UNIVERSIDADE FEDERAL DO PAMPA
CAMPUS SÃO BORJA
BACHARELADO EM DIREITO

ALINE DA SILVA RODRIGUES

RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS PELO USO FRAUDULENTO DA BIOMETRIA FACIAL EM CONTRATOS DIGITAIS: análise de padrões técnicos de decisões judiciais no Tribunal de Justiça do RS de 2020 a 2024

São Borja
2025

ALINE DA SILVA RODRIGUES

RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS PELO USO FRAUDULENTO DA BIOMETRIA FACIAL EM CONTRATOS DIGITAIS: Tendências de decisões judiciais no Tribunal de Justiça do RS de 2020 a 2024

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Federal do Pampa - UNIPAMPA, campus São Borja.

Orientadora: Aline Fagundes dos Santos

São Borja
2025

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais) .

R696r Rodrigues, Aline da Silva
RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS PELO USO FRAUDULENTO DA BIOMETRIA FACIAL EM CONTRATOS DIGITAIS: Tendências de decisões judiciais no Tribunal de Justiça do RS de 2020 a 2025 / Aline da Silva Rodrigues.
34 p.

Trabalho de Conclusão de Curso(Graduação)-- Universidade Federal do Pampa, DIREITO, 2025.
"Orientação: Aline Fagundes dos Santos".

1. biometria facial. 2. responsabilidade civil. 3. contratos digitais . 4. fraudes bancárias. 5. hipervulnerabilidade do consumidor. I. Título.

ALINE DA SILVA RODRIGUES

RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS PELO USO FRAUDULENTO DA BIOMETRIA FACIAL EM CONTRATOS DIGITAIS: análise de padrões técnicos de decisões judiciais no Tribunal de Justiça do RS de 2020 a 2024

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Bacharel em Direito.

Trabalho defendido e aprovado em: 03/07/2025.

Banca examinadora:

Documento assinado digitalmente
gov.br
ALINE FAGUNDES DOS SANTOS
Data: 15/07/2025 09:35:17-0300
Verifique em https://validar.iti.gov.br

_____

Prof. Drª. Aline Fagundes dos Santos
Orientadora
(Unipampa)

Documento assinado digitalmente
gov.br
ANELINE DOS SANTOS ZIEMANN LUCIO
Data: 15/07/2025 08:59:50-0300
Verifique em https://validar.iti.gov.br

_____

Prof. Post. Drª. Aneline dos Santos Ziemann Lucio
(Unipampa)

Documento assinado digitalmente
gov.br
LETICIA GHELLER ZANATTA CARRION
Data: 14/07/2025 22:39:24-0300
Verifique em https://validar.iti.gov.br

_____

Prof. Drª. Leticia Gheller Zanatta Carrion
(Unipampa)

Toda a descoberta da ciência pura é potencialmente subversiva; por vezes a ciência deve ser tratada como um inimigo possível.

Aldous Huxley

RESUMO

O presente trabalho tem como objetivo analisar a responsabilidade civil das instituições financeiras diante do uso fraudulento da biometria facial em contratos bancários digitais, com foco nas decisões proferidas pelo Tribunal de Justiça do Rio Grande do Sul (TJRS) entre os anos de 2020 e 2024. O estudo parte da crescente digitalização dos serviços bancários e da adoção de tecnologias biométricas como forma de assinatura de contratos, especialmente após a pandemia de Covid-19. No entanto, essa evolução trouxe consigo novos desafios, como o aumento de fraudes que afetam, em especial, consumidores em situação de hipervulnerabilidade. A metodologia utilizada foi quantitativa, com pesquisa exploratória, descritiva e documental, através da análise de cinco acórdãos do TJRS relacionados a contratos de empréstimo consignado firmados com uso de biometria facial. A análise revelou que, embora o Tribunal reconheça a responsabilidade objetiva das instituições financeiras com base no Código de Defesa do Consumidor, as decisões raramente mencionam normas técnicas fundamentais, como as diretrizes da Empresa de Tecnologia e Informações da Previdência (Dataprev), do Instituto de Tecnologia de Informação (ITI) e a Lei Federal nº 14.063/2020, que regulam a segurança da autenticação biométrica. Conclui-se que há uma lacuna entre a legislação técnica existente e sua aplicação prática pelo Poder Judiciário do Rio Grande do Sul, o que compromete a proteção do consumidor. Defende-se a necessidade de maior integração entre direito e tecnologia, com exigência de provas técnicas robustas e capacitação dos operadores do direito, para que a inovação digital não se transforme em instrumento de exclusão ou insegurança.

Palavras-chave: biometria facial; contratos digitais; fraudes bancárias; hipervulnerabilidade do consumidor; responsabilidade civil.

ABSTRACT

This study aims to analyze the civil liability of financial institutions in cases involving the fraudulent use of facial biometrics in digital banking contracts, with a focus on decisions issued by the Court of Justice of the State of Rio Grande do Sul (TJRS) between 2020 and 2024. The research is grounded in the growing digitalization of banking services and the adoption of biometric technologies as a method of contract authentication, particularly after the Covid-19 pandemic. However, this technological advancement has brought new challenges, such as the increase in fraud, especially affecting consumers in situations of heightened vulnerability. The methodology employed is quantitative, involving exploratory, descriptive, and documentary research through the analysis of five appellate decisions by the TJRS concerning payroll loan contracts authenticated via facial biometrics. The findings show that, although the court recognizes the strict liability of financial institutions based on the Consumer Protection Code, the rulings rarely reference essential technical standards, such as those issued by the Social Security Technology and Information Company (Dataprev), the National Institute of Information Technology (ITI), and Federal Law No. 14,063/2020, which regulate biometric authentication security. The study concludes that there is a gap between existing technical legislation and its practical application by the judiciary in Rio Grande do Sul, which undermines consumer protection. It advocates for greater integration between law and technology, emphasizing the need for robust technical evidence and the training of legal professionals so that digital innovation does not become a tool of exclusion or insecurity.

Keywords: banking fraud; civil liability; consumer vulnerability; digital contracts; facial biometrics.

SUMÁRIO

1 INTRODUÇÃO

O mundo moderno trouxe transformações significativas nas formas de interação humana, destacando-se, entre elas, a ascensão das relações mediadas pelo ambiente digital.

As mudanças significativas e mais visíveis no mundo digital ocorreram após a pandemia de Covid-19 no mundo. Essa situação de saúde pública impôs que a sociedade buscasse se adaptar com dinâmicas de interação que não envolvessem o contato físico. Desse modo, os setores da sociedade que já estavam em processo de digitalização de seus serviços aceleraram tal demanda, como forma de viabilizar o acesso às pessoas o acesso a serviços essenciais e indispensáveis à manutenção da vida em sociedade de forma segura e rápida, o que continuou de forma exponencial após a pandemia.

Nesse contexto, no âmbito das operações financeiras surgiram diversas novidades quanto ao acesso pelos consumidores aos serviços oferecidos pelos bancos e instituições financeiras.

A Federação Brasileira dos Bancos (Febraban, 2025), através de uma Pesquisa[1] de Tecnologia Bancária recente, realizada com 85% dos ativos bancários do País, divulgou que as instituições financeiras estão cada vez mais aderindo ao movimento tecnológico no intuito de oferecer agilidade ao consumidor, motivo pelo qual no último ano houve o crescente número de 82% de investimento em inovação tecnológica no setor.

Em relação a contratação de crédito, a federação bancária explanou que 96% dessas operações estavam sendo realizadas de forma digital até o ano de 2023, indicando uma possibilidade de estarem sendo realizadas de forma inteiramente digital após o período (Febraban, 2024).

Assim, com a crescente utilização do ambiente digital para contratações bancárias, houve também um aumento expressivo de fraudes e golpes nesse setor que atingem especialmente um público hipervulnerável constituído por pessoas analfabetas, deficientes e idosos não inseridos na cultura digital (Marquetti, 2023).

[1] Pesquisa disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_01%20-%205.pdf.

Com o crescente número de contratos digitais bancários passou-se a utilizar com maior frequência a assinatura por biometria facial, o que ocasionou a ocorrência de um aumento significativo de fraudes e golpes com essa assinatura.

Destarte, o objetivo geral da pesquisa é analisar as tendências das decisões judiciais no Tribunal de Justiça do Rio Grande do Sul (TJRS) no julgamento de casos de fraudes decorrentes do uso fraudulento da biometria facial em contratos bancários digitais entre os anos 2020 e 2024.

