Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

Fraudes na abertura de contas digitais e assinatura biométrica facial: responsabilidade civil bancária à luz da Súmula 479 do STJ

Fraud in the opening of digital accounts and facial biometric signature: banking civil liability in light of Precedent 479 of the STJ

Luccas Matheus Marinho Varela[1] e Anna Emanuella Nelson dos Santos Cavalcanti da Rocha[2]

v. 14/ n. 2 (2026)
Abril/Junho

Aceito para publicação em 26/05/2026.

[1]Graduando em Direito pela Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte. ORCID: 0009-0008-1795-4085. E-mail: luccasvmarinho@gmail.com;
[2]Doutora em Direito Constitucional pela Universidade de Fortaleza, Fortaleza, Ceará. ORCID: 0000-0002-7515-7884. E-mail: manusantos@uol.com.br.

https://www.gvaa.com.br/revista/index.php/RDG

RESUMO: O presente artigo analisa se a mera apresentação de assinatura biométrica facial é suficiente para afastar a responsabilidade civil da instituição financeira pela abertura fraudulenta de conta digital, ou se esse risco deve ser compreendido como fortuito interno inerente ao modelo de contratação bancária massificada. A pesquisa adota abordagem qualitativa com método dedutivo, combinando revisão bibliográfica, análise normativa e exame jurisprudencial selecionado. O estudo examina os deveres regulatórios impostos às instituições financeiras pela Resolução CMN nº 4.753/2019 e pela Resolução BCB nº 343/2023 quanto à identificação segura, à rastreabilidade e à integridade dos procedimentos de autenticação, além das vulnerabilidades técnicas conhecidas dos mecanismos de autenticação facial, documentadas concretamente pela Operação Face Off, deflagrada pela Polícia Federal em maio de 2025. A responsabilidade civil bancária é analisada à luz do Código de Defesa do Consumidor, da teoria do risco do empreendimento e das Súmulas 297 e 479 do Superior Tribunal de Justiça. A análise jurisprudencial demonstra que tribunais têm recusado a selfie isolada como prova conclusiva da contratação digital quando ausentes elementos técnicos mínimos, como logs, trilha de auditoria, prova de vivacidade e registros de integridade, ou quando presentes incongruências que indicam fraude, como incompatibilidade de geolocalização. Conclui-se que a biometria facial pode constituir meio legítimo de autenticação, mas seu efeito liberatório depende da demonstração concreta, por registros técnicos auditáveis, da integridade, da autenticidade e da rastreabilidade do procedimento adotado. Ausente essa demonstração, a fraude configura fortuito interno, atraindo a responsabilidade objetiva da instituição financeira e seu consequente dever de indenizar.
Palavras-chave: abertura de conta digital; biometria facial; responsabilidade civil bancária; fortuito interno; Súmula 479 do STJ; Código de Defesa do Consumidor.

ABSTRACT: This article examines whether the mere presentation of facial biometric authentication is sufficient to exempt a financial institution from civil liability for the fraudulent opening of a digital bank account, or whether such risk should be classified as an internal fortuity inherent to the model of mass digital banking contracting. The research adopts a qualitative approach based on the deductive method, combining bibliographical review, regulatory analysis, and selected case law examination. The study analyzes the regulatory duties imposed on financial institutions by CMN Resolution No. 4,753/2019 and BCB Resolution No. 343/2023 regarding secure identification, traceability, and the integrity of authentication procedures, as well as the known technical vulnerabilities of facial authentication mechanisms, concretely evidenced by Operation Face Off, launched by the Brazilian Federal Police in May 2025. Bank civil liability is examined in light of the Brazilian Consumer Protection Code, the enterprise risk theory, and Precedents Nos. 297 and 479 of the Superior Court of Justice (STJ). The case law analysis demonstrates that courts have rejected a standalone selfie as conclusive evidence of digital contracting when minimum technical elements are absent, such as logs, audit trails, liveness detection evidence, and integrity records, or when inconsistencies indicative of fraud are present,

such as geolocation incompatibility. The study concludes that facial biometrics may constitute a legitimate means of authentication; however, its exculpatory effect depends on the concrete demonstration, through auditable technical records, of the integrity, authenticity, and traceability of the adopted procedure. In the absence of such demonstration, the fraud constitutes an internal fortuity, giving rise to the strict liability of the financial institution and its corresponding duty to compensate the victim.
Keywords: digital bank account opening; facial biometrics; bank civil liability; internal fortuity; STJ Precedent No. 479; Brazilian Consumer Protection Code.

1 CONSIDERAÇÕES INICIAIS

A atividade bancária brasileira passou, nos últimos anos, por intenso processo de digitalização. Serviços que antes dependiam de atendimento presencial, conferência física de documentos e assinatura manuscrita passaram a ser realizados por aplicativos, plataformas digitais e mecanismos remotos de autenticação. Nesse cenário, a abertura de contas digitais tornou-se prática ordinária do mercado financeiro, acompanhada do uso crescente de tecnologias de identificação, como a captura de selfie e a chamada assinatura biométrica facial. Dados da FEBRABAN indicam que 82% das transações bancárias dos brasileiros já são realizadas por canais digitais, especialmente pelo celular e pelo internet banking (Febraban, 2025). Bruno Miragem observa que os contratos bancários e financeiros viabilizam o acesso ao crédito, aos meios automatizados de pagamento e à própria participação econômica no mercado (Miragem, 2019, p. 403), destacando ainda que a atividade bancária contemporânea é marcada pela desmaterialização do dinheiro, pela automação e pelo uso massivo da tecnologia da informação, fatores que aumentam a complexidade dos serviços prestados e, consequentemente, os riscos de falhas (Miragem, 2019, p. 404).

A contratação remota, embora lícita e socialmente relevante, desloca para o ambiente digital etapas antes realizadas presencialmente, identificação do cliente, validação documental e confirmação da vontade contratual, submetendo toda a cadeia de fornecimento bancário a deveres de segurança, controle e rastreabilidade. A Resolução CMN nº 4.753/2019 determina que as instituições financeiras adotem procedimentos capazes de verificar e validar a identidade e a qualificação dos titulares, bem como a autenticidade das informações fornecidas, inclusive mediante confronto com bases públicas ou privadas (Brasil, 2019). A abertura digital de conta, portanto, não se resume ao recebimento de uma imagem ou à aprovação automatizada de cadastro.

O problema surge quando contas digitais são abertas fraudulentamente em nome de terceiros, mediante uso indevido de dados pessoais, documentos falsificados ou burla de mecanismos de validação facial. Nessas situações, é comum que a instituição financeira busque afastar sua responsabilidade pela simples apresentação de selfie ou relatório interno de autenticação biométrica. Todavia, a existência de uma imagem facial vinculada ao cadastro não demonstra, por si só, manifestação válida de vontade, nem comprova a integridade e a rastreabilidade do procedimento

adotado. A Operação Face Off, deflagrada pela Polícia Federal, evidenciou esse risco ao apontar associação criminosa especializada em fraudar contas digitais vinculadas à plataforma GOV.BR mediante técnicas avançadas de alteração facial para burlar sistemas de autenticação biométrica demonstrando que a fraude biométrica não é hipótese remota, mas risco concreto no ambiente de identificação digital.

