AMANDA MACIEL RIBEIRO

# RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS EM CASOS DE FRAUDES BANCÁRIAS:

## Análise Jurídica e Perspectivas de Proteção ao Consumidor.

CURSO DE DIREITO – UniEVANGÉLICA

2024

AMANDA MACIEL RIBEIRO

# RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS EM CASOS DE FRAUDES BANCÁRIAS: Análise Jurídica e Perspectivas de Proteção ao Consumidor.

Monografia apresentado ao Núcleo de Trabalho Científico do curso de Direito da Universidade Evangélica, como exigência parcial para a obtenção do grau de bacharel em Direito, sob orientação da professora M.e. Ana Paula M. Ferreira Russo.

ANÁPOLIS – 2024

AMANDA MACIEL RIBEIRO

# RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS EM CASOS DE FRAUDES BANCÁRIAS: Análise Jurídica e Perspectivas de Proteção ao Consumidor.

Anápolis, 06 de junho de 2024.

BANCA EXAMINADORA

_____

_____

# AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão à minha professora orientadora pelo suporte e orientação essenciais ao longo deste trabalho.

Agradeço a Deus pela força e sabedoria concedidas durante todo o processo.

À minha família, meu agradecimento especial pelo apoio incondicional e encorajamento constantes.

# RESUMO

Este trabalho aborda a responsabilidade das instituições financeiras diante de fraudes bancárias. O estudo explora as obrigações legais dessas instituições na prevenção, detecção e mitigação dos impactos dessas fraudes, destacando a responsabilidade objetiva prevista na legislação brasileira. A pesquisa inclui uma análise das excludentes de responsabilidade e discute a importância e formas de engenharia social na perpetração de golpes. Além disso, o trabalho apresenta uma análise jurisprudencial, o qual enfatiza a proteção ao consumidor e as vulnerabilidades nas relações bancárias, bem como, traz casos emblemáticos de decisões do Superior Tribunal de Justiça (STJ) sobre a responsabilidade objetiva dos bancos por danos causados por terceiros e é destacada a necessidade de medidas preventivas eficazes para proteger os consumidores.



**Palavras-chave:** Responsabilidade Civil. Fraude. Engenharia Social.

# SUMÁRIO

# INTRODUÇÃO

A responsabilidade civil das instituições financeiras em casos de fraudes bancárias tem se tornado um tema de crescente importância e complexidade no direito contemporâneo, especialmente devido à rápida digitalização dos serviços financeiros. Isso se dá em virtude da inovação tecnológica no setor bancário, que trouxe consigo uma série de benefícios, como a facilidade e rapidez nas transações, mas também abriu espaço para a proliferação de práticas fraudulentas que colocam em risco a segurança dos consumidores e a integridade das operações financeiras.

O advento da tecnologia e a crescente utilização de plataformas digitais para a realização de operações bancárias criaram um ambiente propício para fraudes, onde criminosos aproveitam vulnerabilidades nos sistemas de segurança para obter ganhos ilícitos. Esta situação exige uma análise crítica das obrigações legais das instituições financeiras na prevenção, detecção e mitigação dos impactos decorrentes de tais eventos. Com isso, legislação brasileira, incluindo o Código de Defesa do Consumidor e o Código Civil, junto com a jurisprudência vigente, fornece uma base normativa crucial para abordar essas questões.

A transformação digital dos serviços bancários, impulsionada por inovações como o Pix e a expansão das *FinTechs*, trouxe novos desafios em termos de segurança e regulação. Com a crise financeira de 2008-2009, que evidenciou falhas significativas na gestão de riscos e na regulamentação financeira, reforçou a necessidade de aprimorar as políticas de segurança e os mecanismos de proteção ao consumidor. Neste contexto, o Banco Central do Brasil e outras entidades reguladoras desempenham um papel vital na definição e fiscalização dos padrões de segurança.

Esse trabalho visa explorar de forma detalhada e crítica as responsabilidades das instituições financeiras frente às fraudes bancárias, avaliando

os mecanismos legais e regulatórios existentes e as práticas adotadas para proteger os consumidores.

