Fraudes bancárias: enfrentamento correto para um desenvolvimento econômico sadio

Igor Sant'Anna Tamasauskas
Advogado.
Doutor e Mestre em Direito do Estado pela Faculdade de Direito da Universidade de São Paulo.

Pierpaolo Cruz Bottini
Advogado.
Livre Docente em Direito Penal.
Professor da Faculdade de Direito da Universidade de São Paulo.

RESUMO

O artigo analisa o aumento das fraudes bancárias no Brasil e propõe estratégias jurídicas e tecnológicas para seu enfrentamento. Destaca o impacto da digitalização e do PIX no crescimento de golpes financeiros, que causam bilhões em prejuízos anuais. Defende-se a cooperação entre instituições financeiras, órgãos de controle e o Judiciário, bem como o investimento contínuo em segurança e educação do consumidor. A Súmula 479 do STJ e decisões recentes reforçam a responsabilidade objetiva dos bancos, mas o texto ressalta a importância de limitar essa responsabilidade quando houver culpa do usuário. O estudo conclui que o combate efetivo às fraudes deve equilibrar prevenção, responsabilização e eficiência econômica, assegurando um desenvolvimento financeiro sustentável e seguro.

Palavras-chave: Fraudes bancárias. Responsabilidade civil. Sistema financeiro. Direito digital.

ABSTRACT

This article analyzes the rise in bank fraud in Brazil and proposes legal and technological strategies to combat it. It highlights the impact of digitalization and the PIX (Investor's ID) on the growth of financial scams, which cause billions in annual losses. It advocates for cooperation between financial institutions, regulatory agencies, and the judiciary, as well as continued investment in security and consumer

education. Summary 479 of the Superior Court of Justice (STJ) and recent decisions reinforce the strict liability of banks, but the text emphasizes the importance of limiting this liability when the user is at fault. The study concludes that effective fraud prevention must balance prevention, accountability, and economic efficiency, ensuring sustainable and secure financial development.

Keywords: Bank fraud. Civil liability. Financial system. Digital law.

Sumário: Introdução; 1. Fraudes bancárias: necessidade de controle adequado; 2. Contribuição do Direito e do Judiciário;

Introdução

Escrever um artigo em homenagem ao Ministro Antonio Carlos Ferreira e não citar temas afetos à atividade bancária seria desconsiderar a exitosa carreira como advogado e diretor jurídico de relevante instituição financeira pública brasileira, para além da contribuição desse jurista brasileiro como integrante do Superior Tribunal de Justiça.

Não bastasse a provocação em razão da carreira do homenageado, a atividade bancária configura-se essencial ao desenvolvimento econômico sadio de um país e, com o avanço da tecnologia, tem propiciado o atendimento de cada vez maiores contingentes de brasileiros, ao mesmo tempo em que se tornou foco crescente de interesses criminosos.

Procuraremos abordar, neste artigo, algumas tipologias de fraudes e sugestões para seu enfrentamento. Nessa linha, o trabalho é dividido em 4 partes: além desta breve introdução, no Capítulo 2 serão apresentadas tipologias mais comuns das fraudes que vêm sofrendo as instituições financeiras.

No Capítulo 3, pretende-se analisar a contribuição do Direito e do Judiciário para controlar minimamente tal cenário.

Em arremate, procuraremos destacar a importância de a sociedade brasileira dedicar atenção ao correto tratamento desse tipo específico de criminalidade, usando todos os enfoques oferecidos pelo Direito para minimizar as graves consequências à economia e aos cidadãos.

1 Fraudes bancárias: necessidade de controle adequado

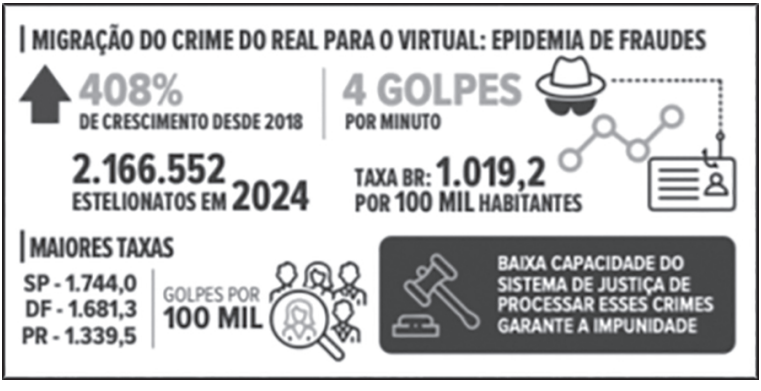
Qualquer atividade econômica está sujeita à ação de fraudadores, interessados na obtenção de retornos financeiros,

usualmente desproporcionais, às custas dos demais atores sociais que agem segundo as normas aprovadas e vigentes. Quando tratamos de atividades financeiras, além da perspectiva desses lucros indevidos, há a possibilidade de escamotear ganhos advindos de outras ações ilícitas.