Diante desse cenário, formula-se o seguinte problema de pesquisa: a mera apresentação de assinatura biométrica facial é suficiente para afastar a responsabilidade do banco pela abertura fraudulenta de conta digital, ou esse risco deve ser compreendido como fortuito interno inerente ao modelo de contratação bancária massificada, especialmente quando ausente demonstração técnica da integridade e da rastreabilidade do procedimento adotado?

O objetivo do estudo é analisar se, à luz do Código de Defesa do Consumidor, da teoria do risco do empreendimento e da Súmula 479 do STJ, a abertura fraudulenta de contas digitais mediante utilização de assinatura biométrica facial deve ser tratada como fortuito interno quando a instituição financeira não comprova, por registros técnicos verificáveis, a regularidade do procedimento de autenticação. A hipótese sustentada é a de que a biometria facial, inserida em processo massificado de contratação bancária digital, integra o risco próprio da atividade econômica explorada pelo banco, de modo que a fraude somente poderia afastar a responsabilidade da instituição quando demonstrada, de forma técnica e robusta, a regularidade do procedimento.

Para desenvolver essa tese, o artigo adota abordagem qualitativa com método dedutivo, partindo do regime geral de proteção do consumidor e da responsabilidade civil bancária para examinar, em concreto, a suficiência probatória da biometria facial em contratações contestadas. A pesquisa combina revisão bibliográfica de direito do consumidor, responsabilidade civil e assimetria técnica; análise documental de normas do Banco Central e do CMN; e exame jurisprudencial selecionado e instrumental, voltado a identificar como os tribunais têm tratado a selfie isolada como prova de contratação bancária digital. Na sequência, o artigo examina o processo de digitalização bancária e seus efeitos jurídicos, os deveres regulatórios de identificação segura, as vulnerabilidades técnicas da autenticação facial, o regime de responsabilidade civil bancária e, por fim, a suficiência probatória da biometria facial à luz da jurisprudência e da regulação aplicável.

2 DIGITALIZAÇÃO BANCÁRIA, MASSIFICAÇÃO CONTRATUAL E NOVOS RISCOS DE FRAUDE:

A digitalização bancária representa uma mudança estrutural na forma de prestação dos serviços financeiros. A relação entre consumidor e instituição financeira, antes fortemente vinculada

à agência física, à conferência presencial de documentos e à assinatura física, passou a ser progressivamente mediada por aplicativos, internet banking, canais remotos e sistemas automatizados de autenticação. Essa transformação decorre de escolha empresarial orientada por ganhos de escala, redução de custos operacionais, ampliação da base de clientes e maior velocidade na contratação de produtos e serviços financeiros. Farias e Rosenvald observam que a migração das relações entre clientes e bancos do ambiente físico para o digital é conveniente aos consumidores, mas também, e sobretudo, às instituições financeiras, por permitir a otimização de lucros e a redução de custos, razão pela qual cabe aos bancos o ônus da rastreabilidade das operações realizadas nesse ambiente, especialmente por meio de logs e registros técnicos verificáveis (Farias; Rosenvald, 2019, p. 1940).

A intensidade dessa mudança é demonstrada pelos dados do setor. Segundo a FEBRABAN, em 2024, 82% das transações bancárias dos brasileiros foram realizadas por canais digitais, dentro de um universo de 208,2 bilhões de transações, com o mobile banking concentrando 75% das operações e crescimento de 15% em relação ao ano anterior (FEBRABAN, 2025). Entre junho de 2018 e dezembro de 2023, o número de usuários ativos no Sistema Financeiro Nacional cresceu 103,2%, com as pessoas físicas passando de 77,2 milhões para 152 milhões de usuários ativos (Banco Central do Brasil, 2023a). O Banco Central identifica as chamadas entidades digitais como aquelas que utilizam plataformas digitais, prestam atendimento preponderantemente remoto e fazem uso intensivo de tecnologia na interação com o público (Banco Central do Brasil, 2022), e sua expansão evidencia que a digitalização não apenas alterou o canal de atendimento, mas ampliou significativamente a quantidade de vínculos financeiros formados e mantidos por meios remotos.

Essa massificação produz efeitos jurídicos relevantes. A contratação bancária digital substitui etapas presenciais por fluxos padronizados de cadastro, envio de documentos, validação de dados, captura de imagem facial e decisões automatizadas. A eficiência do modelo está justamente na possibilidade de replicar o mesmo procedimento para milhões de usuários com mínima intervenção humana, contudo, quanto maior a escala da contratação remota, maior também a importância dos mecanismos de controle, rastreabilidade e prevenção de fraudes. Os riscos associados a esse modelo são reconhecidos em documentos regulatórios: conforme o AIR do Voto nº 84/2023-BCB, o crescimento dos meios digitais para realização de transações financeiras vem sendo acompanhado pela ocorrência de fraudes, golpes e crimes cibernéticos, registrando-se crescimento de 165% nos golpes de engenharia social em relação ao primeiro semestre de 2021 (Banco Central do Brasil, 2023b).

Portanto, a digitalização bancária não é juridicamente neutra. Se a instituição financeira se beneficia da escala, da redução de custos e da velocidade dos canais digitais, a abertura remota de contas não pode ser tratada como simples comodidade tecnológica dissociada de deveres de controle

e documentação. A fraude na abertura de contas digitais deve ser analisada à luz do ambiente de identificação, autenticação e contratação estruturado pela própria instituição, especialmente quando a controvérsia envolve a ausência de registros técnicos capazes de demonstrar a integridade e a rastreabilidade do procedimento adotado.

Portanto, a digitalização bancária não é juridicamente neutra. Se a instituição financeira se beneficia da escala, da redução de custos e da velocidade dos canais digitais, a abertura remota de contas não pode ser tratada como simples comodidade tecnológica dissociada de deveres de controle e documentação. A fraude na abertura de contas digitais, nesse sentido, deve ser analisada à luz do ambiente de identificação, autenticação e contratação estruturado pela própria instituição, especialmente quando a controvérsia envolve a ausência de registros técnicos capazes de demonstrar a integridade e a rastreabilidade do procedimento adotado.

