GOLPES DIGITAIS NO SETOR BANCÁRIO: DESAFIOS AO USUÁRIO E TAMBÉM AO JULGADOR

DIGITAL SCAMS IN THE BANKING SECTOR: challenges for the user and also for the judge.

Aleff Guilherme da Silva Nascimento - Graduado em Direito pela Universidade Positivo. Assessor de Juiz de Direito, atualmente perante a Turma Recursal. Aleff.nascimento@tjpr.jus.br

Fernanda Bernert Michielin - Graduada em Direito pela UFPR. Juíza de Direito Substituta no TJPR atualmente lotada perante a 2ª Turma Recursal. Especialista em Direito Processual Civil. febm@tjpr.jus.br.

O presente artigo trata do desafio atual relacionado as inúmeras fraudes bancárias que vitimizam muitas pessoas e abalam a ordem econômica e social. Dando um panorama dos golpes no setor bancário e o impacto no judiciário, expõe a responsabilidade civil nestes casos e os desafios das provas digitais. Demonstra que o número de crimes virtuais e a distância aumentam exponencialmente, e que necessárias medidas de prevenção e a educação como alicerces da confiança digital.

PALAVRAS-CHAVE: Golpe, fraude virtual, contratos bancários, educação digital, desafios

This article addresses the current challenge posed by the numerous cases of banking fraud that victimize many individuals and undermine economic and social order. By providing an overview of scams in the banking sector and their impact on the judiciary, it discusses civil liability in such cases and the challenges related to digital evidence. It demonstrates that the incidence of cybercrime and the geographical distance between offenders and victims are increasing exponentially, highlighting the need for preventive measures and education as cornerstones of digital trust.

***KEYWORDS**: Scam, online fraud, bank contracts, digital education, challenges*

INTRODUÇÃO

A expansão do uso da internet, o avanço tecnológico, e a massificação das tecnologias da informação e comunicação transformaram profundamente as relações sociais e suas dinâmicas.

Esta digitalização exponencial das relações humanas apresentou inúmeras vantagens, facilitando a vida das pessoas ao trazer rapidez e aproximar partes e localidades, mas também abriu espaço a novas vulnerabilidades, expondo indivíduos, empresas e organizações a novos riscos.

O ambiente cibernético tornou-se um espaço propício para práticas criminosas, desde fraudes financeiras até invasões a sistemas, roubo de identidade, informações pessoais e senhas.

Os mecanismos tradicionais de persecução penal foram pensados em uma realidade analógica e territorializada.

O meio digital potencializa o "artificio" e o "ardil" presentes na conduta típica do estelionato (artigo 171 do Código Penal), por exemplo, de uma maneira sem precedentes. Utilizam-se de conhecimentos de informática e tecnologia, da inteligência artificial, da manipulação da psicologia da vítima e da velocidade que as transações digitais viabilizam.

Tais crimes podem ser planejados e executados a distância e são mais dificilmente combatidos. O agente criminoso se expõe e se arrisca menos, protegendo-se por meio de muitas barreiras.

As modalidades fraudulentas e suas invenções são mais rápidas que as inovações legislativas. Normalmente fazem muitas vítimas de uma única vez, em um mesmo golpe, após a criação de um link sitio eletrônico falso, por exemplo. O investimento na persecução criminosa acaba sendo baixa, pois o conhecimento e manipulação da tecnologia pode render muito e fazer inúmeras vítimas, em um bom "custo benefício".

Ante este cenário, o Direito enfrenta o desafio de acompanhar a evolução desses delitos e de garantir uma regulamentação eficaz para a sua prevenção e repressão. Há o desafio do tempo, antes as rápidas transformações e por vezes a transnacionalidade dessas infrações e à necessidade de mecanismos mais ágeis de investigação e cooperação.

Com esta metamorfose da criminalidade as fraudes digitais se tornaram um dos principais desafios contemporâneos da segurança pública. Há um impacto econômico significativo, seja pelas perdas financeiras oriundas dos ataques, seja pelos valores para a implementação de medidas de segurança. O mencionado panorama demanda medidas cada vez mais dinâmicas por parte das autoridades que são então responsáveis pela aplicação da lei.

> O ciberespaço, antes um domínio restrito à vanguarda tecnológica, consolidou-se como a principal arena para transações comerciais, interações sociais e o exercício da cidadania. Esta migração, acelerada por eventos globais e pela conveniência de ferramentas como os pagamentos instantâneos – notadamente o sistema PIX no Brasil, que revolucionou a dinâmica financeira –, trouxe consigo não apenas progresso, mas a sofisticação e a massificação de condutas criminosas. As fraudes digitais, em suas múltiplas roupagens (como phishing, pharming, engenharia social e golpes de falsa central de atendimento), deixaram de ser incidentes isolados para se tornarem um fenômeno endêmico, com profundo impacto na estabilidade econômica e na sensação de segurança da população (...) o aparato estatal de persecução penal, historicamente moldado para combater o crime físico e territorializado, encontra-se em severa dificuldade para responder a esta nova modalidade delitiva. A velocidade, o anonimato relativo, a transnacionalidade e, principalmente, a escala industrial das fraudes digitais impõem um desafio sistêmico[34].

[34] Douglas Angelo Ferrari, Marcianita Lopata de Lima , Flávia Jeanne Ferrari. **Edição Atual .** v. 1 n. 32 (2025): REVISTA JURÍDICA GRALHA AZUL OUT/2025 - NOV/2025 : FRAUDES DIGITAIS E SEGURANÇA PÚBLICA: a atuação integrada entre juizados especiais, ministério público e polícia militar. GRALHA AZUL – periódico científico da EJUD-PR. p. 4.