A metodologia exploratória será empregada como ferramenta para o alcance dos objetivos propostos, investigando as legislações que pautam a problemática central do trabalho, com base na análise da legislação do direito civil, do direito do consumidor e na legislação mais recente pertinente ao uso das tecnologias na contratação bancária por biometria facial. Além disso, será realizada a metodologia descritiva para descrever como o Poder Judiciário do TJRS tem aplicado essas legislações aos casos selecionados.

A abordagem metodológica adotada foi pesquisa quantitativa, por amostragem, a partir de decisões do Tribunal de Justiça do Rio Grande do Sul (TJRS), sendo procedida a coleta dados e análise das decisões com base nas legislações e normas técnicas existentes relacionadas ao uso da biometria facial em contratos bancários digitais.

Para atender tal proposta o trabalho será estruturado em oito partes. A primeira parte trata da responsabilidade civil das instituições financeiras. Em seguida, a segunda parte aborda o uso da biometria facial nas contratações bancárias digitais. A terceira parte discute a segurança cibernética no contexto bancário, enquanto a quarta parte analisa a Lei Federal nº 14.063/2020, bem como as diretrizes técnicas estabelecidas pelo Instituto Nacional de Tecnologia da Informação (ITI) e pela Empresa de Tecnologia e Informações da Previdência (Dataprev). A quinta parte apresenta uma breve exposição sobre a hipervulnerabilidade do consumidor no ambiente digital. Na sexta parte, realiza-se a análise de decisões judiciais proferidas pelo Tribunal de Justiça do Rio Grande do Sul (TJRS). A sétima parte consiste em um estudo comparativo entre as normas técnicas aplicáveis e os entendimentos adotados nas decisões judiciais analisadas, seguido pela discussão dos resultados. Por fim, na oitava parte, são apresentadas as considerações finais do trabalho.

2 RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS

De acordo com Gonçalves, “responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiro, em razão de ato

próprio, de pessoas por quem ela responde, ou de fato de coisa ou animal sob sua guarda" (Gonçalves, 2022, p. 21). A doutrina destaca que a responsabilidade pode ser subjetiva (exigindo a presença de culpa) ou objetiva, baseada no risco assumido, nos casos previstos em lei. O fundamento da responsabilidade civil é a ideia de que ninguém deve causar prejuízo a outrem (*neminem laedere*), princípio basilar do Direito Civil.

No âmbito de operações financeiras, sobre a responsabilidade civil Rosenvald e Neto (2023, págs. 410-411), definem:

> [...]Talvez possamos, historicamente falando, vislumbrar uma escada teórica da responsabilidade civil. Uma escada em que cada degrau não exclui o degrau anterior, mas o pressupõe. Os degraus convivem, não cabendo pleitear a existência exclusiva de determinados pisos, cada qual com funções específicas e relevâncias diferenciadas (...) as discussões, aqui, devem orbitar em torno do nexo causal. Talvez pudéssemos falar, no quarto degrau, em responsabilidade objetiva agravada (ou outra denominação equivalente, as denominações são, em parte, secundárias). Seriam situações em que se dispensa o nexo de causalidade adequada entre o fato e o dano. Exige-se, porém, que haja estreita conexão entre o dano e a atividade do ofensor. Os danos, nesse sentido, precisam guardar conexão com a atividade desenvolvida (os bancos, por exemplo, respondem objetivamente perante os clientes por fraudes praticadas por terceiros – fortuitos internos, consoante reconhece a Súmula 479 do STJ).

À vista disso, a responsabilidade civil das instituições financeiras por fraudes é uma problemática de grande relevância no cenário jurídico brasileiro, considerando o crescente número de golpes eletrônicos que afetam consumidores em todo o país, como se verifica diariamente na mídia.

As instituições financeiras são responsáveis pela vida financeira de inúmeros clientes, seja no recebimento salarial, na aplicação de valores, concessão de crédito, dentre outros. Nesse sentido, mesmo que estejam amparadas por sistemas tecnológicos rebuscados, não são isentas de falhas e fraudes nestes mecanismos, o que gera diversos prejuízos aos usuários.

Nesse sentido, a jurisprudência e a doutrina têm evoluído para garantir maior proteção aos clientes bancários, reconhecendo a responsabilidade objetiva das instituições financeiras em casos de fraudes decorrentes de falhas na prestação de serviços.

A responsabilidade civil das instituições financeiras está fundamentada no Código de Defesa do Consumidor (CDC), que estabelece a responsabilidade objetiva dos fornecedores de serviços por danos causados aos consumidores, independentemente da existência de culpa, conforme art. 14 da lei. ‘

Com base nisso, o Superior Tribunal de Justiça (STJ) pacificou o entendimento de 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, conforme a Súmula 479 do STJ.

Com isso, o fortuito interno refere-se a eventos previsíveis e inerentes à atividade bancária, como fraudes eletrônicas, que devem ser prevenidas pelas instituições financeiras por meio de sistemas de segurança eficazes. Assim, mesmo que a fraude seja praticada por terceiros, a falha na prestação do serviço bancário configura responsabilidade da instituição financeira.

A 9ª Câmara Cível do Tribunal de Justiça do Rio Grande do Sul (TJ/RS), na Apelação Cível nº 5013458-51.2022.8.21.0039, por exemplo, destacou que as instituições financeiras devem adotar mecanismos de segurança necessários para garantir ao consumidor a integridade de sua vida financeira, respondendo objetivamente pelos danos materiais e morais gerados por fraudes no âmbito de operações bancárias.

Em outro caso (Apelação Cível nº 50047854320218210059), o TJ/RS condenou uma instituição bancária a indenizar uma cliente vítima de fraudes devido a falha na segurança do sistema, fixando reparação por danos morais e ressarcimento do dano material.

À vista da responsabilidade civil das instituições financeiras na presente discussão, Marquetti (2023) relata o entendimento jurisprudencial que tem sido adotado em tribunais superiores, nos quais já existe entendimento pacificado de que a instituição financeira possui responsabilidade objetiva em casos de fraude – respondendo objetivamente por fraudes ocorridas na falha de prestação de serviço, quando ausente culpa exclusiva do cliente ou terceiros, bem como a existência de nexo causal entre o dano ocorrido e a conduta do agente.

Diferencia-se, assim, da responsabilidade subjetiva, que exige a demonstração de culpa (negligência, imprudência ou imperícia) por parte do agente causador do dano para que haja obrigação de indenizar (Gagliano; Pamplona Filho, 2021). Nesse contexto, a responsabilidade objetiva prescinde da comprovação de culpa, bastando a existência do dano e do nexo causal.

Entretanto, a responsabilidade civil das instituições financeiras por fraudes contra seus clientes se mostra em inúmeras decisões que estão amplamente fundamentadas em sua maioria no CDC e no entendimento jurisprudencial pacificado. Diante disso, vislumbra-se que as instituições financeiras devem adotar medidas eficazes de segurança para prevenir fraudes e proteger os consumidores. Do contrário, em caso de falha na prestação do serviço, respondem objetivamente pelos danos causados, sendo obrigadas a indenizar os clientes prejudicados.

3 BIOMETRIA FACIAL EM CONTRATAÇÕES BANCÁRIAS DIGITAIS

Estudos demonstram que a biometria facial é resultado de um processo de evolução da tecnologia que criou sistemas de segurança rebuscados, baseados em informações que incluem o *"algo que você é"* do indivíduo:

> Mecanismos de autenticação se baseiam em três paradigmas: algo-que-você-sabe (senha de acesso, por exemplo), algo-que-você-tem (chaves, cartões de acesso e chaves criptográficas, por exemplo) ou algo-que-você-é (voz, impressão digital, retina, palma da mão e qualquer outra) (Maziero, 2019, p. 371 apud Menezes, 2024, p. 8).

> Inicialmente essas soluções estavam restritas ao uso da biometria da digital. Com a evolução das tecnologias, hoje podemos utilizar também as biometrias faciais, por íris, voz, retina, digitação, dentre outras. (Menezes, 2024, p. 8).

Assim, a biometria é a análise de características físicas ou comportamentais de uma pessoa, como digitais, rosto, voz ou forma de andar, feita com métodos matemáticos e estatísticos. Quanto mais dados forem coletados dessas características, maior a chance de identificar alguém de forma única, tornando a análise mais precisa e confiável (Cebrian et al, 2024).