A dificuldade de controle das ações ocorridas no ambiente financeiro surge a partir de uma simples constatação do volume elevado de transações e atores que compõem o Sistema Financeiro Nacional. Para se ter uma ideia, foram 130,7 bilhões de operações bancárias realizadas por meio de *smartphones* no ano de 2023, de um total de quase 190 bilhões de transações[1]. Temos 200 milhões de concidadãos bancarizados[2] e 890 milhões de chaves PIX cadastradas[3], dados de 2025. Ou seja, uma média de mais de 4 chaves de PIX para cada usuário do serviço.

Há, portanto, considerável complexidade, ao menos pelo volume, para se identificarem, segregarem e afastarem comportamentos que fujam à regra a utilização correta do sistema.

Partindo para esses comportamentos ilícitos, os números também chamam a atenção. Como vemos no excerto do infográfico a seguir, elaborado pelo Fórum Nacional de Segurança Pública, há uma migração da criminalidade para o ambiente virtual:



Fonte: https://forumseguranca.org.br/wp-content/uploads/2025/07/anuario-2025-infografico.pdf)

1 https://agenciabrasil.ebc.com.br/economia/noticia/2024-06/febraban-aponta-que-7-em-cada-10-transacoes-bancarias-sao-celular.

2 https://valor.globo.com/financas/noticia/2025/02/22/brasil-chega-a-200-milhoes-de-pessoas-bancarizadas.ghtml.

3 https://www.bcb.gov.br/estabilidadefinanceira/estatisticaspix.

Nada menos que 36% dos brasileiros foram vítimas de golpes bancários[4], em um total acima de R$ 25 bilhões[5] de prejuízos somente em 2024. São mais de 4,5 mil tentativas de golpes financeiros por hora[6], além de 100 *smartphones* furtados ou roubados por hora[7], com a finalidade de se obterem acesso às contas bancárias das vítimas.

Para fazer frente a essa realidade, bancos dobraram o investimento em tecnologia nos últimos 8 anos, atingindo quase R$ 40 bilhões[8]. Estabeleceu-se modificação legislativa em 2021, para ajustar tipos mais adequados a esse tipo de criminalidade, além de penas mais agravadas[9].

Há também uma crescente preocupação das autoridades no sentido de se limitarem as possibilidades de utilização do sistema financeiro para realocar os recursos obtidos com as condutas criminosas. Desde 2012, sucessivas reformas legislativas e estruturais buscaram dotar o Estado de um aparato que permita acompanhar as movimentações financeiras e acionar as autoridades responsáveis pela persecução penal, em caso de atipicidades.

Como exemplo, colhe-se a referência à atuação do Banco Central e do Conselho Monetário Nacional em estudo elaborado pelo Instituto Esfera, em parceria com o Fórum Brasileiro de Segurança Pública:

> A Resolução Conjunta nº 6/2023 do Banco Central e do Conselho Monetário Nacional (CMN) estabelece que todas as instituições financeiras e de pagamento autorizadas pelo Bacen devem compartilhar informações sobre indícios de fraude entre si, por meio de um sistema eletrônico padronizado e interoperável. A resolução prevê que o registro de informações deve contemplar, no mínimo: a identificação de quem, segundo os indícios disponíveis, teria executado ou tentado exe-

4 https://cbn.globo.com/brasil/noticia/2025/02/18/golpes-bancarios-atingiram-mais-de-36percent-dos-brasileiros-em-2024-aponta-febraban.ghtml.

5 https://forumseguranca.org.br/wp-content/uploads/2025/09/anuario-2025.pdf, pg. 110 e 111.

6 https://g1.globo.com/jornal-nacional/noticia/2024/08/13/pesquisa-revela-que-brasileiros-sao-alvos-de-mais-de-46-mil-tentativas-de-golpe-financeiro-por-hora.ghtml.

7 https://www.poder360.com.br/brasil/brasil-registra-mais-de-100-furtos-ou-roubos-de-celular-por-hora/.

8 https://securityleaders.com.br/cibersegurança-e-prioridade-estrategica-para-100-dos-bancos-brasileiros-afirma-febraban/.

9 https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm.