A população segue desconfiada e com uma sensação de insegurança, impunidade. Não se resolvem facilmente as situações postas, os golpes são por vezes realizados fora da localidade, em outros estados e até mesmo países. Há um abalo a ordem pública.

Há um descrédito nas instituições, dentre elas a Justiça e o aumento do número de demandas.

1 PANORAMA DOS GOLPES DIGITAIS NO SETOR BANCÁRIO E O IMPACTO NO JUDICIÁRIO

O Brasil enfrenta uma epidemia de golpes digitais que afeta diretamente o setor bancário e seus contratos eletrônicos. De acordo com pesquisa do DataSenado[35] entre outubro de 2023 e outubro de 2024, cerca de 40,85 milhões de brasileiros (24% da população acima de 16 anos) tiveram prejuízo financeiro em razão de crimes cibernéticos como clonagem de cartões, fraudes on-line ou invasões de contas bancárias. O estudo ainda mostra que os golpes não escolhem classe social ou região, a vitimização é distribuída de forma relativamente uniforme no país.

Da mesma forma, a Associação de Defesa de Dados Pessoais e do Consumidor (ADDP) apontou um crescimento alarmante na incidência de golpes: quase 50% de aumento em 2024 em comparação a 2023, sendo que estimativas preliminares indicam que cerca de 5 milhões de golpes on-line foram efetivamente consumados em 2024, confirmando a tendência de expansão desse tipo de crime[36].

Os golpistas têm aprimorado suas táticas em velocidade e criatividade surpreendentes, que ganham ainda mais impulso com a ajuda de tecnologia, inclusive simulações de voz e imagem via inteligência artificial, dificultando a distinção entre comunicações legítimas e fraudes.

É de fácil compreensão e até mesmo perceptível que organizações criminosas enxerguem nos crimes cibernéticos uma relação custo-benefício vantajosa em comparação aos crimes tradicionais, como assaltos e sequestros, pois a ação digital implica em menores riscos de prisão ou violência física.

Muitas são as notícias de que os crimes patrimoniais cometidos presencialmente tem diminuído, dando espaço justamente ao exponente crescimento do crime virtuais.

Segundo dados da edição 2024 do Anuário Brasileiro de Segurança Pública, essa mudança reflete uma tendência mundial e se

35 https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado <acessado em 01/12/2025>

36 https://addp.com.br/addp/golpes-on-line-tiveram-alta-significativa-em-2024/ <acessado em 01/12/2025>

> consolidou de maneira definitiva no Brasil após o arrefecimento da pandemia, quando uma parcela mais significativa da população começou a digitalizar mais aspectos de suas vidas.[37]

Como resultado, golpes bancários diversos, *phishing* sofisticado e fraudes por engenharia social encabeçam a lista das fraudes mais praticadas.

A FEBRABAN (Federação Brasileira de Bancos) divulgou[38], em 2024, um ranking das principais fraudes enfrentadas por clientes bancários. Dentre os 10 golpes mais comuns destacam-se modalidades de engenharia social, por exemplo:

- golpe do WhatsApp (clonagem de conta de mensagem mediante código de verificação enviado à vítima);

- falsa central telefônica/falso funcionário (fraudador se passa por atendente do banco e induz transferências);

- phishing clássico (mensagens ou sites falsos para capturar senhas e dados);

- golpe do falso investimento (pirâmides financeiras on-line prometendo altos rendimentos);

- troca de cartão (subtração do cartão físico após observar a senha);

- falso motoboy (coleta indevida do cartão sob pretexto de perícia, após obtenção da senha);

- entre outros.

Todas essas fraudes exploram a confiança do usuário e vulnerabilidades nos canais digitais de atendimento, vejamos:

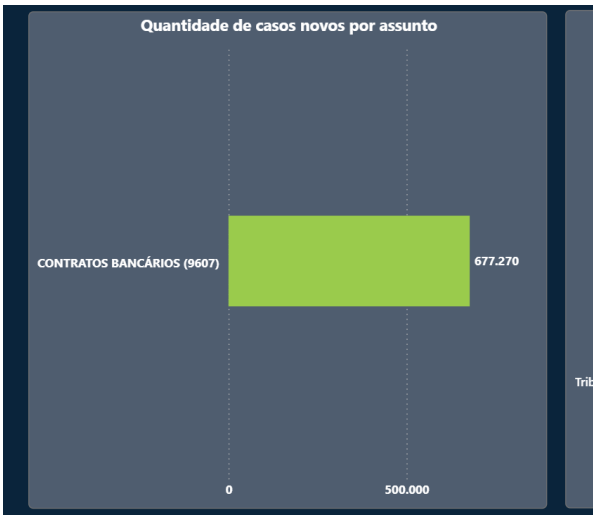
O impacto no Judiciário tem sido imediato. De acordo com dados estatísticos do judiciário, divulgados pelo site do CNJ[39], o tema "contratos bancários" está entre os maiores assuntos de judicialização, eis que somente no ano de 2023 foram verificados 595.088 novos casos, e não bastasse o número alarmante, em 2024 foram 677.270 novas ações ajuizados, o que representa um aumento de aproximadamente 12%:

---

37 https://oglobo.globo.com/brasil/noticia/2024/07/18/golpes-virtuais-crescem-no-brasil-enquanto-roubos-presenciais-diminuem.ghtml <acessado em 14/12/2025>

38 https://portal.febraban.org.br/noticia/4279/pt-br/ <acessado em 01/12/2025>

39 https://justica-em-numeros.cnj.jus.br/painel-estatisticas/ <acessado em 01/12/2025>



Grande parte dessas demandas decorre justamente de fraudes e golpes digitais associados a contratos eletrônicos. Por exemplo, consumidores que buscam anular empréstimos contratados por terceiros em seu nome, vítimas pleiteando ressarcimento de valores transferidos indevidamente, ou bancos executando contratos eletrônicos cuja autenticidade é questionada em juízo. O resultado é uma sobrecarga no sistema de justiça, que precisa lidar com novas questões de fato e de direito trazidas pela era digital.