Desse modo, a biometria facial é uma tecnologia que identifica e autentica indivíduos com base em características únicas do rosto. No setor bancário, seu funcionamento envolve várias etapas, como a captura da imagem facial, extração de características (distância dos olhos, formato do queixo,etc), conversão em código numérico único das características extraídas (dados biométricos), armazenamento dos dados no sistema da instituição e por fim a comparação e autenticação desses dados para futuras operações. Essa tecnologia permite que clientes realizem operações bancárias, como abertura de contas e autorizações de transações, de forma remota e segura se for devidamente utilizada.

A utilização da biometria facial está alinhada com a Lei Geral de Proteção de Dados Pessoais (LGPD), desde que sejam adotadas medidas adequadas de segurança e privacidade. A lei trata em seu artigo 5º que os dados biométricos de uma pessoa são considerados dados sensíveis:

> Art. 5º Para os fins desta Lei, considera-se: [...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, **dado genético ou biométrico**, quando vinculado a uma pessoa natural (BRASIL, 2018, grifo nosso)

Assim sendo, a biometria facial pode ser apresentada como uma tecnologia que visa garantir maior segurança e individualização na identificação dos clientes nas operações bancárias digitais. Soares e Carvalho (2023), enfatizam que, apesar da pretensa segurança da

tecnologia, a biometria não é infalível, sendo também vulnerável a fraudes e falhas técnicas. Ainda, o estudo trata que fraudes envolvendo a contratação de empréstimos sem o consentimento dos clientes estão se tornando cada vez mais frequentes.

Além disso, em casos em que o consumidor precisa recorrer ao sistema de justiça para buscar reparação da fraude que foi vítima, a prova pericial no sistema de biometria da instituição financeira é considerada essencial, mas por ser de alta complexidade não pode ser realizada nos juizados especiais cíveis exigindo o ajuizamento da ação na justiça comum.

Assim, embora a biometria represente um avanço nos sistemas de contratação de crédito, abertura de conta e demais demandas financeiras, ainda é insuficiente para proteger plenamente o consumidor, especialmente os hipervulneráveis, motivo que como a contratação de crédito presencial pode ser uma alternativa na prevenção de fraudes (Soares; Carvalho, 2023). Em contrapartida o consumidor pode enfrentar filas de espera o que pode ser prejudicial para clientes com algum tipo de deficiência física, por exemplo.

No mesmo sentido, em pesquisa de Tecnologia Bancária, a Federação Brasileira de Bancos (Febraban, 2024) destacou o uso crescente da biometria facial como uma aplicação consolidada de inteligência artificial no setor bancário. Segundo o estudo, 75% dos bancos respondentes já adotam essa tecnologia como meio de autenticação (Febraban, 2024, p. 21), evidenciando a relevância da biometria para a segurança e a personalização da experiência do cliente. Além disso, a biometria facial é apontada como um dos principais recursos voltados à inovação e à prevenção de fraudes nas operações digitais, principalmente em serviços como contratação de empréstimos.

No entanto, o relatório também observa que, embora essas soluções tragam agilidade e reforcem a confiabilidade das transações, seu uso demanda cuidados com privacidade e ética, além de investimentos contínuos em cibersegurança para previnir riscos de falsificação e acesso indevido. Assim, a pesquisa aponta a biometria como um avanço tecnológico importante, mas que precisa estar inserido num sistema robusto de proteção de dados.

Os benefícios da utilização da biometria facial por instituições bancárias são inúmeros. A biometria facial pode oferecer um nível elevado de segurança, dificultando fraudes e acessos não autorizados, desde que programada de forma segura. Esta forma de assinatura proporciona uma experiência mais fluida e conveniente, uma vez que se faz desnecessário o uso de senhas – as quais podem ser esquecidas - ou dispositivos adicionais para autenticação. Além disso, reduz a burocracia e acelera processos, como a abertura de contas e a assinatura de contratos, que podem ser realizados de forma totalmente digital, sem que o cliente precise sair de sua casa muitas vezes.

Em contrapartida, a utilização dessa tecnologia também apresenta desafios diante de situação de exclusão digital de muitos consumidores, em sua maioria idosos, que não possuem conhecimentos básicos sobre o uso de aplicativos bancários e a utilização da biometria facial, o que implica num impasse na aplicação desta tecnologia, uma vez que muitos a utilizam de forma indevida – em contratações equivocadas – ao mesmo passo que ficam vulneráveis a golpes, inclusive resultando em decisões judiciais que reconhecem fraudes mesmo em contratos que há a captura da biometria facial do consumidor hipervulnerável na situação (FIGUEIRA; COUTO, 2024).

4 SEGURANÇA CIBERNÉTICA E A RESPONSABILIDADE DAS INSTITUIÇÕES FINANCEIRAS

A segurança cibernética é um campo que busca proteger sistemas de informação contra acessos não autorizados e ataques maliciosos.

Segundo Pedroso (2023), diversos estudos apontam que o avanço tecnológico e a digitalização forçada pela pandemia impulsionaram o aumento de ataques cibernéticos e fraudes, afetando organizações em diferentes níveis e locais. Conforme destaca, o Brasil ocupa posição de destaque negativo nesse cenário, com um aumento expressivo nos ataques cibernéticos entre 2020 e 2022.

No contexto das instituições financeiras, a segurança cibernética é crucial, especialmente quando envolvem tecnologias como a biometria facial, ferramenta que pode ser alvo fácil de criminosos. Um exemplo disso são os casos que ocorrem frequentemente e já que se tornaram notícias na mídia, como uma simples “entrega de flores” que se tornou uma oportunidade para criminosos realizarem a captura da biometria facial da pessoa abordada e, assim, possuírem acesso aos dados bancários e a vida financeira da vítima (Terra, 2024).

A responsabilidade das instituições financeiras por falhas de segurança, como fraudes digitais, tem sido amplamente discutida na doutrina do direito do consumidor. Em muitos casos, a falta de adoção de medidas adequadas de proteção pode acarretar a responsabilização objetiva das instituições financeiras, conforme a Súmula 479 do Superior Tribunal de Justiça (STJ), que estabelece que as instituições financeiras respondem objetivamente pelos danos causados por fraudes em suas operações (STJ, 2012).

Nesse contexto, legislações, como a Lei Federal nº 14.063/2020, que regula o uso de assinaturas eletrônicas, incluindo a biometria facial, estabelecem normas sobre como as instituições financeiras devem adotar essas tecnologias, a fim de evitar vulnerabilidades e proteger os consumidores.

> Art. 3º Para os fins desta Lei, considera-se:
>
> I - autenticação: o processo eletrônico que permite a identificação eletrônica de uma pessoa natural ou jurídica;
>
> II - assinatura eletrônica: os dados em formato eletrônico que se ligam ou estão logicamente associados a outros dados em formato eletrônico e que são utilizados pelo signatário para assinar, observados os níveis de assinaturas apropriados para os atos previstos nesta Lei;
>
> III - certificado digital: atestado eletrônico que associa os dados de validação da assinatura eletrônica a uma pessoa natural ou jurídica;
>
> IV - certificado digital ICP-Brasil: certificado digital emitido por uma Autoridade Certificadora (AC) credenciada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na forma da legislação vigente.

O não cumprimento dessas normas pode implicar na responsabilização civil das instituições financeiras em casos de fraudes contra o consumidor, conforme consagrado no artigo 4º do Código de Defesa do Consumidor (CDC), que assegura a proteção contra práticas comerciais abusivas e exige que os fornecedores (nesse caso bancos e instituições financeiras) garantam a segurança das transações realizadas por seus clientes (Brasil, 1990).

A legislação brasileira de defesa do consumidor, por meio do Código de Defesa do Consumidor (CDC), é clara quanto à proteção do consumidor contra práticas abusivas e prejudiciais em relações de consumo. No ambiente digital, os consumidores estão sujeitos a riscos específicos, como fraudes digitais, que podem ser agravadas pela falta de compreensão da tecnologia por parte dos consumidores e pela inadequação das medidas de segurança adotadas pelas instituições financeiras.

A vulnerabilidade dos consumidores em transações bancárias digitais é amplificada quando se trata de grupos hipervulneráveis. Segundo Lopes e Rezende (2023), esses grupos enfrentam barreiras adicionais para entender e adotar novas tecnologias, o que os coloca em risco de serem alvo de fraudes. Assim, a proteção legal nesses casos deve ser ainda mais rigorosa, garantindo que as instituições financeiras adotem protocolos de segurança robustos e compreensíveis.