A análise incluirá uma revisão da literatura jurídica, estudo de casos e interpretação das normas vigentes, com o objetivo de esclarecer os limites e as extensões da responsabilidade civil das instituições financeiras. Outrossim, serão abordados conceitos fundamentais como o nexo causal, o dano e a culpa, e como esses elementos são aplicados em casos concretos de fraudes bancárias.

Além disso, serão discutidas as excludentes de responsabilidade e os mecanismos de segurança que podem ser implementados para mitigar os riscos de fraude. No mesmo viés, a responsabilidade objetiva das instituições financeiras, conforme estabelecido na Súmula 479 do Superior Tribunal de Justiça (STJ), e a aplicabilidade do Código de Defesa do Consumidor à essas entidades são aspectos centrais deste estudo.

A importância deste trabalho reside na necessidade de assegurar uma proteção eficaz aos consumidores contra fraudes bancárias e de garantir que as instituições financeiras cumpram suas obrigações legais de maneira adequada. Ao explorar essas questões, espera-se contribuir para um entendimento mais profundo e atualizado das responsabilidades e das medidas de segurança que permeiam o setor financeiro, promovendo um ambiente mais seguro e confiável para todos os envolvidos. A análise crítica apresentada visa fomentar um debate fundamentado sobre as melhores práticas e políticas para enfrentar os desafios impostos pela digitalização dos serviços bancários e garantir a proteção dos direitos dos consumidores.

# CAPÍTULO I – RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS

Busca-se no presente capítulo abordar o conceito e as complexidades envolvidas na responsabilidade civil das instituições financeiras diante de casos de fraudes bancárias. A digitalização dos serviços financeiros desenvolve um ambiente propício para práticas fraudulentas, exigindo uma análise crítica das obrigações legais das instituições financeiras na prevenção, detecção e mitigação dos impactos decorrentes de tais eventos, principais mecanismos de segurança e procedimentos e controles norteados pelo Banco Central do Brasil.

## 1.1 Conceito e noções gerais

A responsabilidade civil sempre trouxe a noção de recomposição de dano ou prejuízo e tem suas origens desde os primórdios da humanidade, cravada na vingança privada e pleiteada pela vingança, sem qualquer noção estatal. Subsequente, a mesma vingança passa a ter relações jurídicas e intervenção do Estado, com condições estabelecidas pelo governante, como o Código de Hamurabi, regido pelas Leis de Talião: olho por olho, dente por dente (Souza, 2009).

Nesse viés, para Giselda Hinoraka (2005), o Código de Hamurabi é talvez a mais antiga legislação da humanidade e reafirma como a justiça baseada na vingança está instaurado desde os povos mais antigos. Assim, surgia-se o domínio do Estado e a decisão do poder público, sendo cabível a execução da vingança à vítima.

Posteriormente, no Direito Romano passa-se à concepção da obrigação civil relacionada a ideia aquiliana, ou seja, a culpa não é um elemento fundamental, e sim a causalidade em relação a ação pelo descumprimento de um dever legal (Correa, 1973). Alvino Lima (1999), também reforça essa ideia e diz que a evolução do instituto

da responsabilidade extracontratual se operou no direito romano, introduzindo no direito o elemento subjetivo da culpa, substituindo a ideia de pena, pela reparação do dano sofrido.

Outrossim, partindo para o ordenamento jurídico brasileiro em que a responsabilidade civil passa a ser regulamentada, tem-se o Código Civil de 1916, ou Código de Beviláqua, o qual permaneceu vigente até 2002. Para Sérgio Cavalieri Filho (2003), esse código era meramente subjetivista, à medida em que a responsabilidade civil fundava em seu artigo 159 “Aquele que, por ação ou omissão voluntária, negligência, ou imprudência, violar direito, ou causar prejuízo a outrem, fica obrigado a reparar o dano”.

Em contrapartida, em 1990 a implantação do Código de Defesa do Consumidor em consonância com a Constituição Federal, trouxe consigo um marco importante de mudanças e inovação do conceito de responsabilidade civil, com isso, intercorre a contemplar a reparação de danos causados a outrem de forma objetiva, ou seja, a culpa passou a ser um elemento não necessariamente fundamental (Brasil, 1990).