Esse cenário coloca em xeque a segurança jurídica dos contratos bancários eletrônicos. De um lado, a transformação digital trouxe agilidade e conveniência para contratação de empréstimos, abertura de contas e realização de transações financeiras via aplicativos e internet banking. De outro lado, a ausência de um documento físico e os conhecimentos limitados de muitos usuários geram incerteza e disputas sobre a validade de contratos firmados virtualmente.

Muitos são os casos em que o consumidor alega não ter reconhecido a contratação ou não ter sido devidamente ou suficientemente informado acerca da mesma, enquanto a instituição financeira apresenta registros eletrônicos que, em tese, demonstram a anuência do contratante.

Com efeito, questões sobre validade da assinatura eletrônica, falhas na informação ao consumidor, vazamento de dados e práticas enganosas tornaram-se centrais nesses litígios, exigindo dos tribunais uma adaptação rápida a temas de direito digital.

Em síntese, os números evidenciam que fraudes digitais massivas minam a confiança nas operações bancárias e acabam repercutindo no Judiciário e no debate jurídico.

Necessário o exame das bases legais e doutrinárias que asseguram a validade dos contratos eletrônicos bancários, bem como a distribuição de responsabilidades e os meios de prova utilizados para resolver tais conflitos.

2 VALIDADE JURÍDICA DOS CONTRATOS BANCÁRIOS ELETRÔNICOS

Os contratos celebrados por meio eletrônico possuem amparo legal expresso no Brasil, gozando da mesma eficácia dos contratos tradicionais escritos em papel. O Código Civil estabelece, em seu art. 104, os requisitos de validade dos negócios jurídicos (agente capaz, objeto lícito e forma não proibida por lei), critérios que se aplicam igualmente aos contratos eletrônicos.

Não há, portanto, vedação à forma digital; ao contrário, o princípio da liberdade de formas (art. 107 do CC) e o reconhecimento da equivalência funcional dos documentos eletrônicos sustentam a legitimidade dos acordos firmados em meio virtual.

Como resume Fábio Ulhoa Coelho[40], *"o contrato eletrônico é celebrado por meio de transmissão eletrônica de dados. A manifestação de vontade dos contratantes (oferta e aceitação) não se vincula nem oralmente, nem por documento escrito, mas pelo registro em meio virtual (isto é, despapelizado)"*. Ou seja, muda o suporte, mas o acordo de vontades continua tendo valor jurídico.

Nos últimos anos, várias normas reforçaram a segurança jurídica dos contratos eletrônicos. Dentre elas, a Lei da Liberdade Econômica (Lei 13.874/2019) consagrou princípios de desburocratização, reconhecendo a validade de contratos e acordos realizados por meios digitais como expressão da autonomia das partes, salvo exigência legal específica em contrário.

Já o Marco Civil da Internet (Lei 12.965/2014) estabeleceu direitos e deveres para uso da internet no Brasil, garantindo a validade jurídica dos registros eletrônicos e a proteção de dados pessoais e privacidade nas relações on-line – elementos fundamentais para dar confiança aos contratos celebrados via internet.

A Lei Geral de Proteção de Dados (LGPD, Lei 13.709/2018), embora não trate diretamente de contratos, impõe às empresas (inclusive bancos) deveres de proteger os dados pessoais dos clientes. Isso abrange dados coletados para firmar contratos eletrônicos (como biometria facial, documentos digitalizados, identificadores de dispositivo etc.), cuja guarda segura é essencial. A conformidade com a LGPD previne vazamentos que poderiam comprometer contratos e evidencia a seriedade no tratamento das informações do consumidor.

A Medida Provisória 2.200-2/2001, ainda em vigor, criou a ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) e conferiu validade legal às assinaturas digitais certificadas por autoridade credenciada. Importante destacar que essa MP *não* invalidou outros meios de comprovação de autoria, conforme seu art. 10, §2º, documentos eletrônicos assinados por meios diversos (não ICP) também são válidos se admitidos pela pessoa a quem forem opostos e desde que atendam aos requisitos de autenticidade e integridade. Em suma, o certificado digital padrão ICP-Brasil gera uma presunção legal de autenticidade, mas não é o único método possível de assinatura eletrônica no âmbito privado.

[40] COELHO, Fábio Ulhoa. Curso de direito comercial. São Paulo: Saraiva, 2012. v. 3, pg. 64 E-book.

Mais recentemente, a Lei 14.063/2020 disciplinou as assinaturas eletrônicas em interações com entes públicos, classificando-as em três tipos: simples, avançada e qualificada. Essa classificação foi absorvida pela prática geral e pela jurisprudência, que passou a aplicar tais conceitos também às relações entre particulares.

A Lei 14.620/2023, por sua vez, alterou o Código de Processo Civil para incluir o §4º no artigo 784, dispondo que documentos assinados eletronicamente, em qualquer modalidade de assinatura, têm força de título executivo extrajudicial, desde que seja possível verificar sua integridade.

A jurisprudência do Superior Tribunal de Justiça (STJ) tem acompanhado e consolidado esse arcabouço legal. Um caso representativo é o REsp 2.150.278/PR, julgado em setembro de 2024 pela 3ª Turma (Rel. Ministra Nancy Andrighi), que envolveu a execução de uma cédula de crédito bancário assinada eletronicamente por plataforma não vinculada à ICP-Brasil.