Além disso, as decisões judiciais sobre o uso da biometria facial nas contratações digitais devem observar as normas técnicas e legais relacionadas à segurança cibernética. De acordo com a Lei Federal nº 14.063/2020, é responsabilidade das instituições financeiras garantir a segurança das transações realizadas digitalmente, principalmente quando essas envolvem dados biométricos, como a face do consumidor. A falha em cumprir tais normas configura violação aos direitos do consumidor, sujeitando as instituições financeiras à responsabilidade civil por danos causados por fraudes (Ghani, 2023).

4.1 Lei Federal nº 14.063/2020 e Diretrizes do ITI e Dataprev

A aplicação dessas normas é uma exigência legal que visa proteger tanto as partes envolvidas nas transações (consumidores e bancos) quanto a integridade do próprio sistema financeiro. Contudo, há uma lacuna entre o que as normas técnicas prevêem e o que as instituições financeiras efetivamente implementam, o que resulta em vulnerabilidades e fraudes que prejudicam consumidores, principalmente os mais hipervulneráveis.

A adequação das instituições financeiras a essas normas técnicas é crucial para garantir a segurança dos consumidores e evitar a ocorrência de fraudes.

A Lei Federal nº 14.063 sancionada em setembro de 2020, representa um avanço significativo na regulamentação das assinaturas eletrônicas no Brasil, especialmente ao permitir sua utilização em interações com entes públicos, estabelecendo três níveis distintos de segurança: simples, avançada e qualificada.

> Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:
> I - assinatura eletrônica simples:
> a) a que permite identificar o seu signatário;
> b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;
> II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:
> a) está associada ao signatário de maneira unívoca;
> b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;
> c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;
> III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001. (BRASIL, 2020);

Embora a lei não trate diretamente da biometria facial, ela abre espaço para o uso de tecnologias que permitam autenticação com segurança adequada, desde que estejam em conformidade com os níveis estabelecidos. Essa abertura normativa tem permitido que mecanismos como o reconhecimento facial sejam incorporados a serviços públicos e privados, desde que respaldados por diretrizes técnicas específicas (Belli; Gaspar; Zingales, 2024).

Nesse contexto, o Instituto Nacional de Tecnologia da Informação (ITI), responsável pela infraestrutura de chaves públicas brasileiras (ICP-Brasil), e a Dataprev, empresa pública de tecnologia da informação vinculada ao Governo Federal, têm exercido papel crucial na

normatização e padronização do uso da biometria facial como forma de autenticação (Brasil, 2020; Dataprev, 2022; DOU, 2022).

Assim, o Decreto Federal nº 10.543/2020, que regulamenta a Lei Federal nº 14.063/2020, atribui aos órgãos e entidades públicas a competência para definir o nível mínimo de assinatura exigido, permitindo que a biometria facial seja adotada como fator de autenticação, desde que cumpra as exigências técnicas (Brasil, 2020).

Desse modo, a Nota Técnica nº 01/2022 da Dataprev (NT/DRN/001/2022), publicada em 14/12/2022, estabelece requisitos rigorosos para a utilização da biometria facial, como a captura de imagem de qualidade compatível com os padrões internacionais, que garantem nitidez e iluminação adequada; detecção de vivacidade, que busca evitar fraudes por uso de fotos ou vídeos; e a necessidade de validação cruzada com bases de dados oficiais, como os cadastros do Governo Federal (CTPS Digital, Meu INSS, CNH Digital, etc). A biometria deve, ainda, estar associada a um documento de identidade válido e recente, para que o reconhecimento facial seja considerado seguro e eficaz. Esses parâmetros visam garantir que a tecnologia seja aplicada com alto grau de confiabilidade e segurança, evitando fraudes e falsificações.

Nesse sentido, tribunais ao redor do Brasil tem utilizado a legislação e os parâmetros técnicos existentes para fundamentar decisões. Um exemplo disso é a decisão do Tribunal de Justiça do Estado de Goiás (TJ/GO), na Apelação Cível nº 5350176-65.2022.8.09.0149, que anulou o contrato de empréstimo objeto da lide e condenou a instituição financeira por danos morais em razão de falha na prestação de serviço e devolução dos valores indevidamente descontados, utilizando a Lei Federal nº 14.063/2020 como fundamento na decisão.

Na mesma senda, o Tribunal de Justiça do Estado de São Paulo (TJ/SP), na Apelação Cível nº 1000265-92.2024.8.26.0438, manteve a sentença que condenou o autor por litigância de má-fé, fundamentando que os contratos de empréstimo controvertidos estariam consoante a Lei Federal nº 14.063/2020, bem como em consonância com os padrões técnicos do Dataprev.

Na mesma linha, o Superior Tribunal de Justiça (STJ), no Recurso Especial nº 2150278 - PR, anulou o acórdão recorrido reconhecendo a validade da assinatura eletrônica no contrato discutido nos autos da ação, cuja fundamentação incluiu a Lei Federal nº 14.063/2020 para demonstrar que não é obrigatório uma assinatura digital em contrato bancário possuir certificado digital emitido por autoridade certificadora credenciada ao ICP – Brasil, conforme defendido pelo autor da ação. Ainda, a decisão mencionou que o documento contratual teria

como elemento válido de comprovação o endereço IP, hora, código *hash* e localização. Contudo, é necessário salientar que o STJ não possui jurisprudência pacificada sobre o tema.

A adoção da biometria facial nos serviços bancários representa uma inovação relevante, principalmente por ampliar o acesso da população aos serviços de maneira mais ágil e sem necessidade de deslocamento físico, o que se mostra especialmente importante em regiões distantes ou em contextos de vulnerabilidade social.

Contudo, é fundamental que a utilização da biometria facial ocorra de forma segura, transparente e em conformidade com os direitos fundamentais dos cidadãos, incluindo a proteção de dados pessoais, conforme previsto na Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018). O uso indiscriminado ou tecnicamente falho da biometria pode gerar consequências jurídicas graves, como fraudes, exclusão digital ou violação da privacidade, como já referido.

Portanto, é essencial que os órgãos públicos e privados invistam não apenas em infraestrutura tecnológica, mas também em treinamento, supervisão e auditoria constante dos sistemas utilizados. A Lei Federal nº 14.063/2020, aliada às diretrizes do ITI e da Dataprev, fornece a base normativa e técnica para que a biometria facial seja incorporada de maneira eficaz e responsável, permitindo avanços na digitalização dos serviços sem comprometer a segurança jurídica e a dignidade dos cidadãos.

5 HIPERVULNERABILIDADE DO CONSUMIDOR NO AMBIENTE DIGITAL

Santin (2023, p.38), em pesquisa publicada na Revista da Defensoria Pública do RS, afirma que “a internet das coisas e o uso da inteligência artificial fazem do consumidor digital um sujeito hipervulnerável”, vulnerável por ser consumidor e simultaneamente vulnerável ao contratar no meio digital. Em outras palavras, a tecnologia acentua ainda mais a fragilidade da parte mais fraca da relação de consumo.

As fraudes que atingem grupos vulneráveis — como idosos, pessoas com baixo letramento digital ou com limitações cognitivas — agravam esse quadro. É amplamente reconhecido que os idosos enfrentam dificuldades com tecnologia, maior isolamento social e, muitas vezes, dependência financeira, o que os torna alvos fáceis de práticas abusivas.

Sieradzki e Moreira (2021), na Revista Brasileira de Direito do Consumidor, afirmam que o superendividamento na velhice frequentemente decorre da contratação impensada de serviços por canais digitais ou telefônicos, em que há ausência de um controle institucional adequado. Além disso, práticas conhecidas como “padrões sombrios”, como técnicas de design

de interfaces que induzem o consumidor ao erro, tornam a experiência digital ainda mais arriscada.

Silva (2022), em sua pesquisa sobre persuasão digital e direito do consumidor, alerta que essas estratégias são amplamente utilizadas por *e-commerces* e plataformas digitais, dificultando o exercício do direito de escolha e obscurecendo informações essenciais. Essa manipulação acentua a vulnerabilidade informacional e técnica, especialmente de consumidores que não compreendem as complexidades tecnológicas, o que os coloca em situação de desvantagem ainda maior.

O impacto das fraudes digitais sobre grupos vulneráveis é profundo. Vai desde perdas financeiras até danos morais e emocionais, além do enfraquecimento da confiança no setor e no próprio sistema de proteção ao consumidor. No campo das fraudes bancárias, por exemplo, são comuns os casos de engenharia social, *phishing*, empréstimos indevidos e uso indevido de biometria facial.