Do mesmo modo que, o Código Civil de 2002 incorporou elementos do Código de Defesa do Consumidor e trouxe duas possibilidades de responsabilidade civil, sendo a responsabilização objetiva expressa em seu artigo 927, parágrafo único, em que prevê a obrigação de reparação independentemente de culpa em casos especificados em lei ou caso a atividade desenvolvida pelo autor implicar riscos para direitos de outrem (Aguiar Júnior, 2003).

Na perspectiva do Código de Defesa do Consumidor, essa responsabilidade se expressa em seu artigo 14, o qual o fornecedor de serviços abstrai-se da culpabilidade e responde pela reparação dos danos causados aos consumidores por defeitos, informações insuficientes ou inadequadas. Esse dispositivo, fundamenta a ideia de que toda pessoa (física ou jurídica) deve agir de maneira a não prejudicar outros e, caso faça, está sujeita a ressarcir os danos (Brasil, 1990).

Em análise aos códigos é possível identificar os pressupostos da responsabilidade civil que regem o dever de indenizar, são eles, a conduta, o dano, o nexo causal e a culpa (Venosa, 2010). Mediante a isso, pode-se definir que, a conduta é a ação comissiva ou omissiva que cause dano a outrem, o dano pode ser explicado como a lesão sofrida (Diniz, 2005), o nexo de causalidade é a relação de causa e

efeito entre a conduta e o resultado e, por fim, a culpa é advinda da intenção deliberada de ofender o direito (Stoco, 2007).

Essa responsabilidade abrange tanto a esfera contratual quanto extracontratual, ou seja, pode envolver situações em que há violação de deveres previamente previstos no contrato ou aquelas em que surge uma obrigação legal em virtude de conduta ilícita que viola um dever jurídico preexistente, desconsiderando a culpa como elemento indispensável (Stoco, 2007).

As instituições financeiras foram regulamentadas pela Lei 4.595/1964, onde a responsabilidade ainda era predominantemente subjetiva, ou seja, pautada pela culpa, conforme Código Civil vigente na época. Hodiernamente, a relação entre essas entidades e seus clientes rege-se pela lei consumerista. A propósito, preconiza a Súmula 297 do STJ: “O Código de Defesa do Consumidor é aplicável às instituições financeiras”, e assim, se torna irrelevante se a responsabilidade é advinda de previsão contratual ou não, pois, aquele que expõe aos riscos outras pessoas deve arcar com a reparação (Tartuce, 2018).

Por conseguinte, a responsabilização dessas instituições não necessariamente resulta de descumprimento contratual estabelecido e compactuado entre as partes no que diz respeito ao fornecimento de produtos e serviços, mas simplesmente relacionada a responsabilidade aquiliana, como é o caso das fraudes bancárias, uma vez que, o consumidor ao contratar a abertura de uma conta, espera segurança e sigilo de seus bens e informações (Gonçalves, 2020).

Destarte, a responsabilidade civil das instituições financeiras refere-se à obrigação legal dessas entidades de reparar danos causados por fortuito interno – acontecimento que está ligado à organização da atividade desenvolvida - relativo a fraudes e delitos praticados por terceiros dentro na esfera das operações bancárias. Em geral, se conceitua meramente no dever indenizatório a fim de assumir as consequências jurídicas do infortúnio (Villar, 2015).

No mesmo sentido, a responsabilidade civil subsiste se o prestador de serviços não comprova culpa exclusiva do consumidor ou de terceiros, ou a inexistência de falha ou defeito na prestação do serviço, conforme disposto no Código de Defesa do Consumidor, em seu artigo 14. Assim, resta configurada a responsabilidade objetiva das instituições financeiras, conforme expresso na Súmula 479 do STJ: “As instituições financeiras respondem objetivamente pelos danos

gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.”

Nesse sentido, pode-se concluir que as fraudes bancárias ocasionadas por terceiros que envolvam falsidade ideológica e movimentações atípicas, configuram fortuito interno e devem ser reparadas pelas instituições financeiras (Silva; Kalassa; Callegaro, 2022).

No cerne, a responsabilidade civil das instituições financeiras consiste na obrigação de reparação de qualquer dano que seus clientes possam a vir sofrer advindas da exposição à riscos inerentes às suas atividades desenvolvidas. No caso das fraudes bancárias em confronto com a prestação de serviços e fornecimento de produtos, garante não apenas a indenização, como também, fomenta a adoção de práticas e mecanismos mais seguros de proteção de dados.

