecha o cerco contra as fraudes ao atuar na defesa da confiança pública na moeda (AGU, 2025). Resta evidente que a garantia da cidadania financeira no ambiente digital não depende apenas de tecnologia, mas de uma arquitetura jurídica que transfira o risco da inovação para quem a explora economicamente. Apenas com a perene atualização normativa e o *enforcement* rigoroso dos órgãos de controle será possível assegurar a integridade do patrimônio do consumidor brasileiro diante das novas fronteiras do crime digital.

Referências

ADVOCACIA-GERAL DA UNIÃO (AGU). **AGU e Banco Central se unem para combater golpes na Internet.** Brasília: AGU, 10 out. 2025. Disponível em: https://www.gov.br/agu. Acesso em: 18 fev. 2026.

BRASIL. Banco Central do Brasil. **BC aprimora o Mecanismo Especial de Devolução do Pix**. Brasília: BCB, 28 ago. 2025a. Disponível em: https://www.bcb.gov.br. Acesso em: 18 fev. 2026.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB 587, de 31 de janeiro de 2025**. Estabelece requisitos técnicos e operacionais para o uso de inteligência artificial. Diário Oficial da União: seção 1, Brasília, DF, 2025b.

BRASIL. Banco Central do Brasil. **Resolução BCB 402, de 22 de julho de 2024**. Altera o regulamento anexo à Resolução BCB 1, de 12 de agosto de 2020. Diário Oficial da União: seção 1, Brasília, DF, 23 jul. 2024.

BRASIL. Banco Central do Brasil. **Resolução BCB 501, de 11 de setembro de 2025**. Altera a Resolução BCB 142, de 23 de setembro de 2021. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 2025c.

BRASIL. Banco Central do Brasil. **Resolução BCB 506, de 26 de setembro de 2025**. Dispõe sobre o uso de dados compartilhados no Open Finance para prevenção de fraudes. Diário Oficial da União: seção 1, Brasília, DF, 2025d.

BRASIL. Banco Central do Brasil. **Resolução BCB 507, de 26 de setembro de 2025**. Aprova o Manual de Penalidades do Pix. Diário Oficial da União: seção 1, Brasília, DF, 2025e.

BRASIL. Banco Central do Brasil. **Resolução Conjunta 6, de 23 de maio de 2023**. Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes. Diário Oficial da União: seção 1, Brasília, DF, 24 maio 2023a.

BRASIL. Banco Central do Brasil. **Voto 84/2023–BCB, de 10 de maio de 2023**. Assuntos de Regulação. Brasília: BC, 2023b.

BRASIL. Conselho Monetário Nacional. **Resolução CMN 5.274, de 18 de dezembro de 2025**. Altera a Resolução CMN 4.893, de 26 de fevereiro de 2021. Diário Oficial da União: seção 1, Brasília, DF, 2025f.

BRASIL. **Lei 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais. Diário Oficial da União: seção 1, Brasília, DF, 22 dez. 2022.

BRASIL. **Lei 15.252, de 4 de novembro de 2025**. Dispõe sobre os direitos da pessoa natural usuária de serviços financeiros. Diário Oficial da União: seção 1, Brasília, DF, 5 nov. 2025g.

BRASIL. Ministério da Fazenda. **Tentativas de fraudes e golpes mais comuns com o Pix**: conheça quais são e saiba como evitá-los. Brasília: Ministério da Fazenda, 9 mar. 2023c.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 2.220.333/DF**. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma. Julgado em 14 nov. 2025. Diário da Justiça Eletrônico, Brasília, 2025h.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 2.222.059/SP**. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma. Julgado em 7 out. 2025. Diário da Justiça Eletrônico, Brasília, 21 out. 2025i.

CC BY NC SA

BRASIL. Tribunal de Contas da União. **Acórdão 2.875/2025 – Plenário**. Relator: Ministro Augusto Nardes. Processo TC 007.081/2025-1. Sessão de 3 dez. 2025. Diário Oficial da União, Brasília, DF, 2025j.

BRASIL. Tribunal de Contas da União. **Acórdão 168/2026 – Plenário**. Tomada de Contas Especial. Relator: Ministro Augusto Nardes. Processo TC 040.538/2023-0. Sessão de 28 jan. 2026. Diário Oficial da União, Brasília, DF, 2026.

FINSIDERS BRASIL. CMN e BC regulamentam o compartilhamento de dados entre bancos para melhorar prevenção a fraudes. **Finsiders Brasil**, 23 maio 2023.

INFOMONEY. Foi vítima de golpe com Pix? Conheça ferramenta do Banco Central para reaver seu dinheiro. **InfoMoney**, 27 out. 2023.