No referido julgado, o STJ reafirmou pontos cruciais: (i) as assinaturas eletrônicas simples, avançada e qualificada possuem diferentes níveis de segurança e força probatória, mas todas têm validade jurídica, respeitando-se a autonomia privada das partes quanto à forma de se vincular; (ii) a assinatura eletrônica avançada (com múltiplos fatores de autenticação, como login, senha, token SMS, biometria ou geolocalização) foi comparada por analogia pela Ministra relatora à firma reconhecida por semelhança em papel, enquanto a assinatura qualificada (com certificado digital) equivale à firma reconhecida por autenticidade em cartório. Ambas são válidas, diferenciando-se apenas no grau de dificuldade de impugnação técnica da autoria ou integridade do documento.

Em outras palavras, prevalece o entendimento de que a forma eletrônica é livre e válida, desde que haja algum método confiável de identificação das partes e de preservação do conteúdo contratado.

Vale ressaltar que, no contexto bancário, as instituições têm investido em medidas para validar contratos à distância. Muitos bancos exigem que o cliente, ao contratar um empréstimo via aplicativo, realize um reconhecimento facial (selfie), ou insira códigos recebidos no celular, de forma a gerar evidências da autenticidade do consentimento. Tais práticas são coerentes com o estabelecido no art. 441 do Código de Processo Civil, que admite documentos eletrônicos produzidos conforme legislação específica.

Desde que o banco guarde corretamente essas provas digitais, em conformidade com as normas de proteção de dados, o contrato eletrônico assim firmado terá plenas condições de ser apresentado em juízo e de vincular as partes.

A atenção à cadeia de custódia das evidências eletrônicas (armazenamento seguro de dados biométricos, certificados e logs) é parte da segurança jurídica, porquanto evita-se alegações de adulteração ou extravio, reforçando

a confiança do Judiciário naquilo que foi contratado virtualmente.

Destarte, contratos bancários eletrônicos são válidos e exigíveis, assim como os físicos, desde que observados os requisitos gerais dos contratos e as garantias de identificação das partes.

A jurisprudência recente pacificou que não há hierarquia entre os diferentes tipos de assinatura eletrônica – todas são admitidas, apenas variando o peso probatório. Essa flexibilização, aliada às normas sobre títulos executivos digitais, confere estabilidade ao comércio eletrônico bancário, permitindo que acordos feitos por aplicativos ou internet tenham respaldo legal equivalente aos firmados no balcão da agência.

Resta examinar, no entanto, como se distribui a responsabilidade em eventuais fraudes nesses contratos e quais são os direitos dos consumidores lesados.

3 RESPONSABILIDADE CIVIL EM CASOS DE GOLPES DIGITAIS BANCÁRIOS

A expansão dos golpes digitais trouxe ao centro do debate jurídico a questão de quem responde pelos prejuízos causados por fraudes em operações bancárias eletrônicas, especialmente quando um contrato ou transação é realizado sem o consentimento real do cliente, mediante ardil de terceiros.

Nesse campo, aplica-se a principiologia do Direito do Consumidor: as instituições financeiras, ao oferecerem serviços aos clientes, assumem obrigações de segurança e são responsáveis pelos defeitos na prestação desses serviços.

O STJ consolidou, por meio da Súmula 479, 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"*. Em outros termos, se um cliente sofre um dano em razão de um golpe vinculado à sua conta ou contrato bancário, a princípio o banco responde independentemente de culpa ante o risco do empreendimento bancário (um *fortuito interno*, previsível dentro da atividade).

Essa orientação deriva diretamente do Código de Defesa do Consumidor (artigos. 6º, 14 e 17 do CDC) e da teoria do risco profissional: quem aufere lucro com o serviço (no caso, o banco) deve arcar com os riscos inerentes a ele, protegendo o consumidor, parte vulnerável na relação.

Situações típicas de fortuito interno incluem operações não reconhecidas (saques, transferências via internet banking por hackers), empréstimos contratados por falsários com documentos do cliente, clonagem de cartão com gastos indevidos, abertura de conta fantasma em nome de terceiro, entre outras.

A jurisprudência é firme em considerar que fraudes dessa natureza não rompem o nexo de causalidade entre o serviço bancário e o dano,

pois representam justamente o risco contra o qual o consumidor espera ser protegido pelo fornecedor do serviço.

Em apoio a essa posição, o STJ já destacava há décadas passadas, que furtos de talões, cheques falsificados ou contas abertas com documentos falsos eram eventos previsíveis no negócio bancário. Um banco diligente deveria implementar sistemas para prevenir ou ao menos rapidamente remediar esses incidentes, sob pena de responder por falha no dever de segurança.

Não se ignora que as instituições financeiras adotam medidas para reduzir fraudes, exigindo assinaturas eletrônicas, seja por meio de assinatura digital ou biometria facial, garantindo a proteção das informações e a manifestação de vontade do consumidor.

Contudo, o crescente aumento de demandas judiciais indica que apesar dos investimentos significativos na proteção dos sistemas digitais, a vulnerabilidade do próprio consumidor acaba por ser negligenciada. Não basta possuir um sistema robusto de segurança se o usuário continua exposto a invasões, fraudes e golpes.

É importante esclarecer, todavia, os limites da responsabilidade objetiva. O próprio Código de Defesa do Consumidor prevê que o fornecedor não será responsabilizado quando provar que o defeito no serviço decorreu de culpa exclusiva do consumidor ou de terceiro (art. 14, §3º, II).

Em termos bancários, isso significa que se o cliente agiu de forma totalmente imprudente ou intencionalmente contribuiu para o golpe, o banco poderá ficar isento de responsabilidade.