## 1.2 Excludentes de responsabilidade

A exclusão de responsabilidade civil refere-se a situações ou condições que podem isentar uma pessoa ou entidade da obrigação legal de reparar danos causados a outra parte. Ou seja, por intentar um dos pressupostos de responsabilidade civil, aniquilam pretensões indenizatórias, sendo: a) o estado de necessidade, b) a legítima defesa, c) exercício regular do direito, d) estrito cumprimento do dever legal - excluem a ilicitude, bem como, e) caso fortuito e força maior, f) fato de terceiro g) a culpa exclusiva do consumidor - excluem o nexo causal (Araújo Júnior, 2014).

O estado de necessidade tem sua previsão legal no artigo 188, II, do Código Civil de 2002, o qual prevê que: “não constituem atos ilícitos a deterioração ou destruição da coisa alheia, ou a lesão a pessoa, a fim de remover perigo iminente”. Ou seja, se baseia na situação de agressão a um direito alheio, para aniquilar perigo iminente, quando as circunstâncias não permitirem outra forma de atuação (Gagliano; Pamplona, 2012). Vale ressaltar que, há limites expressos neste artigo e o autor pode se responsabilizar pelos excessos cometidos, logo, o estado de necessidade não extingue a responsabilidade, apenas o dá direito à ação regressiva contra o causador do perigo (Lima, 1988).

Também abordada no artigo 188 do Código Civil de 2002, não constituem atos ilícitos os praticados em legítima defesa ou no exercício regular de um direito reconhecido (Brasil, 2002). Isto é, uma reação a uma situação injusta, contudo,

também limitada a atuação do agente, que pode responder pelos excessos, assim como a excludente só ocorre se presentes os pressupostos: a) a ameaça ou agressão partir de outrem, não sendo provocada pelo causador do dano; b) quando a agressão for atual ou iminente; e c) quando a reação for proporcional à agressão. (Costa; Padilha; Carneiro, 2014).

Nos casos de exercício regular de direito e estrito cumprimento de dever legal são fundadas na ideia de que quem utiliza seu direito não pode ofender ao de outrem (Costa; Padilha; Carneiro, 2014). Estes estão conectados e sua previsão legal está no artigo 188, I, do Código Civil, e assim como os pressupostos descritos até o presente momento, possuem limites do lídimo exercício de seu direito, sendo que, o abuso de direito está expresso no artigo 187 do Código Civil, podendo assim se manifestar de forma ilícita.

No tocante dos pressupostos que excluem o nexo causal, o Código Civil definiu o caso fortuito ou coisa maior em seu artigo 393, o qual prevê que o devedor não responde pelos casos fortuitos ou força maior, se expressamente não houver por eles se responsabilizado, sendo que este se verifica no fato necessário, os quais os efeitos não poderiam ser evitados. A força maior tem por característica a sua inevitabilidade, já o caso fortuito, a imprevisibilidade (Araújo Júnior, 2014).

Ademais, de acordo com a súmula 479, citada neste capítulo, as instituições financeiras respondem objetivamente por casos de fortuito interno, ainda que decorrentes de fatos de terceiro. Por conseguinte, são considerados fortuitos internos, todos que ocorram durante o processo de elaboração e execução do produto ou serviço, cabendo ao fornecedor se responsabilizar com os danos decorrentes de sua atividade. Por outro lado, os fortuitos externos são alheios a esse processo, frente à culpa exclusiva do consumidor ou existência de defeitos. Dessa forma, explica Sergio Cavalieri Filho (2010, p.301):

> Entende-se por fortuito interno o fato imprevisível, e, por isso, inevitável, que se liga à organização da empresa, que se relaciona com os riscos da atividade desenvolvida pelo transportador. O estouro de um pneu de ônibus, o incêndio do veículo, o mal súbito do motorista etc. são exemplos do fortuito interno [...] O fortuito externo é também fato imprevisível e inevitável, mas estranho à organização do negócio. É fato que não guarda nenhuma ligação com a empresa, como fenômenos da Natureza – tempestades, enchentes etc. Duas são, portanto, as características do fortuito externo: autonomia em relação aos riscos da empresa e inevitabilidade, razão pela qual alguns autores o denominam de força maior.