Para enfrentar esse cenário, o ordenamento jurídico brasileiro precisa adotar medidas protetivas concretas e eficazes. O dever de informação deve ser reforçado com clareza, transparência e acessibilidade, principalmente quando a comunicação se dá com públicos vulneráveis. Nos contratos celebrados com idosos ou pessoas com baixo domínio digital, é essencial garantir condições específicas, como confirmação em etapas, tempo de reflexão e assistência técnica. A fiscalização contra padrões sombrios deve ser intensificada por órgãos como o Procon e o Ministério Público, e pode haver inclusive regulamentações específicas que proíbam práticas persuasivas e manipulações ocultas nas plataformas.

A LGPD, por sua vez, precisa ser aplicada com rigor, especialmente nos setores bancário e financeiro, responsabilizando objetivamente os fornecedores que não garantem a segurança dos dados de seus clientes. Ao lado disso, deve haver ações de educação digital voltadas para populações mais vulneráveis, permitindo que essas pessoas reconheçam tentativas de golpe, compreendam os riscos dos ambientes virtuais e saibam se proteger.

Diante disso, pode-se afirmar que a hipervulnerabilidade do consumidor digital exige uma abordagem integrada, que envolva tanto o direito quanto a tecnologia e a educação. As fraudes que atingem grupos vulneráveis expõem a urgência de políticas públicas eficazes, de fiscalização ativa e de medidas protetivas específicas. A combinação entre proteção de dados, educação digital e defesa coletiva dos consumidores representa um caminho viável e necessário para garantir que os direitos fundamentais do consumidor se mantenham eficazes diante das novas configurações digitais.

Nesse cenário, é essencial que o direito acompanhe as transformações da sociedade de forma sensível e humanizada, protegendo aqueles que mais necessitam.

6 ANÁLISE DAS DECISÕES JUDICIAIS DO TJRS

A metodologia adotada para a realização deste estudo foi dividida em etapas, englobando levantamento bibliográfico e análise documental.

O levantamento bibliográfico foi importante para resgatar conceitos pertinentes à responsabilidade civil das instituições financeiras, biometria facial, segurança cibernética no contexto bancário e à hipervulnerabilidade do consumidor no ambiente digital.

A revisão de literatura foi baseada em estudos acadêmicos sobre a temática e documentos técnicos de órgãos governamentais como o Instituto Nacional de Tecnologia da Informação (ITI) e a Empresa de Tecnologia e Informações da Previdência (Dataprev). O objetivo é estabelecer um embasamento teórico sobre o contexto da digitalização bancária, a adoção de biometria facial e os aspectos legais envolvidos.

A escolha das decisões foi feita por meio de pesquisa no site oficial do TJRS, utilizando as palavras-chave “biometria facial”, “fraude” e “contrato bancário”, limitando-se a seleção de Apelações por ser o recurso que busca reformar a decisão de primeiro grau. Ainda, foram selecionadas decisões que foram julgadas entre 2020 e 2024 por ser o período em que houve uma crescente na assinatura de contratações digitais em razão da Pandemia de Covid-19, sendo uma decisão de cada ano. Ademais, foram escolhidas somente decisões julgadas pelas câmaras cíveis responsáveis por julgar a matéria de negócios jurídicos bancários — 4ª Câmara Cível à 25ª Câmara Cível — conforme específica o Regimento Interno do TJ/RS (Tribunal de Justiça do Rio Grande do Sul, 2018).

A pesquisa realizada com base nas palavras-chave resultou em 66 (sessenta e seis) decisões encontradas até o mês de dezembro de 2024. Adotou-se como critério de amostragem julgados que versam sobre contratos de empréstimos consignados, considerando que é a modalidade de contrato com mais adesão dos consumidores bancários, especialmente os idosos, totalizando cinco decisões representativas a partir do ano 2020 até 2024. Salienta-se que a maioria das decisões na pesquisa realizada no site do TJ/RS versam sobre o mesmo tema, motivo pelo qual foram escolhidas as decisões que possuem uma diversidade temática que representam em grande parte a totalidade das decisões.

A análise buscou identificar a consistência das decisões escolhidas com as legislações em vigor, as normas técnicas e recomendações que regulamentam as assinaturas eletrônicas.

Dá analise realizada, foi elaborada uma tabela comparativa, a qual se encontra no Anexo 1, que expõe a síntese das decisões e análise da referência tecnológica mencionada no julgado.

A análise permitiu identificar uma linha interpretativa que oscila entre a validação da biometria facial como meio de assinatura contratual, desde que acompanhada de provas técnicas robustas, e a proteção do consumidor hipervulnerável diante de contratações feitas em contextos de desinformação, fraude ou indução ao erro. Destaca-se a aplicação recorrente dos artigos 6º, VIII, e 14 do Código de Defesa do Consumidor, bem como o princípio da boa-fé objetiva e da teoria do risco do empreendimento.

As decisões analisadas revelam que o TJRS reconhece a validade da biometria facial como instrumento de assinatura contratual eletrônica, desde que associada a elementos técnicos como geolocalização, trilha digital da contratação, endereço IP do dispositivo utilizado, documentação pessoal do cliente, e demais elementos formativos da biometria facial.

Contudo, a jurisprudência também demonstra forte inclinação à fundamentação das decisões com base Código de Defesa do Consumidor (CDC), visando a proteção do consumidor idoso ou hipervulnerável, admitindo nulidade contratual quando houver evidência de indução, ausência de informação adequada ou falha na segurança da contratação. Há especial atenção à inversão do ônus da prova, que tem sido deferida mesmo diante de contratações tecnológicas, considerando a vulnerabilidade informacional e tecnológica do consumidor.

Nesse cenário, ainda se verifica que a legislação pertinente sobre a temática — Lei Federal nº 14.063/2020 — bem como a Norma Técnica do Dataprev (NT/DRN/001/2022) e recomendações do ITI não são mencionadas na fundamentação das decisões, muito embora haja nas decisões a menção de existência ou não de elementos como geolocalização, cópia de documentos pessoais, endereço IP, etc, requisitos estes presentes na lei, normas e recomendações acima referidas.

Com isso, o TJRS equilibra inovação contratual e proteção jurídica no ambiente digital no que se refere às decisões que envolvem contratos bancários digitais, consolidando um entendimento legal sobre as relações de consumo, utilizando majoritariamente princípios do CDC e de forma indireta requisitos técnicos para a análise da biometria facial, demonstrando uma limitação entre o conhecimento técnico e a aplicação jurídica.

7 ESTUDO COMPARATIVO: NORMAS TÉCNICAS X DECISÕES JUDICIAIS

O estudo comparativo entre as normas técnicas e as decisões judiciais evidencia uma lacuna notável na aplicação prática das diretrizes de segurança diante de contratações bancárias digitais. Entende-se como lacuna porque a Nota Técnica do Dataprev nº 01/2022 não possui força de lei, o que resulta em certa fragilidade em sua aplicação, tanto no âmbito administrativo das operações financeiras quanto na sua utilização como fundamento jurídico. Isso evidencia a necessidade de que a norma seja convertida em lei, conferindo-lhe maior segurança e obrigatoriedade.

Os requisitos técnicos do Dataprev, por exemplo, em contratações de crédito consignado definem padrões rigorosos para imagem facial, detecção de vivacidade e qualidade de dados biométricos:

> **Requisitos Técnicos para Integração da Solução de Biometria no Processo de Concessão de Empréstimo Consignado**
>
> [...]
>
> Sobre o processo de contratação:
>
> I – Mecanismo que possibilite detectar se o documento foi alterado depois de assinado;
>
> **II - Captura biométrica com garantia de vivacidade (liveness). A solução de liveness deverá implementar o nível iBeta2 e dentro dos padrões definido no IEEE Std 2790- 2020 – Standard for Biometric Liveness Detection, além da ISO/IEC 30.107-3, referente aos testes para detecção de possíveis ataques;**
>
> **III - A captura de biometria facial deve ser capaz de capturar a imagem facial com qualidade mínima de acordo com a ISO/IEC 29.794-5, levando em consideração aspectos como taxa de compressão, nitidez e luminosidade mínima, entre outros;**
>
> [...]
>
> **VIII - O processo de assinatura deverá incluir a localização da operação e o controle de data e hora da assinatura (timestamp);**
>
> IX - O registro biométrico utilizado deverá ser disponibilizado junto ao instrumento contratual que aplicou a biometria para apoiar a assinatura no padrão 2D. Quando a validação se der a partir de um documento com foto, o documento scaneado deverá ser igualmente disponibilizado. A qualidade dos documentos e registros biométricos devem ser suficientes para permitir futura auditoria do processo e batimento entre o rosto utilizado na identificação no momento da autenticação biométrica e aqueles presentes em bases biométricas e/ou documentais onde ocorrerá a conferência da solução;
>
> X - A biometria capturada na operação de assinatura deverá ser utilizada exclusivamente para este processo; (DATAPREV, 2022, p. 5-6, grifo nosso).