3 ABERTURA DIGITAL DE CONTAS E DEVER REGULATÓRIO DE IDENTIFICAÇÃO SEGURA:

A abertura digital de contas bancárias é juridicamente admitida no ordenamento regulatório brasileiro, mas essa autorização não significa liberdade irrestrita para a criação automática de vínculos bancários. A regulamentação do Conselho Monetário Nacional parte da premissa de que a abertura de conta, ainda que realizada por meio eletrônico, deve ser acompanhada de procedimentos capazes de identificar o proponente, validar suas informações e preservar a segurança dos documentos utilizados. Nesse sentido, as normas expedidas pelo Banco Central e pelo CMN não atuam como simples recomendações administrativas, mas como parâmetros objetivos de conformação da atividade financeira digital.

A Resolução CMN nº 4.753/2019 estabelece os requisitos para abertura, manutenção e encerramento de contas de depósito. Em seu art. 2º, determina que as instituições financeiras devem adotar procedimentos e controles que permitam verificar e validar a identidade e a qualificação dos titulares, bem como a autenticidade das informações fornecidas, inclusive mediante confronto com bases de dados públicas ou privadas (Brasil, 2019). O art. 3º admite a abertura por qualquer canal de atendimento, inclusive por meios eletrônicos, e essa definição é relevante: a ausência de contato físico não autoriza a redução da segurança do procedimento, mas exige que a instituição estruture controles digitais equivalentes ou superiores, compatíveis com o risco próprio da contratação remota. O art. 7º, por sua vez, determina que as instituições assegurem a integridade, a autenticidade e a confidencialidade das informações e documentos eletrônicos, bem como a proteção contra acesso, uso, alteração, reprodução e destruição não autorizados (Brasil, 2019). Já o art. 8º exige que os

critérios de identificação e os procedimentos de controle adotados sejam formalizados em documento específico, mantido atualizado e à disposição do Banco Central (Brasil, 2019). Tais exigências evidenciam que os controles de abertura de conta devem ser previamente estruturados, documentados e auditáveis, não se trata de liberalidade operacional, mas de dever regulatório incorporado ao próprio modo de prestação do serviço bancário digital.

Esse padrão de exigência não é recente. A Resolução CMN nº 4.480/2016, que disciplinava a abertura de contas por meio eletrônico antes de sua revogação pela Resolução nº 4.753/2019, já exigia que os procedimentos e tecnologias empregados assegurassem integridade, autenticidade, confidencialidade, cópia de segurança, rastreamento e auditoria, com manutenção dos registros à disposição do Banco Central pelo prazo mínimo de cinco anos (Brasil, 2016). A continuidade dessa preocupação regulatória demonstra que a auditabilidade da abertura digital de contas não é exigência nova nem acidental, mas elemento estrutural da segurança esperada em procedimentos remotos de identificação e vinculação bancária.

O estudo das normativas expedidas pelo Banco Central deve ser compreendido como um *standard* da segurança legitimamente esperada do serviço bancário, e não como instrumento de aferição de negligência ou imperícia da instituição financeira. A análise do cumprimento regulatório, portanto, não importa retorno à responsabilidade subjetiva, pois não se investiga a culpa do banco, mas o padrão objetivo de segurança que deve permear a prestação do serviço financeiro em ambiente digital **(Cesa, 2025, p. 60).**

Nessa mesma linha, o mero cumprimento formal das normativas não possui efeito exoneratório automático. É necessário verificar, no caso concreto, se houve quebra do dever de segurança e se está presente alguma excludente de causalidade juridicamente idônea **(Cesa, 2025, p. 61).** Aplicado à abertura digital de contas, isso significa que a instituição não se libera apenas afirmando possuir procedimento de biometria, fluxo cadastral automatizado ou política interna de validação, deve demonstrar que tais mecanismos efetivamente asseguraram, naquele caso específico, a identificação segura do titular e a integridade do procedimento.

Dessa forma, quando a instituição financeira invoca a existência biometria facial para justificar a abertura de conta contestada, deve demonstrar não apenas a existência de uma imagem, selfie ou relatório sistêmico, mas a regularidade técnica do procedimento que capturou, validou, armazenou e vinculou aquele dado biométrico ao cadastro. Se a própria regulação exige autenticidade, integridade, proteção contra manipulação, formalização de controles, rastreamento e auditabilidade, a prova da contratação digital deve refletir esses mesmos critérios. O dever regulatório de identificação segura exerce, assim, dupla função: confirma que a abertura digital de contas é juridicamente admitida e socialmente útil; e evidencia que tais contratações devem ser acompanhadas

de controles técnicos adequados capazes de garantir a segurança de todos aqueles utilizam e são afetados por elas, servindo de ponte entre a regulação bancária e a responsabilidade civil.

4 BIOMETRIA FACIAL, ASSINATURA ELETRÔNICA E VULNERABILIDADES CONHECIDAS:

A expressão "assinatura biométrica facial" deve ser utilizada com cautela, pois pode abranger realidades técnicas distintas. Em sentido amplo, a biometria corresponde ao reconhecimento automatizado de uma pessoa a partir de características físicas ou comportamentais, sendo as imagens e características faciais exemplos de dados biométricos (Estados Unidos, 2026a). Para fins deste estudo, a biometria facial pode ser compreendida como modalidade de identificação ou verificação de identidade baseada em características da face, submetidas a processamento automatizado.

Essa definição, contudo, não permite concluir que qualquer selfie equivale a uma autenticação biométrica segura. A selfie é apenas uma imagem facial; a autenticação biométrica pressupõe um procedimento técnico mais amplo, que envolve captura, comparação, validação e registro. Entre a simples fotografia anexada a um cadastro e um fluxo biométrico robusto há diferença relevante: a primeira apenas demonstra a existência de uma imagem; o segundo pode demonstrar, se adequadamente documentado, que houve procedimento controlado de identificação ou verificação da identidade do usuário. Por isso, quando a instituição financeira afirma que houve "assinatura biométrica facial", é necessário identificar o que efetivamente foi realizado, se apenas a captura de uma selfie, uma comparação facial com determinada base de dados, um procedimento com prova de vivacidade ou um fluxo completo acompanhado de logs, metadados, hash, IP, geolocalização, identificação do dispositivo e trilha de auditoria.

A prova de vivacidade, também chamada de *liveness detection*, é o mecanismo pelo qual o sistema biométrico verifica se a imagem capturada corresponde a uma pessoa real, presente fisicamente no momento da autenticação e não a uma fotografia impressa, a um vídeo exibido na tela de outro dispositivo, a uma máscara ou a qualquer outro artifício utilizado para enganar a câmera. Em termos simples, o sistema tenta distinguir um rosto vivo de uma simulação desse rosto.

Essa distinção é necessária porque, sem ela, bastaria ao fraudador fotografar o documento de identidade da vítima, capturar uma imagem de seu rosto nas redes sociais ou utilizar um vídeo para tentar se passar por ela perante o sistema de autenticação. As tentativas de burlar o reconhecimento facial por meio desses recursos são chamadas, na literatura técnica, de ataques de apresentação expressão que designa qualquer tentativa de enganar o sistema biométrico pela apresentação de algo que simule, sem sê-lo, a característica biométrica real da pessoa. Para identificar e bloquear esses

ataques, os sistemas biométricos utilizam mecanismos denominados PAD (*Presentation Attack Detection*), que funcionam como uma camada adicional de segurança responsável por distinguir, dentro do próprio fluxo de autenticação, um rosto humano real de qualquer simulação apresentada à câmera (BIOID, 2026).