> cutar a fraude, ou seja, o CPF do suspeito; a descrição dos indícios da ocorrência ou da tentativa de fraude; a identificação da instituição responsável pelo registro dos dados e das informações; e a identificação dos dados da conta destinatária e de seu titular, em caso de transferência ou pagamento de recursos.[10]

Por esse tipo de iniciativa, as instituições integrantes do Sistema Financeiro Nacional são estimuladas a integrarem uma rede de prevenção para detecção de condutas indesejadas – porque fraudadoras – e, a partir disso, adotarem as medidas para controlar a má utilização desse importante setor da economia.

Outro ponto de atenção reside no empréstimo de contas bancárias, de titulares inicialmente legítimos, para que fraudadores as utilizem como passagem para dificultar o rastreamento e a detecção pelas autoridades. Os chamados *conteiros* usualmente acabam à margem da responsabilização criminal por ocuparem posição indevidamente considerada de menor relevância, vis-à-vis daqueles que dirigem as atividades criminosas.

Veio em boa hora, portanto, a iniciativa do Banco Central quanto ao estabelecimento de registros de suspeitas de contas inidôneas ("laranjas"), para que as instituições financeiras possam objetivamente rejeitar operações ou bloquear recursos em determinadas operações[11].

2 Contribuição do Direito e do Judiciário

Um primeiro tópico de relevância para que as fraudes bancárias sejam adequadamente enfrentadas é haver um crescente estímulo, por parte do direito posto e do direito aplicado, à prevenção. Quando se trata de relações estabelecidas entre as instituições financeiras e o usuário final, geralmente, há incidência do Código de Defesa do Consumidor e suas normas de proteção contra falhas de serviço.

Haverá *falha de serviço* quando algum pormenor transacional se desviar da tipicidade corriqueira das operações praticadas por aquele perfil de cliente ou, até mesmo, por determinado correntista em especial. A tecnologia já permite esse tipo de acompanhamento e é natural que as normas que regu-

[10] https://esferabrasil.com.br/wp-content/uploads/2025/07/Lavagem-de-dinheiro-e-enfrentamento-ao-crime-organizado-no-Brasil.pdf.

[11] https://www.bcb.gov.br/detalhenoticia/677/noticia.

lam o sistema financeiro – administrativas, cíveis e mesmo criminais – assim o exija, punindo os responsáveis pelas condutas que contrariarem tal caminho.

Nessa toada, o Superior Tribunal de Justiça editou a Súmula 479, a qual disciplina que *as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias*.

O fortuito interno pode ser caracterizado por falha decorrente do fator humano ou brechas nos sistemas de segurança que permitam a sobreposição volitiva do agente fraudador às regras usuais de prestação desse serviço, ainda que tal agente fraudador seja um terceiro em relação à estrutura bancária.

Esse tipo de reforço normativo é relevante porque estimulará as instituições financeiras a investirem em tecnologia antifraude, monitoramento de operações atípicas e na educação do usuário do serviço. Precisa ficar cada vez mais evidente para o cliente de um banco quais os limites e os padrões de comunicação, por exemplo, para evitar que senhas e outras informações sejam repassadas, via engenharia social, a quadrilhas de fraudadores. De forma similar, o usuário que "empresta" conta bancária precisa ficar ciente que sua conduta não é neutra criminalmente e pode vir a ensejar sua responsabilidade por aquilo que executarem em seu nome.

Ao lado dessa estratégia de estímulo à prevenção pela responsabilização das instituições financeiras, deve-se aprofundar a ideia de cooperação e integração entre as organizações do sistema financeiro e os órgãos de controle e repressão, a serem cada vez mais especializados. Protocolos de atuação, de troca de informações e de integração de comunicações são fundamentais para a devida atuação no controle de práticas fraudadoras, com a agilidade que o atual sistema opera.

Seria impossível cogitar, há pouco tempo, a realização de transações instantâneas via PIX, mesmo em feriados, finais de semana, período noturno. Atualmente – e essa é a realidade de muitos anos já –, praticamente não se tem necessidade de pisar em uma agência bancária, sequer para abrir uma conta.

Dessa forma, tanto o sistema financeiro quanto seus órgãos de controle devem estar autorizados a agir prontamente quando houver fundado receio de práticas indevidas, quer pelo monitoramento mais detido de determinados indivíduos, quer pelo bloqueio de operações suspeitas. De maneira similar, o Poder Judiciário, quando devidamente acionado, não se deve fur-

tar à adoção de mecanismos céleres de remediação, como sequestros e arrestos de valores, cautelares diversas e outras medidas que permitam comunicar claramente as consequências jurídicas a quem não se porta conforme as regras esperadas.