A Lei Federal nº 14.063/2020, representou um importante avanço no Brasil ao estabelecer critérios para o uso de assinaturas eletrônicas. Essa norma reconhece a validade da biometria facial como forma de assinatura eletrônica simples, desde que seja garantida a autenticidade do signatário e a integridade do documento. O Decreto Federal nº 10.543/2020

que regulamenta a aplicação dessa lei, reforça a necessidade de adoção de mecanismos de segurança digital, como geolocalização, trilhas de auditoria e detecção de vivacidade (*liveness*), principalmente em contextos que envolvem a celebração de contratos à distância, ou seja, em local diverso da instituição financeira.

Além da legislação supra, a Dataprev estabeleceu parâmetros técnicos complementares, exigindo conformidade com padrões internacionais como a norma ISO/IEC 19794-5, que define a qualidade da imagem facial, e a norma IEEE 2790-2020, que trata da verificação de vivacidade. Tais requisitos são fundamentais para assegurar que a biometria facial seja utilizada de maneira técnica, confiável e auditável.

O Instituto Nacional de Tecnologia da Informação (ITI), por sua vez, recomenda que para que a biometria facial seja considerada juridicamente válida ela esteja vinculada a elementos de autenticação seguros e tecnicamente robustos, como logs, metadados e a vinculação com um certificado digital da ICP-Brasil, nos casos em que se exige assinatura qualificada. Inclusive, o ITI possui um Guia de Orientação aos Desenvolvedores para que a arquitetura dos programas de assinatura digital (e biométrica) sejam passíveis de validação na plataforma governo sob domínio deste Instituto, e assim acrescentar um grau de confiabilidade no documento (Instituto Nacional de Tecnologia da Informação, 2022).

Ao se comparar essas exigências normativas e técnicas com as decisões judiciais analisadas no âmbito do TJRS, observa-se uma aplicação ainda limitada e variável dos dispositivos legais e das normas técnicas no julgamento de litígios envolvendo contratos celebrados com biometria facial, o que é surpreendente tendo em vista a postura vanguardista do TJRS em vários outros temas e sua posição de destaque no cenário nacional.

Na Apelação Cível nº 5002327-05.2020.8.21.5001, a 24ª Câmara Cível manteve a condenação do banco réu, com base na existência de geolocalização da biometria facial (aceite e captura) em duas cidades diversas no mesmo lapso temporal, além da existência de dois endereços IPs empregados na contratação, demonstrando a fraude sofrida pela consumidor. No entanto, embora o argumento utilizado demonstre terem sido analisados os padrões de conformidade para uma biometria facial, não houve qualquer menção à legislação ou às recomendações do ITI (Tribunal de Justiça do Rio Grande do Sul, 2021).

Na Apelação Cível nº 5018602-20.2023.8.21.0023, da 24ª Câmara Cível, ainda que a contratação tenha sido anulada, a fundamentação também não abordou as exigências técnicas estabelecidas pela legislação e pelas normas institutos governamentais. O caso foi tratado com base exclusivamente nos princípios gerais do CDC, sem a referência expressa à Lei 14.063 ou aos padrões do ITI e Dataprev (Tribunal de Justiça do Rio Grande do Sul, 2024).

Já na Apelação Cível nº 5002727-56.2021.8.21.0095, da 16ª Câmara Cível, houve o reconhecimento da nulidade de contrato firmado por meio de biometria facial em que o consumidor idoso foi induzido a erro. A decisão enfatizou o vício de consentimento e a responsabilidade objetiva do fornecedor, com base no CDC, mas também deixou de abordar se a contratação cumpriu ou não os critérios técnicos definidos pelas normas do ITI e da Dataprev (Tribunal de Justiça do Rio Grande do Sul, 2023).

No caso da Apelação Cível nº 5006524-78.2019.8.21.0008, da 19ª Câmara Cível, a contratação foi considerada válida, com base na apresentação de logs e informações de acesso, mas, novamente, não se verificou se tais elementos estavam conforme a legislação federal sobre o tema ou com as recomendações do ITI, conforme as normas técnicas discutidas (Tribunal de Justiça do Rio Grande do Sul, 2022).

Por fim, na Apelação Cível nº 5003530-32.2019.8.21.0023, a 11ª Câmara Cível reforçou que a prova de biometria facial — embora com fotografia do cliente e formulários eletrônicos — apresentada pela instituição financeira ré não apresentou vínculo com os contratos controvertidos, declarando nulidade nas contratações. Contudo, apesar de mencionar a responsabilidade objetiva da instituição ré com base no CDC, deixou de enfrentar a legislação federal aplicável e as recomendações do ITI (Tribunal de Justiça do Rio Grande do Sul, 2020).

O que se observa a partir desses julgados é que, embora haja uma certa sensibilidade do TJRS em proteger o consumidor e em reconhecer a complexidade das contratações digitais, as decisões não mencionam explicitamente a Lei Federal nº 14.063/2020, tampouco o Decreto Federal nº 10.543/2020, ou as normas técnicas do Dataprev e recomendações do ITI.

A falta de referência a esses parâmetros evidencia uma falta de aplicação da legislação vigente (Lei Federal nº 14.063/2020) no Poder Judiciário gaúcho, bem como revela uma lacuna diante da inexistência de legislação que estabeleça requisitos técnicos como aqueles definidos pela Nota Técnica nº 01/2022 da Dataprev.

Em termos práticos, isso significa que contratos firmados com biometria facial têm sido validados ou invalidados sem que o tribunal verifique se os requisitos técnicos mínimos foram de fato cumpridos, o que pode comprometer a segurança jurídica das relações digitais bancárias. Ainda que as decisões se aproximem de uma análise técnica ao reconhecer a importância de geolocalização, dos logs ou da trilha digital, o Poder Judiciário do TJ/RS ainda não adotou uma linha uniforme que integre as normas técnicas como parte da prova obrigatória para validar contratações biométricas.

Diante disso, uma solução viável é que o Poder Judiciário do TJ/RS passe a exigir expressamente que as provas de contratação eletrônica com biometria facial estejam

acompanhadas de elementos que sigam os padrões estabelecidos nas legislações sobre o tema e nas normas técnicas dos órgãos federais, como detecção de vivacidade, qualidade da imagem, metadados do dispositivo, localização geográfica e cruzamento com base de dados oficial. Além disso, é fundamental que a perícia técnica, quando requisitada, seja realizada por profissionais capacitados e com base nesses parâmetros objetivos.

Outro passo importante seria a capacitação dos magistrados e operadores do direito em relação às exigências técnicas que regem as autenticações biométricas, permitindo uma análise mais rigorosa das provas apresentadas. O alinhamento entre a legislação técnica, os padrões normativos e as decisões judiciais é essencial para garantir a proteção do consumidor no ambiente digital, especialmente os mais vulneráveis, como idosos e pessoas com baixa familiaridade com tecnologia. Esse alinhamento não apenas fortalece a confiança nas ferramentas digitais, como também assegura que a inovação tecnológica não seja usada como instrumento de abuso ou de exclusão, mas sim como meio de inclusão segura, responsável e juridicamente válida.

8 DISCUSSÃO

A análise da biometria facial em contratos digitais revela uma complexa relação entre as normas legais e técnicas e sua efetiva aplicação prática. Embora a Lei Federal nº 14.063/2020, a norma regulatória da Dataprev e recomendações do ITI definam critérios importantes de segurança, o que se observa nas decisões analisadas do TJRS é a quase total ausência de menção direta a essas exigências.

Como já referido, as decisões geralmente baseiam-se em princípios gerais do CDC e aceitam provas frágeis, como "*prints de telas*" ou "*selfies*", sem que se exija comprovação técnica robusta, o que compromete a segurança jurídica das contratações realizadas por meio de reconhecimento facial.

Do ponto de vista tecnológico, a adoção isolada da *selfie*, sem validação técnica de vivacidade ou conformidade com padrões de qualidade de imagem facial, expõe os sistemas a vulnerabilidades graves e não são suficientes para comprovar uma suposta contratação no contexto bancário.

Observa-se que "há uma controvérsia entre o motivo da implementação de sistemas biométricos em utilitários para a proteção da identidade de seus usuários e a segurança dos dados biométricos armazenados", chamando atenção para os riscos de vazamentos, fraudes e uso indevido dos dados biométricos caso os processos não sejam auditáveis nem padronizados (Souza, 2020, p. 95).