Verificam-se dois exemplos recentes e emblemáticos, ambos do Superior Tribunal de Justiça em 2025, ilustram os critérios:

Em outubro de 2025, a Terceira Turma do STJ (Rel. Min. Ricardo Villas Bôas Cueva) julgou o REsp 2.220.333/DF, que versa sobre o chamado golpe da "mão fantasma". O estelionatário, fingindo ser funcionário do banco, convenceu a cliente a instalar um aplicativo de acesso remoto supostamente para "regularizar" sua conta. Com isso, realizou um empréstimo de R$ 45 mil em nome da vítima e transferências em série, operações totalmente atípicas para o perfil da conta. Em primeira instância, o banco foi condenado a restituir todo o prejuízo; o TJDFT, porém, entendeu que houve culpa concorrente da vítima (reduzindo a indenização à metade) por ela ter instalado o app malicioso.

No entanto, o STJ reverteu essa decisão, afirmando que *não cabe atribuir culpa concorrente ao consumidor* em tais circunstâncias. O Ministro Cueva enfatizou que validar operações completamente fora do perfil do cliente constitui defeito do serviço bancário, o banco deveria ter sistemas para detectar e barrar movimentações suspeitas (como empréstimos e PIX em montante vultoso incompatíveis com o histórico).

Além disso, para haver culpa concorrente seria preciso que a vítima tivesse assumido conscientemente um risco. No caso, a cliente acreditou estar seguindo orientações do próprio banco para proteger sua conta, não podendo ser

considerada negligente a ponto de prever que sofreria um golpe.

Conclusão do STJ: a fraude ocorreu por falha de segurança da instituição financeira, logo esta deve arcar integralmente com os danos, sem redução. Esse julgado reforça que fraudes por engenharia social bem-sucedidas geralmente revelam uma vulnerabilidade do sistema (seja tecnológica, seja na comunicação com o cliente), e não mera culpa do usuário.

Poucas semanas depois, em dezembro de 2025, a Quarta Turma do STJ (Rel. Min. Antonio Carlos Ferreira) analisou outro golpe no AREsp 2.455.230, com desfecho inverso, conforme noticiado no portal Migalhas[41].

Nesse caso, a vítima recebeu uma ligação fraudulenta e, para cumprir as instruções dos golpistas, dirigiu-se presencialmente a um terminal de autoatendimento bancário, onde, usando sua biometria/senha, escaneou um código que liberou acesso remoto de terceiros à sua conta dentro da agência. Os criminosos então efetuaram empréstimos e diversas transferências via PIX. O TJDFT entendeu que o banco não teve falha, o sistema de segurança funcionou normalmente, sendo a própria correntista quem, embora iludida, quebrou todos os protocolos de segurança.

Ato contínuo, o STJ não conheceu do recurso, mantendo a decisão que afastou a responsabilidade do banco, sob o fundamento de culpa exclusiva da vítima (art. 14, §3º, II, CDC). No voto vista, o Min. Raul Araújo ressaltou que a consumidora cooperou ativamente com a fraude, deslocando-se até a agência e realizando procedimentos claramente irregulares sem buscar ajuda dos funcionários ali presentes.

Assim, tratou-se de conduta imprudente que *"quebrou todas as regras de segurança desenvolvidas pela instituição bancária"*. Nesse cenário extremo, entendeu-se configurado o fortuito externo (ato de terceiro somado à ação decisiva da vítima), rompendo o nexo causal com o serviço bancário.

Confrontando os dois casos, percebe-se que a linha divisória está na previsibilidade e evitabilidade do evento pelo banco versus a contribuição do cliente**.** No primeiro, a cliente agiu dentro do esperado (foi enganada remotamente), e o banco tinha meios de evitar o dano (monitoramento de transações atípicas) mas falhou; no segundo, a cliente tomou uma ação excepcional e inesperada (dar acesso na própria agência sem avisar ninguém), tornando difícil ao banco prevenir o ocorrido.

Em ambos os casos, os golpistas externos originaram a fraude, mas no primeiro isso é

[41]Disponível em: https://www.migalhas.com.br/quentes/446086/stj-ve-culpa-da-vitima-e-afasta-responsabilidade-de-banco-por-golpe <acessado em 11/12/2025>

considerado risco do negócio do banco (*fortuito interno*), e no segundo foi considerado causado por conduta estranha ao serviço (*fortuito externo* pela colaboração inadvertida da vítima).

De modo geral, a jurisprudência do STJ mantém a proteção ampla do consumidor em golpes digitais, aplicando a responsabilidade objetiva da instituição financeira. A eventual imprudência da vítima só exclui a responsabilidade bancária quando for suficiente para ser causa única do dano, isto é, quando o cliente ignorou totalmente os alertas básicos de segurança e agiu de forma altamente atípica. Fora dessas situações extremas, os tribunais tipicamente concluem que as fraudes estão vinculadas a alguma deficiência prevenível no serviço bancário (por exemplo, falta de travas antifraude, de dupla checagem por parte do banco, ou insuficiência de alerta educativo).

Ademais, mesmo quando não há falha sistêmica, argumenta-se que o dever de cuidado do banco inclui instruir claramente seus clientes e adotar medidas para minimizar danos quando detectada uma fraude.

Por exemplo, destaca-se hoje a obrigação dos bancos implementarem o Mecanismo Especial de Devolução (MED) do PIX, criado pelo Banco Central, que permite congelar e restituir valores transferidos em fraude, se comunicado em tempo. Se o consumidor notifica imediatamente a ocorrência de um golpe e, ainda assim, o banco deixa de acionar o MED para tentar recuperar o dinheiro, tal omissão configura falha na prestação do serviço.