O Instituto Nacional de Padrões e Tecnologia (NIST) esclarece que a prova de vivacidade envolve a análise de características anatômicas ou de reações voluntárias e involuntárias do indivíduo, com o objetivo de verificar se a amostra biométrica está sendo capturada de uma pessoa viva e presente no momento da captura (Estados Unidos, 2026b). Essa preocupação é também reconhecida no plano internacional pela ISO/IEC 30107-1:2023, norma técnica dedicada especificamente à detecção de ataques de apresentação em sistemas biométricos (ISO/IEC, 2023). Contudo, a existência dessas normas e mecanismos não significa que a autenticação facial seja imune a fraudes. A própria evolução das técnicas de PAD revela que os ataques de apresentação também evoluem e que sistemas considerados seguros em determinado momento podem ser vulneráveis a métodos mais sofisticados desenvolvidos posteriormente (BIOID, 2026).

Essa vulnerabilidade já foi documentada em casos concretos. A Operação Face Off, deflagrada pela Polícia Federal, teve como objetivo desarticular associação criminosa especializada em fraudar contas digitais vinculadas à plataforma GOV.BR mediante técnicas avançadas de alteração facial para burlar sistemas de autenticação biométrica. Segundo a notícia oficial, os criminosos simulavam traços faciais de terceiros para obter acesso indevido às contas digitais das vítimas (Brasil, 2025). A notícia do G1 sobre a mesma operação registrou que a ferramenta de *liveness* teria sido um dos principais alvos das fraudes, com suspeita de que aproximadamente três mil contas do GOV.BR teriam sido afetadas (PF SUSPEITA..., 2025). Embora o caso envolva plataforma pública, ele demonstra, em termos concretos, que mecanismos de autenticação facial podem ser objeto de fraude sofisticada, inclusive quando associados a ferramentas de vivacidade.

O ponto jurídico relevante não é exigir uma tecnologia perfeita, mas impedir que a instituição financeira trate a simples alegação de biometria ou *liveness* como prova absoluta da regularidade da contratação. O que se exige é a demonstração técnica mínima de que, no caso concreto, o procedimento foi íntegro, rastreável e compatível com o risco da contratação remota, o que encontra respaldo direto na Resolução CMN nº 4.753/2019, que impõe às instituições o dever de assegurar a integridade, a autenticidade e a confidencialidade das informações e documentos eletrônicos utilizados na abertura de contas (Brasil, 2019).

A vulnerabilidade da biometria facial, portanto, não constitui hipótese abstrata, nem conduz à exigência utópica de um sistema imune a qualquer fraude. Trata-se de risco técnico conhecido, documentado e compatível com o debate jurídico sobre fortuito interno. Em casos de abertura digital

de contas em que haja indícios de fraude ou impugnação da contratação pelo suposto titular, a simples apresentação de selfie, print sistêmico ou relatório unilateral de biometria facial sem o emprego de tecnologias antifraude não deve ser tratada como prova absoluta da contratação quando desacompanhada de elementos técnicos mínimos que permitam verificar a autenticidade, a integridade e a rastreabilidade do procedimento.

5 RESPONSABILIDADE CIVIL BANCÁRIA: CDC, RISCO DO EMPREENDIMENTO E SÚMULAS 297 E 479 DO STJ:

A incidência do Código de Defesa do Consumidor às instituições financeiras não constitui questão controvertida no direito brasileiro. O próprio art. 3º, § 2º, do CDC inclui, entre os serviços submetidos ao microssistema consumerista, as atividades de natureza bancária, financeira, de crédito e securitária. Essa opção legislativa foi consolidada pela Súmula n. 297 do Superior Tribunal de Justiça, segundo a qual o Código de Defesa do Consumidor é aplicável às instituições financeiras (Brasil, 2004). Farias e Rosenvald observam, nesse sentido, que a tentativa de afastar os bancos do regime protetivo do CDC foi corretamente superada pela jurisprudência, sobretudo porque a definição legal de serviço foi construída de maneira ampla e expressamente incluiu a atividade bancária e financeira (Farias; Rosenvald, 2019, p. 1940).

Essa incidência é especialmente relevante porque a controvérsia envolvendo abertura fraudulenta de conta digital não se limita à validade formal de um cadastro, à existência de uma selfie ou à apresentação de documento eletrônico unilateral. O que se discute é a segurança do serviço financeiro prestado em ambiente digital. Se a instituição financeira oferece abertura remota de conta, validação automatizada de identidade, autenticação biométrica e contratação por aplicativo, esse conjunto de atos integra a cadeia de fornecimento do serviço bancário. Eventual falha na identificação do titular, na validação dos dados, na manifestação da vontade ou na rastreabilidade do procedimento não ocorre fora da atividade bancária, mas no interior do próprio serviço disponibilizado ao mercado. Nesse ponto, incide a responsabilidade objetiva pelo fato do serviço, prevista no art. 14 do CDC: a instituição financeira responde, independentemente de culpa, pelos danos causados ao consumidor por defeitos relativos à prestação do serviço, salvo se demonstrar a inexistência do defeito, a culpa exclusiva do consumidor ou a culpa exclusiva de terceiro.

A teoria do risco, nesse contexto, deve ser compreendida com precisão. Rosenvald e Braga Netto distinguem o risco-proveito do risco criado, explicando que este último se satisfaz com a constatação objetiva de que o dano decorreu do risco inerente à atividade desenvolvida, independentemente da demonstração específica do proveito auferido pelo agente (Rosenvald; Braga

Netto, 2024, p. 1809). Assim, mais do que afirmar que o banco responde porque lucra com a digitalização, importa reconhecer que ele responde porque organiza, controla e explora uma atividade que cria riscos jurídicos e tecnológicos para terceiros. A abertura remota de contas não é um evento isolado, artesanal ou acidental, mas parte de uma atividade econômica organizada, massificada e tecnicamente estruturada pela instituição financeira: o banco define o fluxo de cadastramento, escolhe os mecanismos de autenticação, estabelece os critérios de validação documental, contrata ou desenvolve sistemas antifraude, armazena os registros técnicos e decide quais elementos serão considerados suficientes para aprovar a abertura da conta. Quando esse ambiente permite a criação fraudulenta de vínculo bancário em nome de terceiro, o risco não se apresenta como fato estranho ao serviço, mas como consequência possível do modelo de contratação digital escolhido e explorado pelo fornecedor.