Ainda, a ausência de requisitos técnicos adequados pode transformar o uso da biometria um fator de risco ao invés de proteção, principalmente se o sistema não for capaz de detectar vivacidade e se não houver validação cruzada com bases oficiais (Mello; Serra, 2023), como no sistema de validação oferecido pelo ITI, por exemplo.

O uso indiscriminado da biometria facial, sem a observação de normas técnicas previstas, como a NT/DRN/001/2022 emitida pela Dataprev, torna-se ainda mais problemático quando se trata de consumidores hipervulneráveis, como idosos e pessoas com baixa familiaridade digital, que dificilmente conseguem compreender ou verificar a autenticidade das etapas do contrato eletrônico.

Esse descompasso entre a tecnologia disponível, as exigências legais e a atuação do TJ/RS revelam a necessidade de medidas mais firmes para fortalecer a segurança jurídica nessas relações. É indispensável que as provas digitais apresentadas nos processos — especialmente quando envolvem biometria facial — venham acompanhadas de elementos técnicos robustos e auditáveis, tais como logs de acesso, geolocalização, data e hora da contratação, verificação de vivacidade, vinculação da imagem facial a documentos oficiais e trilha digital da contratação.

Da mesma forma, é necessário que o TJ/RS passe a exigir perícia técnica nos casos de contestação de autenticidade contratual, com base na legislação vigente e em padrões estabelecidos por órgãos técnicos como o ITI e a Dataprev.

Além disso, é fundamental que magistrados e operadores do direito sejam capacitados para interpretar essas provas digitais com base em critérios objetivos, superando a atual falta de aplicação da legislação aplicável ao tema e a ausência de legislação técnica pertinente que muitas vezes impede a análise qualificada da biometria facial. O próprio Conselho Nacional de Justiça pode contribuir com essa mudança, promovendo diretrizes sobre como julgar casos que envolvem autenticação biométrica, criando protocolos padronizados e recomendando exigências mínimas de documentação técnica.

A partir dessa integração entre direito e tecnologia, será possível consolidar uma prática jurídica mais segura e coerente com a complexidade dos contratos digitais bancários, reduzindo as incertezas e garantindo maior proteção ao consumidor. Esse alinhamento é especialmente importante para garantir que a inovação não se torne um instrumento de insegurança ou exclusão, mas sim de fortalecimento das garantias contratuais, da confiança nas plataformas digitais e da efetividade dos direitos fundamentais.

9 CONSIDERAÇÕES FINAIS

Este trabalho teve como principal objetivo analisar como o Tribunal de Justiça do Rio Grande do Sul tem julgado os casos de fraudes envolvendo a biometria facial em contratos bancários digitais, especialmente no período da pandemia e após, com o aumento da digitalização das relações de consumo.

Para isso, buscou-se compreender, à luz da doutrina, da legislação e das normas técnicas, como o uso da biometria tem sido regulamentado e aplicado na prática, além de identificar se há coerência entre a tecnologia utilizada e a proteção dos direitos do consumidor, sobretudo os mais vulneráveis.

Após o estudo teórico e a análise das decisões judiciais selecionadas, conclui-se que os objetivos propostos foram alcançados. A pesquisa permitiu identificar uma tendência importante: embora o TJ/RS reconheça a responsabilidade das instituições financeiras em muitos casos de fraude, especialmente quando o consumidor é idoso ou hipervulnerável, as decisões raramente fazem referência direta às normas técnicas que regulam o uso da biometria facial, como as recomendações da Dataprev, do ITI ou a Lei Federal nº 14.063/2020.

Percebe-se, portanto, um certo caráter pedagógico da decisão, pois os julgamentos utilizam critérios do Código de Defesa do Consumidor e protegem o consumidor, bem como em última análise observam parâmetros técnicos para a biometria facial, mas não exigem das instituições financeiras o cumprimento de tais parâmetros técnicos básicos para garantir a segurança dessas contratações. Além disso, as decisões não mencionam a Lei Federal 14.063/2020, tampouco a Norma Técnica do Dataprev e recomendações do ITI. Essa ausência de exigência acaba enfraquecendo a proteção que deveria ser assegurada pela justiça.

Também foi possível verificar a possibilidade de contratos serem validados apenas com base em *prints* de telas ou *selfies*, sem a devida análise técnica sobre a autenticidade daquela biometria. Isso é especialmente preocupante quando se considera que o público mais afetado por essas fraudes são pessoas que já enfrentam dificuldades com o mundo digital, como idosos, analfabetos e pessoas com deficiência.

A pesquisa reforça que o uso da biometria facial nos bancos pode, sim, ser uma ferramenta segura e útil, mas somente se for usada com responsabilidade, dentro de critérios técnicos rigorosos e com respeito aos direitos do consumidor. Quando isso não acontece, a tecnologia, em vez de proteger, passa a ser um risco.

Por fim, este trabalho mostra que ainda há um caminho importante a ser percorrido pelo Poder Judiciário do TJRS no que se refere à integração entre direito e tecnologia. É fundamental que as decisões sejam embasadas não apenas na legislação do consumidor, mas também na

legislação e nas normas técnicas específicas que regem as contratações digitais, as quais vem ocorrendo com cada vez mais frequência no mundo atual. Com isso, será possível construir um ambiente mais seguro, justo e equilibrado para todos, especialmente para quem mais precisa de proteção.

REFERÊNCIAS

BRASIL, R. F. DO. DECRETO Nº 10.543, DE 13 DE NOVEMBRO DE 2020. 13 nov. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10543.htm. Acesso em: 05 mai. 2025.

BRASIL, R. F. DO. LEI Nº 14.063, DE 23 DE SETEMBRO DE 2020. 23 set. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm.

BRASIL, R. F. DO. Instituto Nacional de Tecnologia da Informação. Instrução Normativa ITI nº 09, de 30 de junho de 2020: aprova a versão 2.2 do DOC-ICP-05.03 - Requisitos mínimos para coleta biométrica presencial na ICP-Brasil. Brasília, DF: ITI, 2020. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/instrucoes-normativas/IN2020_09_DOCICP05.03_compilada.pdf. Acesso em: 07 jul. 2025.

BRASIL, R. F. DO. INSTITUTO NACIONAL DE TECNOLOGIA DE INFORMAÇÃO. Guia de boas práticas. Disponível em: https://validar.iti.gov.br/guia.html. Acesso em: 01 jun. 2025.

CEBRIAN, Fabiana S. P. Faraco et al. Radar Tecnológico. Biometria e reconhecimento facial: estudos preliminares. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd.pdf. Acesso em: 16 abr. 2025.

DA SILVA, M. R. Hipervulnerabilidade digital do consumidor e padrões sombrios no e-commerce: entre persuasão e manipulação. *Revista Jurídica da Escola do Poder Judiciário do Acre*, v. 1, n. 3, p. 55–78, 2022. Disponível em: https://periodicos.tjac.jus.br/index.php/esjudtjac/article/view/25?utm_. Acesso em: 03 abr. 2025.

DATAPREV. Requisitos Técnicos - Solução de Biometria no Processo de Concessão de Empréstimo Consignado: NT/DRN/001/2022. [s.l: s.n.]. Disponível em: https://docs.dataprev.gov.br/wp-content/uploads/2023/02/202200036965_Requisitos%20Tecnicos-Solucao-de-Biometria-no-Processo-de-Concessao-de-Emprestimo-Consignado-1.pdf. Acesso em: 15 mar. 2025.

DE SOUZA, M. A. A Biometria e suas Aplicações. *Revista Brasileira de Ciências Policiais*, v. 11, n. 2, p. 79–102, 2020. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/710. Acesso em: 03 abr. 2025.

FEBRABAN (Brasil). Deloitte. Pesquisa Febraban de Tecnologia Bancária. **Febraban**, [*s. l.*], v. 2, 2025. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_2.pdf. Acesso em: 20 maio 2025.

FEBRABAN TECH. Disponível em: https://febrabantech.febraban.org.br/especialista/patricia-peck-pinheiro/biometria-facial-utilizacao-por-instituicoes-financeiras-na-prevencao-a-fraudes. Acesso em: 02 jun. 2025.

FELIPE, H.; MARQUETTI, F.; PRETO, O. Universidade Federal de Ouro Preto. Escola de Direito, Turismo e Museologia - Departamento de Direito. *A responsabilidade por fortuito interno em razão das fraudes em empréstimos realizados por idosos mediante aceite por biometria facial*. [s.l: s.n.]. Disponível em: https://monografias.ufop.br/bitstream/35400000/5952/1/MONOGRAFIA_ResponsabilidadeFortuitoInterno.pdf. Acesso em: 28 mai. 2025.