Outro fator relevante nas decisões é verificar se o banco disponibilizou informações e proteção compatíveis com a vulnerabilidade do cliente. Golpes contra idosos ou pessoas com menor familiaridade tecnológica podem ensejar um escrutínio maior da conduta do banco.

A vulnerabilidade agravada do consumidor pode levar o Judiciário a entender que cabia ao banco diligências adicionais. Em certos casos envolvendo aposentados enganados em "empréstimos consignados" não solicitados, por exemplo, tribunais têm reconhecido vício de consentimento e anulação do contrato, com restituição em dobro de parcelas descontadas indevidamente.

Nessas hipóteses, ainda que o banco argumente ter um contrato eletrônico com assinatura ou áudio de confirmação, muitos juízos estão considerando a possibilidade de fraude (como intermediários de má-fé que induzem contratações) e colocando sobre o banco o ônus de provar que o consumidor anuiu de forma consciente, ônus do qual nem sempre a instituição financeira se desincumbe.

A mensagem central é que é atribuído aos bancos o dever legal de proteger seus clientes contra golpes digitais. A relação de consumo impõe um patamar elevado de cuidado na prestação do serviço financeiro.

Há a possibilidade de regresso em face do verdadeiro criminoso, caso identificado. E essa responsabilização supostamente incentiva o aprimoramento das políticas de segurança da

informação, filtros de operações suspeitas e campanhas educativas.

4 PROVAS DIGITAIS E SEGURANÇA JURÍDICA NOS LITÍGIOS

Diante do aumento das disputas envolvendo contratos eletrônicos e operações on-line, a admissibilidade e valoração das provas digitais tornou-se questão crucial para assegurar a segurança jurídica.

Felizmente, o ordenamento jurídico brasileiro evoluiu para acomodar com naturalidade os documentos eletrônicos como meios de prova, equiparando-os às evidências tradicionais, desde que respeitados certos parâmetros de integridade e autenticidade.

O Código de Processo Civil de 2015 já veio adequado a essa realidade. Além do mencionado art. 441 (que reconhece documentos eletrônicos na forma da lei), o art. 422, parágrafo único, estabelece que os documentos produzidos eletronicamente e juntados aos autos gozam de autenticidade presumida quando a autoria e integridade forem certificadas conforme legislação específica.

A já citada MP 2.200-2/2001 e a infraestrutura ICP-Brasil são exemplos dessa legislação. Um documento assinado digitalmente com certificado válido tem a mesma força probante de um original em papel assinado à mão. Mas, como vimos, a falta de certificado não elimina a prova, apenas tira a presunção legal automática, exigindo verificação caso a caso.

Nesse sentido, dois dispositivos do CPC merecem destaque: O art. 411, I, que prevê presunção de autenticidade do documento particular se a parte contra quem foi produzido não o impugnar. Isso vale para documentos físicos e eletrônicos. O ônus da impugnação específica é, portanto, do litigante que quer desqualificar a prova digital.

Já o art. 411, III, merece atenção eis que atribui presunção de integridade aos documentos resultantes de registros eletrônicos feitos de acordo com as leis específicas.

No caso do REsp 2.150.278/PR citado, o STJ enfatizou que cabe à parte que nega o documento impugnar sua veracidade, seja quanto à autoria da assinatura, seja quanto à integridade do conteúdo. Ao fazê-lo, deve apresentar indícios ou argumentos mínimos (por exemplo, alegar falsidade do certificado, ou fraude na geração do documento).

Em contrapartida, quando a parte questiona a autenticidade do contrato eletrônico, os tribunais investigam os elementos de segurança apresentados. Exemplo: se um consumidor nega ter feito um empréstimo e afirma que seus documentos foram usados por terceiros, o banco precisa demonstrar a regularidade da contratação.

Normalmente refutada a suposta prova se trazendo apenas arquivo com suposta assinatura digital simples (imagem colada, sem nenhuma validação).

Cada concreto deve ser apreciado, com as provas trazidas, verificando-se a verossimilhança das alegações e a distribuição do ônus da prova[42].

A Ministra Nancy Andrighi, no julgamento do REsp 2.150.278, afirmou que a *força probatória de seus contratos digitais* está diretamente ligada a adoção de múltiplos fatores de autenticação e registro no momento da contratação. A autenticidade (certeza de quem assinou) depende do número e natureza dos fatores de autenticação empregados – login/senha, OTP por SMS, biometria, etc – e a integridade (certeza de que o documento não foi alterado) é garantida por algoritmos de *hash* criptográfico (como SHA-256) associados ao documento.

Essa explicação técnica do STJ serve como guia: quanto mais robustos os métodos usados no contrato eletrônico, maior sua credibilidade.

Por fim, cabe mencionar que a segurança jurídica também está vinculada ao respeito a normas correlatas, como a LGPD. Os bancos, ao armazenar dados biométricos ou pessoais para fins contratuais, devem fazê-lo com rigor. Uma eventual violação de dados poderia não apenas sujeitá-los a sanções administrativas, mas fragilizar a prova.

Portanto, proteção de dados e segurança jurídica caminham juntas: contratos eletrônicos confiáveis dependem de manejo adequado das informações do cliente. Nesse prisma, a LGPD também reforça a ideia de que o cliente deve ser informado de forma clara sobre o uso de seus dados e das condições do contrato, sob pena de o consentimento ser questionado.

Com tais considerações, os meios de prova digitais em disputas de golpes bancários têm se mostrado aptos a resolver a maioria dos casos, desde que bem apresentados. O CPC fornece as ferramentas (presunções legais, possibilidade de produção de provas técnicas) e a jurisprudência tem sido pragmática, aceitando a inovação tecnológica sem prejuízo do direito das partes de discutir a veracidade.