A teoria do risco do empreendimento reforça essa conclusão. Quem exerce profissionalmente atividade econômica organizada para a produção ou distribuição de bens e serviços deve suportar os ônus decorrentes de eventos danosos inerentes ao processo produtivo ou distributivo, pois o fornecedor controla a organização da atividade e se coloca como garantidor da qualidade e da segurança daquilo que oferece ao mercado (Rosenvald; Braga Netto, 2024, p. 1826-1827). Aplicada às instituições financeiras, essa premissa significa que os riscos derivados da abertura digital de contas, da autenticação remota e da validação biométrica integram a esfera de organização do próprio banco, não podendo ser simplesmente deslocados ao consumidor ou a um terceiro prejudicado.

A fraude praticada por terceiro, nesse cenário, não deve ser automaticamente tratada como causa externa apta a romper o nexo causal. O ponto decisivo não é apenas a existência de atuação fraudulenta de terceiro, mas o local jurídico-funcional em que a fraude se materializa. Se ela ocorre dentro do ambiente de contratação, autenticação e abertura de conta estruturado pela instituição financeira, não se está diante de fato estranho ao serviço, mas de risco que nasce ou se intensifica no modo como o banco organiza sua atividade digital. A responsabilidade objetiva perderia grande parte de sua função protetiva se toda fraude praticada por terceiro fosse imediatamente convertida em excludente de causalidade, sem exame de sua conexão com a atividade bancária.

É nesse contexto que a Súmula n. 479 do Superior Tribunal de Justiça assume papel central. O enunciado consolida a responsabilidade objetiva das instituições financeiras pelos danos decorrentes de fortuito interno relacionado a fraudes e delitos praticados por terceiros no âmbito das operações bancárias (Brasil, 2012). Farias e Rosenvald observam que, no ambiente bancário digital, os bancos respondem pelos riscos do negócio e devem suportar o ônus da rastreabilidade das operações realizadas, especialmente por meio de logs, sendo a Súmula n. 479 expressão dessa

orientação objetiva de responsabilidade por fraudes bancárias inseridas no risco da atividade (Farias; Rosenvald, 2019, p. 1940).

A distinção entre fortuito interno e fortuito externo é, portanto, essencial. O fortuito interno é aquele relacionado à pessoa do devedor ou da empresa e à organização que imprimem ao negócio, ao passo que o fortuito externo corresponde a acontecimento sem conexão com essa esfera de organização (Rosenvald; Braga Netto, 2024, p. 1555-1556). Transportada essa distinção para a abertura digital de contas, a fraude de identidade, o uso indevido de dados pessoais, a apresentação de documento falso ou a burla de mecanismo de validação facial não constituem, por si, fatos automaticamente externos ao banco. Quando esses eventos se realizam dentro do fluxo de onboarding digital, autenticação biométrica e validação cadastral concebido pela própria instituição, configuram fortuito interno, pois se vinculam à organização do serviço bancário. A fraude somente poderia ser tratada como fortuito externo se demonstrada sua completa estraneidade ao serviço, isto é, se comprovado que o dano decorreu de fato inevitável, externo e sem relação com os riscos introduzidos pela atividade financeira digital.

Por fim, na abertura fraudulenta de conta, a pessoa prejudicada pode não ter solicitado serviço, assinado contrato, utilizado aplicativo ou mantido qualquer relação consciente com a instituição financeira. Ainda assim, está revestida pelo sistema de proteção ao consumidor. O art. 17 do CDC equipara a consumidor todas as vítimas do evento danoso, permitindo a incidência do regime consumerista mesmo quando não há relação contratual direta entre a vítima e o fornecedor. Rosenvald e Braga Netto explicam que o microssistema consumerista protege não apenas o consumidor em sentido estrito, mas também as pessoas reflexamente atingidas por fato do produto ou do serviço, ainda que não tenham prévia relação jurídica com o fornecedor (Rosenvald; Braga Netto, 2024, p. 432). A pessoa cujos dados são indevidamente utilizados para abertura de conta digital deve ser compreendida, portanto, como vítima do evento danoso e consumidora por equiparação e a inexistência de contratação voluntária não afasta a incidência do CDC, mas, ao contrário, evidencia a necessidade de proteção daquele que foi atingido pelo risco do serviço bancário digital.

6 A INSUFICIÊNCIA PROBATÓRIA DA MERA EXIBIÇÃO DE SELFIE OU ASSINATURA BIOMÉTRICA FACIAL:

A questão central deste tópico é saber se a mera exibição de selfie, fotografia facial ou relatório unilateral de aprovação biométrica basta para comprovar a manifestação da vontade de um legítimo contratante e a regularidade da abertura digital de uma conta bancária. A resposta defendida neste estudo é negativa. A selfie pode integrar o conjunto probatório da contratação digital, mas não

deve ser tratada, isoladamente, como prova absoluta da manifestação de vontade, da identidade do contratante ou da integridade do procedimento de autenticação.

6.1 ASSIMETRIA TÉCNICA, ÔNUS DA PROVA E OPACIDADE DO PROCEDIMENTO DE AUTENTICAÇÃO

A contratação bancária digital é marcada por evidente assimetria técnica e informacional. Enquanto a instituição financeira possui acesso aos logs, metadados, endereço de IP, identificação do dispositivo, geolocalização, hash da imagem, score de compatibilidade facial, prova de vivacidade, base de comparação utilizada, registros antifraude e trilha de auditoria, o consumidor tem acesso, quando muito, ao resultado final do procedimento: a existência de uma conta, contrato, cobrança, movimentação, restrição cadastral ou negativação indevida de dívida que afirma desconhecer. A controvérsia probatória, portanto, não se estabelece entre partes situadas no mesmo plano técnico, mas entre o fornecedor que estrutura e controla o ambiente digital de contratação e a pessoa que apenas sofre os efeitos externos do procedimento.

Essa desigualdade não é apenas fática, mas juridicamente relevante. Rosenvald e Braga Netto observam que o consumidor, em razão de sua assimetria informacional, ocupa posição objetivamente vulnerável nas relações obrigacionais de consumo, sobretudo quando sua legítima expectativa de segurança é frustrada por defeito do produto ou do serviço, destacando ainda que o déficit de informações pode impedir que o consumidor identifique, de imediato, a existência do dano injusto e sua própria autoria, o que reforça a necessidade de tutela diferenciada em situações nas quais a vítima não dispõe dos elementos técnicos necessários para compreender sequer a origem do prejuízo sofrido (Rosenvald; Braga Netto, 2024, p. 1437-1438).