FIGUEIRA, H. L. M.; FRANÇACOUTO, L. A (Hiper) Vulnerabilidade do Consumidor Idoso nos Contratos Eletrônicos: Desafios e Perspectivas. *Revista Veritas de Difusão Científica*, p. 1078–1111, 12 ago. 2024. Disponível em: https://revistaveritas.org/index.php/veritas/article/view/138/242. Acesso em: 02 abr. 2025.

ITI – Instituto Nacional de Tecnologia da Informação. Instrução Normativa ITI nº 24, de 27 de maio de 2022 – altera DOC-ICP-05.03 (Procedimentos para identificação biométrica na ICP-Brasil). **Diário Oficial da União**, Brasília, 27 maio 2022. Disponível em: https://in.gov.br/web/dou/-/instrucao-normativa-iti-n-24-de-27-de-maio-de-2022-403689935 Acesso em: 07 jul. 2025.

ITI – Instituto Nacional de Tecnologia da Informação. **A biometria na ICP-Brasil**. Notícia publicada em 29 jun. 2016 (atualizada em 31 out. 2022). Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/indice-de-noticias/a-biometria-na-icp-brasil. Acesso em: 07 jul. 2025.

MELO, P. V.; SERRA, P. Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. *Comunicação e sociedade*, v. 42, p. 205–220, 2022. Disponível em: https://scielo.pt/scielo.php?pid=S2183-35752022000200205&script=sci_arttext&utm_source=. Acesso em: 03 abr. 2025.

MENEZES, G. W. A ação do uso da inteligência artificial e microfeições faciais para mitigar os riscos de deepfakes para a autenticação por biometria facial no setor financeiro brasileiro. *Repositorio.esg.br*, 2024. Disponível em: https://repositorio.esg.br/handle/123456789/1965?locale=pt_BR. Acesso em: 28 mai. 2025.

MENEZES, G. et al. Escola Superior de Guerra. *A ação do uso da inteligência artificial e microfeições faciais para mitigar os riscos de deepfakes para a autenticação por biometria facial no setor financeiro brasileiro*. [s.l: s.n.]. Disponível em: https://repositorio.esg.br/bitstream/123456789/1965/1/GEORGE%20WASHINGTON%20MENEZES.pdf. Acesso em: 16 abr. 2025.

PEDROSO, I. F. Análise de casos fraudulentos de segurança cibernética em organizações. 2023. *Trabalho de Concluso de Graduação*. Universidade Federal do Rio Grande do Sul (UFRGS). Disponível em: <https://lume.ufrgs.br/handle/10183/266920>. Acesso em: 20 abr. 2025.

Pesquisa Febraban de Tecnologia Bancária. [s.l: s.n.]. Disponível em: <https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_01%20-%205.pdf>. Acesso em: 18 maio. 2025.

Pesquisa Febraban de Tecnologia Bancária. [s.l: s.n.]. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%20-%20Vol_02%20-%20Imprensa.pdf.

BELLI, Luca; GASPAR, Walter Britto; ZINGALES, Nicolo. *Regulating facial recognition in Brazil*. In: BEDUSCHI, Ana (org.). *The Cambridge handbook of facial recognition in the modern state*. **Cambridge: Cambridge University Press**, 2024. p. 228-241. Disponível em: https://www.researchgate.net/publication/379369496_Regulating_Facial_Recognition_in_Brazil. Acesso em: 09 jul. 2025.

ROBERTO, D. A hipervulnerabilidade digital do consumidor diante do comércio eletrônico, da inteligência artificial e da internet das coisas. *Revista da Defensoria Pública do Estado do Rio Grande do Sul*, v. 2, n. 33, p. 22–43, 2023. Disponível em: https://revista.defensoria.rs.def.br/defensoria/article/view/548?utm_source. Acesso em: 02 abr. 2025.

ROSENVALD, N. Responsabilidade civil e solidariedade social: potencialidades de um diálogo. [s.l: s.n.]. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/cc20%20correto.pdf?d=636808287111878095. Acesso em: 07 abr. 2025.

SANTOS, A. S. V. P. Universidade de Évora - Escola de Ciências Sociais. [s.l: s.n.]. Disponível em: https://dspace.uevora.pt/rdpc/bitstream/10174/32406/1/Mestrado-Economia_e_Gestao_Aplicadas_Economia_e_Gestao_para_Negocios-Abdulay_Seydo_Vaz_Pires_dos_Santos.pdf. Acesso em: 17 abr. 2025.

SIERADZKI, L. M.; MOREIRA, V. V. Superendividamento: Análise acerca da hipervulnerabilidade do consumidor idoso. *Academia de Direito*, v. 3, p. 73–97, 2021. Disponível em: https://www.periodicos.unc.br/index.php/acaddir/article/view/3129?utm_source. Acesso em: 02 abr. 2025.

SOARES, D. V.; DE CARVALHO, E. B. P. Fraudes em contratos eletrônicos de empréstimos bancários: vulnerabilidade do consumidor, inteligência artificial e prova pericial em sistemas de biometria. *Revista Pensamento Jurídico*, ago. 2023. Disponível em: https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/813/645. Acesso em: 18 abr. 2025.

TERRA, Redação. Quadrilha usava flores e reconhecimento facial para aplicar golpes de R$ 70 mil: entenda. *Terra*, São Paulo, 8 abr. 2024. Disponível em: https://www.terra.com.br/economia/nao-caia-nessa/quadrilha-usava-flores-e-reconhecimento-facial-para-aplicar-golpes-de-r-70-mil-entenda,4daa398b8e7d4c71004faccd18cecf7124xz5ctw.html. Acesso em: 09 jul. 2025.

ANEXO 1. Análise comparativa de Apelações Cíveis do TJRS

Nº do Processo	Data do Julgamento	Câmara Cível	Síntese da Decisão	Análise da Referência Tecnológica
5018602-20.2023.8.21.0023	18/12/2024	24ª Câmara Cível	Sentença manteve inexistência do débito e dano moral de R$ 5.000,00. Apelo do autor improvido.	Não há menção à tecnologia empregada na biometria facial. A decisão trata da ausência de consentimento claro, mas não menciona a inexistência de requisitos técnicos na assinatura biométrica realizada, como logs, geolocalização ou padrões técnicos de autenticação, e, portanto, não faz referência às normas técnicas da Dataprev, recomendações do ITI e tampouco à Legislação sobre o tema
5002727-56.2021.8.21.0095	14/12/2023	16ª Câmara Cível	Contrato anulado por vício de consentimento. Dano moral de R$ 10.000,00.	A decisão enfatiza a vulnerabilidade do consumidor idoso, mas não há nenhuma menção às normas técnicas da Dataprev, recomendações do ITI e tampouco à Legislação sobre o tema
5006524-78.2019.8.21.0008	30/09/2022	19ª Câmara Cível	Contratação por biometria facial validada. Improcedência mantida.	A decisão menciona que o banco apresentou “prints” de sistema interno e supostos registros de acesso, mas não há referência direta à existência de elementos técnicos nos contratos, previstos na Legislação sobre o tema e nas recomendações do ITI.
5002327-05.2020.8.21.5001	29/09/2021	24ª Câmara Cível	Decisão manteve a sentença, determinando a rescisão do contrato, a devolução dos valores indevidamente depositados na conta da vítima e vedando o nome desta no rol de inadimplentes.	A decisão menciona que o banco réu apresentou aceite de captura de biometria facial e captura facial, ambos em um minuto de diferença em endereços distintos, bem como utilizando dois aparelhos eletrônicos para a contratação, tendo em vista os endereços IPs diferentes registrados no contrato. Destacou que a mera posse de uma foto não configura aceite de contratação. Contudo, a decisão não faz referência à Legislação sobre o tema, tampouco às recomendações do ITI.
5003530-32.2019.8.21.0023	23/11/2020	11ª Câmara Cível	Banco condenado à devolução de valores por falha na prova de contratação.	O acórdão descreve que a instituição apresentou reprodução de fotografia e formulários eletrônicos com dados ilegíveis que sequer indicam a quais contratos se relacionam. Assim, o Tribunal entendeu que isso não comprova a validade da contratação. Apesar disso, também a decisão não faz referência à Legislação sobre o tema e às recomendações do ITI.

Fonte: Elaborado pela autora (2025).