Isso garante a segurança jurídica, pois, tanto o consumidor pode provar que foi vítima de fraude (com registros e testemunhos, por exemplo), quanto o banco pode demonstrar que cumpriu seu dever, exibindo logs e assinaturas colhidas.

O desafio permanente é acompanhar a evolução dos golpes, já se discute como avaliar um contrato firmado via reconhecimento facial, considerando os riscos de deepfake[43].

---

[42] TJ-PR 00471972920248160182 Curitiba, Relator.: Fernanda Bernert Michielin, Data de Julgamento: 29/07/2025, 2ª Turma Recursal, Data de Publicação: 30/07/2025 e TJ-PR 00342417820248160182 Curitiba, Relator.: Adriana de Lourdes Simette, Data de Julgamento: 11/08/2025, 3ª Turma Recursal, Data de Publicação: 12/08/2025.

[43] Deepfake é uma técnica que permite alterar um vídeo ou foto com ajuda de inteligência artificial (IA). Com ele, por exemplo, o rosto da pessoa que está em cena pode ser trocado pelo de outra; ou aquilo que a pessoa fala pode ser modificado. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/02/28/o-que-e-deepfake-e-como-ele-e-usado-para-distorcer-realidade.ghtml <Acessado em 11/12/2025).

Cumpre as instituições, governos e indivíduos, adaptar-se as regras tradicionais de prova aos novos formatos, mantendo os princípios de igualdade de armas e busca da verdade real no processo.

CONSIDERAÇÕES FINAIS

Viu-se que a era digital trouxe inúmeros benefícios, mas também uma metamorfose aos crimes, em exponencial crescimento dos golpes digitais, acarretando em impacto econômico, medo, insegurança, entre outros.

Muitas são as atitudes e estratégias que podem ser adotadas para a reprimir e evitar a tais crimes. Medidas necessárias, eis que a evolução tecnológica, os contratos digitais e as relações virtuais só irão evoluir.

O combate ao crime cibernético e as fraudes digitais deve fazer parte dos investimentos e das políticas públicas, eis que há uma insegurança da população, abalo a ordem pública. A segurança pública é dever do Estado e hoje ela se mostra necessária em diferentes vertentes.

Necessários constantes avanços, estudos e atualização da legislação e das ferramentas de investigação. Também o poder judiciário deve se atualizar de acordo com as novas demandas e dinâmicas.

É fundamental reconhecer que a mitigação dos golpes digitais em contratos bancários passa por estratégias de prevenção e educação, evitando-se a ocorrência do golpe.

Por isso, órgãos públicos, entidades regulatórias e os próprios bancos têm investido em campanhas de conscientização e melhorias procedimentais, visando aumentar a segurança do ambiente contratual eletrônico.

Em outubro de 2025, a Agência Nacional de Telecomunicações (Anatel) promoveu a campanha #OutubroCiberSeguro[44], reunindo especialistas em combate a fraudes digitais para divulgar boas práticas e alertas à população.

Destacou-se a necessidade de especial atenção a grupos particularmente vulneráveis: crianças, adolescentes e idosos.

Crianças e adolescentes, já inseridos no mundo digital, podem ser alvo de golpes em jogos on-line ou redes sociais, muitas vezes sem discernimento para identificar um perigo.

Idosos, por sua vez, estão cada vez mais conectados (especialmente após a pandemia, muitos aderiram ao banco virtual e aplicativos), porém tendem a confiar mais em autoridades aparentes e podem não ter a vivência tecnológica para suspeitar de um contato falso.

Por isso, recomendou-se supervisão familiar, educação digital preventiva e uma dose saudável

[44] Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/delegado-fala-sobre-os-golpes-mais-comuns-desafios-no-combate-e-a-importancia-da-conscientizacao-digital <Acessado em 11/12/2025>

de desconfiança diante de contatos ou ofertas inesperadas. Ou seja, famílias e comunidades devem orientar seus membros mais suscetíveis sobre como reagir a mensagens suspeitas, nunca compartilhar senhas ou códigos, e sempre confirmar informações pelos canais oficiais.

Os especialistas também ressaltam a sofisticação das quadrilhas digitais. Muitas vezes, os golpistas atuam em rede organizada, com divisão de tarefas: alguns obtêm dados vazados na internet, outros entram em contato telefonicamente encenando um script, outros são responsáveis por movimentar os recursos ilícitos rapidamente para contas "laranja" ou criptoativos, dificultando o rastreamento. Essa "indústria" do crime cibernético demanda resposta igualmente coordenada.

Assim, defende-se uma integração ágil entre polícias, instituições financeiras e órgãos reguladores. Por exemplo, criar centrais de atendimento conjuntas em que, ao noticiar um golpe, o consumidor aciona não só o banco, mas uma rede que englobe as autoridades, aumentando a chance de bloqueio imediato de valores e eventual investigação do destino do dinheiro.

É cediço que os bancos têm investido em soluções antifraude avançadas, utilizando inteligência artificial para monitorar transações e identificar padrões suspeitos em tempo real.

Sistemas especializados detectam sinais de engenharia social, como mudanças abruptas no uso do aplicativo, indicando possível coação. Além disso, protocolos como autenticação em dois fatores e limites para operações sensíveis, incluindo restrições de PIX noturno, são medidas já adotadas para reduzir riscos.

Apesar da tecnologia, a atuação humana continua essencial. Desta forma, é essencial que em âmbito corporativo haja contínuo treinamento de colaboradores para reconhecer sinais de fraude e intervir quando necessário, evitando golpes em situações presenciais.

No ambiente digital, aplicativos passaram a incluir alertas contextuais, como avisos sobre códigos de verificação, para conscientizar clientes e impedir que compartilhem informações sensíveis. Essas ações simples podem evitar prejuízos significativos.