A vulnerabilidade técnica do consumidor digital reforça esse raciocínio. Marques e Mucelin explicam que a vulnerabilidade técnica decorre da ausência de conhecimentos específicos ou especializados do consumidor sobre produtos e serviços, seus componentes, utilidades e efeitos. Ao transportarem essa categoria para a ambiência virtual, os autores observam que o meio eletrônico, automatizado e telemático acrescenta uma camada própria de complexidade, pois o consumidor não pode ser presumido especialista em computadores, sistemas de internet, ciência de dados, plataformas digitais ou inteligência artificial (Marques; Mucelin, 2022, p. 8). Aplicada à abertura digital de contas, essa formulação demonstra que não é razoável exigir da vítima compreensão ou reconstrução técnica do funcionamento interno de mecanismos biométricos, fluxos antifraude, registros sistêmicos ou critérios automatizados de aprovação cadastral.

A opacidade do procedimento de autenticação, nesse cenário, não pode favorecer quem a produziu. Se a instituição financeira escolhe substituir a conferência presencial por fluxos digitais automatizados, define os critérios de validação biométrica, controla os registros técnicos do procedimento e conserva os dados capazes de demonstrar a regularidade da contratação, também deve suportar o ônus de apresentar tais elementos quando a contratação é impugnada. Essa conclusão decorre da própria lógica do art. 6º, VIII, do CDC e do art. 373, II, do CPC: em relações de consumo, a inversão do ônus da prova se justifica quando presentes a verossimilhança das alegações ou a hipossuficiência técnica do consumidor; e quando o banco invoca a biometria facial como fato impeditivo, modificativo ou extintivo de sua responsabilidade, cabe-lhe demonstrar a regularidade técnica do procedimento que afirma ter sido válido.

Exigir que a vítima prove tecnicamente a fraude equivaleria a transferir ao consumidor o encargo de auditar sistema ao qual não tem e nunca teve acesso, pois a prova decisiva não está na esfera de disponibilidade da vítima, mas nos registros internos da instituição financeira: logs de acesso, data e horário da captura, dispositivo utilizado, endereço de IP, geolocalização, trilha de auditoria, base de comparação biométrica, score de compatibilidade, prova de vivacidade e documentos analisados no *onboarding*. Ausentes esses elementos, a selfie ou registro facial isolado permanece como dado visual unilateral, incapaz de comprovar, por si só, identidade, consentimento e integridade do procedimento.

6.2 A ORIENTAÇÃO JURISPRUDENCIAL SOBRE A INSUFICIÊNCIA DA SELFIE COMO PROVA ISOLADA DA CONTRATAÇÃO

A jurisprudência tem sinalizado que a mera apresentação de selfie, fotografia ou relatório unilateral de autenticação facial não constitui prova suficiente da regularidade da contratação bancária digital quando desacompanhada de elementos técnicos ou comparativos mínimos.

O Tribunal de Justiça de São Paulo, ao julgar a Apelação Cível nº 1004810-95.2021.8.26.0541, reconheceu que a selfie, por si só, não comprova a utilização de método de biometria facial. O acórdão destacou a existência de documentos apócrifos, divergência significativa entre a geolocalização indicada nos instrumentos e o endereço da autora, além de inconsistências que apontavam indícios de fraude, reforçando que a selfie não pode ser tratada como prova autônoma e conclusiva da contratação quando o conjunto documental revela fragilidades no procedimento digital.

No mesmo sentido, o Tribunal de Justiça do Rio de Janeiro, no julgamento da Apelação nº 0820990-63.2022.8.19.0208, afastou a validade de contratação eletrônica em que constava apenas selfie da autora, sem evidência adequada de certificação da assinatura eletrônica. O acórdão ressaltou

que a informação de geolocalização no momento da assinatura não correspondia ao endereço de residência da consumidora, concluindo que o instrumento contratual se mostrava facilmente manipulável por terceiros. A decisão reconheceu a falha na prestação do serviço, qualificando a fraude como fortuito interno não imputável ao consumidor hipossuficiente, em consonância com a Súmula 479 do STJ.

O Tribunal de Justiça de Pernambuco, em decisão contida nos autos da Apelação Cível nº 0019953-08.2023.8.17.2810, ao julgar um caso de empréstimo consignado supostamente firmado por assinatura eletrônica com selfie, concluiu que a fotografia apresentada pelo banco não continha critérios ou parâmetros técnicos capazes de vincular a imagem à manifestação de vontade da consumidora, assentando que, impugnada a contratação, cabe à instituição financeira comprovar sua regularidade de forma robusta.

Esses julgados demonstram algo preciso: a imagem facial pode compor o conjunto probatório, mas sua força depende da contextualização técnica do procedimento. Quando apresentada de forma isolada, unilateral e sem registros auditáveis, a selfie não comprova a manifestação de vontade nem a integridade do fluxo digital de contratação.

6.3 ELEMENTOS TÉCNICOS MÍNIMOS PARA QUE A BIOMETRIA TENHA FORÇA LIBERATÓRIA

Para que a biometria facial possa assumir força probatória suficiente, é necessário apresentar elementos técnicos que permitam verificar a regularidade do procedimento. Entre esses elementos destacam-se: data e horário da captura; IP; identificação do dispositivo; geolocalização, quando disponível e juridicamente tratada; logs de acesso; trilha de auditoria; hash da imagem ou do arquivo; score de compatibilidade facial; prova de vivacidade; identificação da base comparada; registros antifraude; evidência de que os dados não foram alterados; documentação do fluxo de onboarding; registro da decisão automatizada; e demonstração de conformidade com os controles exigidos à época.

Esses elementos não têm por finalidade transformar o processo judicial em auditoria técnica completa de sistemas biométricos. Sua função é permitir que o julgador avalie se a biometria invocada pelo banco corresponde a um procedimento íntegro e rastreável, ou se consiste apenas em imagem ou relatório unilateral incapaz de demonstrar a regularidade da contratação.

A Resolução BCB nº 343/2023 reforça a relevância regulatória desses registros ao tratar do compartilhamento de dados e informações sobre indícios de fraudes, prevendo que os registros contenham, quando disponíveis, data, horário, local, canal utilizado, identificação do dispositivo

eletrônico, descrição da causa ou procedimento que ensejou o indício de fraude e indicação sobre eventual atuação do cliente (Banco Central do Brasil, 2023c). O AIR do Voto nº 84/2023-BCB segue a mesma direção ao reconhecer que a fraude na contratação digital é fenômeno regulatoriamente conhecido, mencionando iniciativas de abertura de contas com falsidade ideológica ou uso das mesmas informações cadastrais em diferentes instituições (Banco Central do Brasil, 2023b). Há ainda o antecedente regulatório da Resolução CMN nº 4.480/2016 que, embora revogada, demonstra a continuidade da preocupação com rastreamento e auditoria ao exigir a manutenção de registros e trilhas de auditoria à disposição do Banco Central pelo prazo mínimo de cinco anos (Brasil, 2016) confirmando que, se as normas do Banco Central funcionam como *standard* objetivo da segurança legitimamente esperada do serviço bancário, a prova judicial da autenticação biométrica deve ser minimamente compatível com esse padrão regulatório (CESA, 2025, p. 60 e 61).