O fomento à prevenção é uma realidade, quer pela jurisprudência referida, quer pelas normas do Banco Central que impõem o dever de cuidado em relação a condutas que impliquem a utilização indevida desse relevante setor econômico, vide, por exemplo, as regras de prevenção à prática de lavagem de capitais. Todavia, há que se estabelecerem limites para que a colaboração das instituições financeiras no enfrentamento desse tipo de criminalidade não configure uma real substituição do Estado repressor.

Justamente nesse sentido emerge relevante posicionamento do Ministro Antonio Carlos Ferreira, nos autos do Recurso Especial n. 2.155.065/MG. Nesses autos, uma consumidora acometida por enfermidade grave foi vítima de golpista que se passou por funcionário de banco.

Esse golpista induziu, mediante técnicas de engenharia social, a consumidora a instalar um aplicativo de acesso remoto em seu celular e, a partir disso, logrou realizar movimentações fraudulentas em sua conta bancária.

Identificando possível responsabilidade da instituição financeira, até pela existência da Súmula n. 479, a vítima acionou a Justiça objetivando a reparação de danos na esfera civil. O julgamento do caso estava empatado em 2 votos a favor da reparação e 2 contrários, quando adveio o voto do Ministro Antonio Carlos Ferreira, que definiu a resolução da lide em favor da instituição bancária.

E a tese central de seu voto-desempate residiu na conduta ativa da consumidora no sentido de facultar ao criminoso o acesso aos seus dados bancários: a responsabilidade objetiva da instituição financeira pode ser afastada se houver atuação bastante da vítima a facilitar a atuação criminal.

Esse precedente é relevante porque impõe uma limitação ao risco da atividade bancária, reduzindo, por certo, os custos da operação e, por consequência, a parcela destes que será repassada aos demais usuários, na forma de *spreads* e demais encargos.

Há que se estender esse tipo de raciocínio para as demais hipóteses de responsabilidade – cível e administrativa – de instituições financeiras – e criminal, no caso de seus dirigentes e prepostos, reservando a responsabilidade para hipóteses em que

claramente constatada a falha na prestação do serviço ou o dolo – ou negligência, conforme o tipo penal –, quando se tratarem de pessoas físicas envolvidas.

Conclusão

Como já assinalado, *o emprego de meios tecnológicos para o cometimento de crimes tem aumentado no país. A criatividade humana vai além das artes e dos engenhos, e costuma campear no terreno do delito, por meio de surpreendentes estratégias de fraude, simulação e engodo. Estelionatos virtuais, desvio de recursos, e o uso de moedas digitais para ocultar recursos ilícitos têm frequentado as páginas policiais.*[12]

O enfrentamento dessa criminalidade deve ser realizado pelo incremento do investimento em segurança e tecnologia bancárias, já objeto de substantiva elevação, como visto anteriormente. Todavia, a técnica de responsabilidade das instituições integrantes do Sistema Financeiro Nacional deve encontrar limitação na aferição, no caso concreto, quanto a falhas efetivamente verificadas na prestação dos serviços, sob pena de onerar excessivamente todo o setor de oferta de crédito e movimentação de recursos.

O mesmo Superior Tribunal de Justiça vem concebendo alguns precedentes sugestivos a apontar para a devida calibragem dos sistemas de segurança e integridade das instituições financeiras:

> Constitui atribuição das instituições financeiras, e de todas aquelas que participam dos denominados arranjos de pagamento, criar mecanismos capazes de identificar e coibir a prática de fraudes e de mantê-los em constante aprimoramento, em virtude do dever de gerir com segurança as movimentações de dinheiro dos seus clientes e do elevado grau de risco da atividade por elas desempenhada. (...)
> Para a identificação de possíveis fraudes, os sistemas de proteção contra fraudes desenvolvidos pelas instituições bancárias/de pagamento devem considerar i) as transações que fogem ao perfil do cliente ou ao seu padrão de consumo ii) o horário e local em que as operações foram realizadas, iii)

[12] https://blogs.oglobo.globo.com/fumus-boni-iuris/post/pierpaolo-cruz-bottini-fintechs-e-lavagem-de-dinheiro.html.

> o intervalo de tempo entre uma e outra transação, iv) a sequência das operações realizadas, v) o meio utilizado para a sua realização, enfim, diversas circunstâncias que, conjugadas, tornam possível ao fornecedor do serviço identificar se determinada transação deve ou não ser validada. (STJ RESP 2222059 – SP)

O aprimoramento desse tipo de decisão, uniformizando a jurisprudência nacional, propiciará maior previsibilidade aos atores, minimizando o risco operacional e, ao fim e ao cabo, o custo de transação.