As recomendações tradicionais permanecem fundamentais: não compartilhar senhas ou códigos, ativar verificação em duas etapas, desconfiar de mensagens urgentes, manter dispositivos protegidos e evitar links suspeitos. Tais cuidados básicos são apontados por especialistas como a melhor defesa contra crimes cibernéticos, pois a prevenção reduz a necessidade de buscar ressarcimento após um golpe, poupando transtornos e perdas financeiras.

A proteção contra fraudes também depende da colaboração entre órgãos reguladores, bancos e entidades de defesa do consumidor.

Paralelamente, a legislação brasileira garante validade aos contratos eletrônicos e responsabiliza os bancos quando falham na prevenção. Com tecnologia robusta, boas práticas e evolução normativa, espera-se

consolidar a segurança jurídica nas transações digitais, equilibrando eficiência e proteção ao consumidor.

Por fim, a educação digital deve fazer parte das instituições de ensino, desde os tenros anos, preparando os estudantes para as constantes transformações. Conscientizam-se os riscos no ambiente virtual, mas também se deve lecionar sobre aspectos éticos e de cidadania, fortalecendo o senso crítico e a responsabilidade no uso das tecnologias. O reconhecimento dos golpes, das atitudes não aceitáveis, do respeito a privacidade alheia e de própria proteção, desde senhas, valores, dados, e a própria intimidade e imagem.

Família, escolas e organizações têm papel fundamental na construção de uma cultura de segurança digital, pois os delitos virtuais frequentemente exploram vulnerabilidades humanas, como a falta de informação e o comportamento imprudente online.

REFERÊNCIAS BIBLIOGRÁFICAS

COELHO, Fábio Ulhoa. *Curso de direito comercial*. V. 3. São Paulo: Saraiva, 2012. E-book. p. 64.

TJPR – Processo: 0047197-29.2024.8.16.0182, **Curitiba**. Relatora: Fernanda Bernert Michielin. Julgado em 29 jul. 2025 (2ª Turma Recursal). Publicado em 30 jul. 2025.

TJPR – Processo n.º 0034241-78.2024.8.16.0182, **Curitiba**. Relatora: Adriana de Lourdes Simette. Julgado em 11 ago. 2025 (3ª Turma Recursal). Publicado em 12 ago. 2025.

G1. *O que é deepfake e como ele é usado para distorcer realidade*. 28 fev. 2024. Disponível em: <https://g1.globo.com/tecnologia/noticia/2024/02/28/o-que-e-deepfake-e-como-ele-e-usado-para-distorcer-realidade.ghtml>. Acesso em: 11 dez. 2025.

BRASIL. **Agência Nacional de Telecomunicações (Anatel)**. *Delegado fala sobre os golpes mais comuns, desafios no combate e a importância da conscientização digital*. Brasília, 22 out. 2025. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/delegado-fala-sobre-os-golpes-mais-comuns-desafios-no-combate-e-a-importancia-da-conscientizacao-digital>. Acesso em: 11 dez. 2025.

LACERDA, Schumacher Oliveira de; AGUIAR, Vera Mônica Queiroz Fernandes. *O aumento de crimes cibernéticos na era digital e os desafios legais*. **Revista FT**, v. 29, n. 146, maio 2025. Disponível em: <https://revistaft.com.br/o-aumento-de-crimes-ciberneticos-na-era-digital-e-os-desafios-legais/>. Acesso em: 14 dez. 2025.

AGÊNCIA SENADO. *Golpes digitais atingem 24% da população brasileira, revela DataSenado*. 01 out. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado>. Acesso em: 01 dez. 2025.

ASSOCIAÇÃO DE DEFESA DE DADOS PESSOAIS E DO CONSUMIDOR (ADDP). *Golpes on-line tiveram alta significativa em 2024*. 30 dez. 2024. Disponível em: <https://addp.com.br/addp/golpes-on-line-tiveram-alta-significativa-em-2024/>. Acesso em: 01 dez. 2025.

GARCIA, Rafael. *Golpes virtuais crescem no Brasil, enquanto roubos "presenciais" diminuem*. **O Globo**, São Paulo, 18 jul. 2024. Disponível em: <https://oglobo.globo.com/brasil/noticia/2024/07/18/golpes-virtuais-crescem-no-brasil-enquanto-roubos-presenciais-diminuem.ghtml>. Acesso em: 14 dez. 2025.

FEDERAÇÃO BRASILEIRA DE BANCOS (Febraban). *Saiba quais foram os 10 golpes mais aplicados contra clientes bancários em 2024*. 14

abr. 2025. Disponível em: <https://portal.febraban.org.br/noticia/4279/pt-br/>. Acesso em: 01 dez. 2025.

FERRARI, Douglas Angelo; LIMA, Marcianita Lopata de; FERRARI, Flávia Jeanne. *Fraudes digitais e segurança pública: a atuação integrada entre juizados especiais, Ministério Público e Polícia Militar*. **Revista Jurídica Gralha Azul**, v. 1, n. 32, out./nov. 2025. Disponível em: <https://revista.tjpr.jus.br/gralhaazul/article/view/315>. Acesso em: 11 dez. 2025.

MIGALHAS. *STJ reconhece culpa da vítima e afasta responsabilidade de banco por golpe*. 09 dez. 2025. Disponível em: <https://www.migalhas.com.br/quentes/446086/stj-ve-culpa-da-vitima-e-afasta-responsabilidade-de-banco-por-golpe>. Acesso em: 11 dez. 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Justiça em Números – Painel de Estatísticas do Poder Judiciário*. Disponível em: <https://justica-em-numeros.cnj.jus.br/painel-estatisticas/>. Acesso em: 01 dez. 2025.