Portanto, a força liberatória da biometria facial depende da demonstração de sua consistência técnica no caso concreto. A simples existência de uma imagem facial não a equipara a uma assinatura digital, instituto que pressupõe procedimento certificado, rastreável e juridicamente regulado. Sem registros técnicos auditáveis, a biometria facial perde densidade probatória e se aproxima de uma mera imagem isolada, cuja origem, contexto de captura e integridade não podem ser adequadamente verificados.

Agrava esse quadro o fato de que nem mesmo os mecanismos de *liveness detection* são imunes a fraudes sofisticadas. Essa vulnerabilidade já foi documentada em casos concretos com expressivo alcance. A Operação Face Off, deflagrada pela Polícia Federal em maio de 2025, teve como objetivo desarticular associação criminosa especializada em fraudar contas digitais vinculadas à plataforma GOV.BR mediante técnicas avançadas de alteração facial para burlar sistemas de autenticação biométrica (Brasil, 2025). Segundo a Polícia Federal, as investigações revelaram que os criminosos simulavam traços faciais de terceiros para obter acesso indevido às contas digitais das vítimas, assumindo o controle total dos perfis e, consequentemente, de serviços públicos e informações pessoais sensíveis (Brasil, 2025).

O caso é juridicamente relevante não apenas pelo número de vítimas, mas pelo que revela sobre a natureza do risco: a fraude não decorreu de falha técnica pontual ou descuido isolado, mas de método sistemático e especializado de burla ao próprio mecanismo de prova de vivacidade, demonstrando que esse risco não é hipótese abstrata, mas vulnerabilidade operacional conhecida e explorada de forma organizada. Embora o caso envolva plataforma pública, a técnica de simulação de traços faciais para burlar sistemas biométricos é igualmente aplicável ao ambiente de contratação bancária digital, reforçando que a alegação isolada da existência de captura biométrica facial não pode funcionar como única fonte prova conclusiva de autenticação regular.

7 RESULTADOS E DISCUSSÃO: QUANDO A BIOMETRIA PODE OU NÃO PRODUZIR EFEITO LIBERATÓRIO:

A pesquisa permite sistematizar quatro resultados que, confrontados com a hipótese formulada, confirmam a tese central do estudo.

O primeiro resultado é que a abertura digital de contas é juridicamente admitida, mas condicionada a deveres regulatórios de verificação, validação e rastreabilidade que não se satisfazem com a simples recepção de uma imagem facial ou aprovação automatizada de cadastro. A Resolução CMN nº 4.753/2019 não prescreve meios técnicos específicos, mas impõe deveres regulatórios objetivos: verificar e validar a identidade dos titulares, assegurar a integridade e a autenticidade dos documentos eletrônicos e formalizar os critérios de identificação adotados (Brasil, 2019). Por se tratarem de obrigações de resultado e não de meio, seu cumprimento deve ser avaliado em função do estado da arte das fraudes no momento da contratação. Com o avanço das técnicas de burla biométrica como os ataques de apresentação e o uso de deepfakes, exemplificados concretamente pela Operação Face Off —, os mecanismos de autenticação devem igualmente evoluir para que seja possível corresponder aos imperativos da norma. A conformidade com a resolução é, portanto, condição necessária mas não suficiente para afastar a responsabilidade civil e sua aplicação prática exige atualização contínua dos meios adotados diante da evolução das fraudes.

O segundo resultado é que a biometria facial, isoladamente, não representa prova absoluta da contratação e não pode ser equiparada a uma assinatura digital, instituto que pressupõe procedimento certificado, rastreável e juridicamente regulado. Seu valor probatório depende da demonstração técnica do procedimento utilizado e da extensão e qualidade dos registros comparados, pois quanto mais robusto o conjunto de dados analisados, maior a possibilidade de verificar, com segurança, a autenticidade e a integridade da captura. A simples alegação de que houve biometria ou liveness detection não encerra a controvérsia.

O terceiro resultado decorre da análise jurisprudencial. Os julgados examinados no TJSP, TJRJ e TJPE convergem no sentido de que a apresentação isolada de selfie ou fotografia não tem sido considerada suficiente para demonstrar a regularidade da contratação bancária digital, seja quando ausentes elementos técnicos mínimos, seja quando presentes incongruências que indicam fraude como incompatibilidade entre a geolocalização registrada no momento da contratação e o endereço do suposto contratante, documentos apócrifos ou ausência de certificação adequada da assinatura eletrônica. A jurisprudência não nega a utilidade da biometria facial, mas recusa sua utilização como prova conclusiva quando desacompanhada de trilha de auditoria ou registros capazes de vincular a

imagem à manifestação válida de vontade do legítimo contratante, cabendo à instituição financeira demonstrar a regularidade do procedimento de forma robusta quando a contratação é impugnada.

O quarto resultado é que, diante de fraude na abertura digital de conta, a responsabilidade bancária tende a ser objetiva e enquadrável como fortuito interno quando a fraude se materializa no ambiente de contratação estruturado pela própria instituição. Essa conclusão decorre da aplicação conjunta do art. 14 do CDC, da teoria do risco criado, do risco do empreendimento e da Súmula 479 do STJ, e não significa responsabilização automática por qualquer fato externo, mas por evento danoso situado no interior do modelo digital que o banco organiza, controla e explora economicamente.

Confrontados com a hipótese formulada, esses quatro resultados a confirmam: a biometria facial, enquanto mecanismo inserido em processo massificado de contratação bancária digital, integra o risco próprio da atividade, e a fraude que se vale de suas vulnerabilidades conhecidas configura fortuito interno. O efeito liberatório da biometria não decorre de sua simples invocação, mas da demonstração concreta, por registros técnicos auditáveis, de que o procedimento foi íntegro, rastreável e compatível com os padrões regulatórios exigíveis à época da contratação. Ausente essa demonstração, o dano deve permanecer no campo do risco interno da atividade bancária digital, configurando o dever de indenizar da instituição financeira.

8 CONSIDERAÇÕES FINAIS:

O problema de pesquisa proposto consistiu em verificar se, diante das vulnerabilidades conhecidas dos mecanismos de autenticação facial, a mera apresentação de assinatura biométrica facial seria suficiente para afastar a responsabilidade civil do banco pela abertura fraudulenta de conta digital. A resposta alcançada é negativa.

A pesquisa demonstrou que a abertura digital de contas é juridicamente admitida, mas condicionada à adoção de controles capazes de verificar identidade, qualificação, autenticidade, integridade e segurança das informações utilizadas no procedimento. A contratação remota não elimina os deveres regulatórios da instituição financeira; ao contrário, exige que a substituição da conferência presencial por mecanismos automatizados seja acompanhada de registros técnicos verificáveis. Nesse sentido, o estudo das normativas do Banco Central não serve para investigar culpa, mas para delimitar o padrão objetivo de segurança legitimamente esperado do serviço bancário digital e o mero cumprimento formal dessas normas não possui efeito exoneratório automático**.**

A expressão "assinatura biométrica facial" pode abranger realidades técnicas distintas, desde uma simples selfie até um fluxo robusto com prova de vivacidade, logs, metadados, trilha de auditoria

e registros de integridade. A simples existência de uma imagem facial não a equipara a uma assinatura digital, instituto que pressupõe procedimento certificado, rastreável e juridicamente regulado. As vulnerabilidades desse modelo não são hipótese abstrata: a Operação Face Off demonstrou que associação criminosa especializada conseguiu burlar sistematicamente ferramentas de *liveness detection* mediante simulação de traços faciais de terceiros, comprometendo aproximadamente três mil contas e evidenciando que esse risco é operacional, organizado e conhecido.

Nesse contexto, a fraude biométrica relacionada à abertura digital de contas configura fortuito interno quando se materializa no ambiente de contratação estruturado pela própria instituição financeira. Não se trata de responsabilizar o banco por qualquer fato externo à sua atividade, mas por evento danoso situado no interior do modelo digital que ele organiza e explora economicamente, com ganhos de escala, redução de custos e ampliação da base de clientes. As consequências para a vítima são concretas e graves cobranças indevidas, restrições cadastrais e negativações que afirma desconhecer —, o que torna inadequado transferir a ela o ônus de um risco que o banco criou, organizou e do qual se beneficiou economicamente.

Conclui-se, portanto, que a mera apresentação de selfie, print sistêmico ou relatório unilateral de biometria facial não deve ser considerada suficiente para afastar a responsabilidade civil da instituição financeira quando desacompanhada de registros técnicos auditáveis que demonstrem integridade, autenticidade, rastreabilidade e conformidade do procedimento adotado. Nessas hipóteses, incide a responsabilidade objetiva prevista no Código de Defesa do Consumidor e consolidada pela Súmula 479 do Superior Tribunal de Justiça, por se tratar de fortuito interno relacionado à atividade bancária, configurando o dever de indenizar da instituição financeira.

A biometria facial não deve ser descartada como mecanismo de autenticação, mas tampouco pode funcionar como argumento automático de exoneração. Em um ambiente de contratação massificada, tecnicamente assimétrico e vulnerável a fraudes conhecidas, sua validade probatória depende da demonstração concreta da regularidade do procedimento. Ausente essa demonstração, o dano decorrente da abertura fraudulenta da conta deve permanecer no campo do risco do empreendimento bancário e não ser transferido à vítima da fraude.

REFERÊNCIAS

BIOID. Liveness Detection: Spoof Prevention for Facial Recognition. Nuremberg: BioID GmbH, [2024?]. Disponível em: https://www.bioid.com/liveness-detection/. Acesso em: 22 maio 2026.

BRASIL. Banco Central do Brasil. **Resolução CMN nº 4.753, de 26 de setembro de 2019**. Dispõe sobre a abertura, a manutenção e o encerramento de contas de depósitos. Brasília, DF: BCB, 2019. Disponível em:

https://www.bcb.gov.br/estabilidadefinanceira/exiberegulacao?classe=Resolu%C3%A7%C3%A3o%20CMN&num=4753. Acesso em: 22 maio 2026.

BRASIL. Banco Central do Brasil. **Resolução Conjunta nº 6, de 23 de maio de 2023**. Dispõe sobre requisitos para o compartilhamento de dados e informações sobre indícios de fraudes de que trata o art. 34-A da Lei nº 12.865, de 9 de outubro de 2013. Brasília, DF: BCB, 2023. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exiberegulacao?classe=Resolu%C3%A7%C3%A3o%20Conjunta&num=6. Acesso em: 22 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 297**. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Brasília, DF: Diário da Justiça, 24 nov. 2004.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 479**. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, DF: Diário da Justiça Eletrônico, 1º ago. 2012.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.008.384/SP**. Relatora: Ministra Nancy Andrighi, julgado em 06 de dezembro de 2022. Diário da Justiça Eletrônico, 09 dez. 2022.

CESA, Victor Búrigo. **Responsabilidade civil das instituições financeiras em caso de fraude**. 2025. Dissertação (Mestrado em Direito) – Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina, Florianópolis, 2025. Disponível em: https://repositorio.ufsc.br/. Acesso em: 22 maio 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO); INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 37, Biometrics. ISO/IEC 30107-1:2023(E): Information technology — Biometric presentation attack detection — Part 1: Framework. 2. ed. Genebra: ISO/IEC, 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Biometrics. In: NIST Computer Security Resource Center (CSRC) Glossary. Gaithersburg: NIST, [2024?]. Disponível em: https://csrc.nist.gov/glossary/term/Biometrics. Acesso em: 22 maio 2026.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Novo Tratado de Responsabilidade Civil**. 4. ed. São Paulo: Atlas, 2019. p. 1940-1943.

MARQUES, Claudia Lima; MUCELIN, Guilherme. Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor. **civilistica.com**, Rio de Janeiro, a. 11, n. 3, 2022. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/872. Acesso em: 22 maio 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Biometrics. In: NIST Computer Security Resource Center (CSRC) Glossary. Gaithersburg: NIST, [2024?]. Disponível em: https://csrc.nist.gov/glossary/term/Biometrics. Acesso em: 22 maio 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Presentation Attack Detection (PAD). In: NIST Computer Security Resource Center (CSRC) Glossary. Gaithersburg:

NIST, [2024?]. Disponível em: https://csrc.nist.gov/glossary/term/Presentation_Attack_Detection. Acesso em: 22 maio 2026.

PERNAMBUCO. Tribunal de Justiça do Estado de Pernambuco (4ª Câmara Cível). **Apelação Cível nº 0019953-08.2023.8.17.2810**. Relator: Des. Cândido José da Fonte Saraiva de Moraes, 12 de novembro de 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pe/2850114815. Acesso em: 22 maio 2026.

RIO DE JANEIRO. Tribunal de Justiça do Estado do Rio de Janeiro (17ª Câmara de Direito Privado). **Apelação Cível nº 0820990-63.2022.8.19.0208**. Relatora: Desª. Sandra Santarém Cardinali. Julgado em: 9 maio 2024. Diário da Justiça Eletrônico, publicado em: 10 maio 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rj/2478357497. Acesso em: 22 maio 2026.

ROSENVALD, Nelson; NETTO, Felipe Braga. **Responsabilidade civil**: teoria geral. Indaiatuba, SP: Editora Foco, 2024.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (13ª Câmara de Direito Privado). **Apelação Cível nº 1004810-95.2021.8.26.0541**. Comarca de Santa Fé do Sul. Relator: Des. Cauduro Padin. Julgado em: 23 nov. 2022. Diário da Justiça Eletrônico, publicado em: 2 dez. 2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pe/2850114815. Acesso em: 22 maio 2026.