Diante disso, embora no contexto das fraudes bancárias seja necessária uma conduta praticada por terceiro (um dos pressupostos de excludente de responsabilidade), o que teoricamente romperia o nexo causal, a ocorrência dessas fraudes depende de diversos fatores intrinsecamente ligados aos danos decorrentes das atividades das instituições.

Dito isso, tem-se a utilização de documentos falsos no ato da abertura de contas, a clonagem de cartões e a falha de monitoramento, que por exemplo, caracterizam como fortuito interno, pois decorreram de falhas na execução e elaboração do produto e serviço prestado, visto que, essas entidades tem o dever de monitorar e garantir a segurança de seus clientes (Silva; Kalassa; Callegaro, 2022).

Por sua vez, a culpa exclusiva da vítima ou consumidor pode ser efetiva excludente de responsabilidade, pois desvanece o nexo causal entre o ato danoso e o prejuízo, devido advir de acidente ou comportamento da própria vítima, em virtude de sua imprudência ou negligência. Contudo, a culpa exclusiva desta, só exclui a responsabilidade civil se o evento for ocasionado unicamente por ela, a indenização pode ser compartilhada entre as partes (autor do fato e vítima/consumidor), caso houver o pressuposto de culpa (Costa; Padilha; Carneiro, 2014).

A culpa exclusiva da vítima está ligada a caracterização do dever de indenizar a teor dos artigos 196 e 927 do Código Civil, análogo a isso, por sua vez, a culpa exclusiva do consumidor também está prevista no Código de Defesa do Consumidor em seu artigo 14, § 3°, II, em que o fornecedor de serviços não será responsabilizado caso provar a culpa exclusiva do consumidor ou terceiro.

Ante o exposto, no ambiente bancário, as fraudes fazem parte dos riscos inerentes e previsíveis às atividades desenvolvidas pelas instituições financeiras, ao ponto que, quem exerce atividade remuneratória deve responder pelos eventos danosos (Silva Neto, 2013). Isto posto, a elisão da responsabilidade civil dessas entidades está ligada à culpa exclusiva de terceiros, à vista que integra fortuito externo, ou seja, não possui relação de causalidade com a atividade do fornecedor e assim, não resta responsabilidade objetiva (Pereira, 2018).

Em suma, os excludentes de responsabilidade civil desempenham um papel crucial no âmbito jurídico, proporcionando um equilíbrio entre a justiça e a razoabilidade. Ao analisar as diversas situações em que tais excludentes são aplicáveis, percebe-se a necessidade da consideração de cada caso de forma individual, levando em conta os princípios da proporcionalidade e da equidade.

## 1.3 Mecanismos de segurança

Em meados dos anos 70 houve um rápido avanço tecnológico conhecido como “Quinta Revolução Tecnológica”, sendo que, somente após o ano 2000 sucedeu a proliferação do uso da internet mundialmente. Do mesmo modo, o setor bancário também investiu e teve que se adaptar à essas mudanças, com isso, as TIC’s – Tecnologia da Informação e Comunicação, se tornaram essenciais à mercê de depósitos, pagamentos, transações e entre outros serviços financeiros (Rezende, 2012).

Com a crise de 2008-2009, também conhecida como a Grande Recessão, a qual teve suas raízes no setor imobiliário dos Estados Unidos, em virtude do *boom* imobiliário provocado por práticas de empréstimos arriscados, títulos lastreados em hipotecas *subprime*, falta de regulamentação adequada e distribuição de produtos completos, muitas instituições financeiras foram afetadas, desencadeou uma crise financeira mundial e fez com que esse setor ameaçasse estagnar o crescimento e desenvolvimento de países (Unisc, 2020).

Diante o cenário, fez-se necessário a implantação de medidas mais eficazes e mudanças na regulamentação, melhoria de políticas monetárias, gestão de risco e reforço da regulação e, consequentemente, investimento em tecnologia. Por outro lado, o avanço tecnológico no sistema financeiro reconduziu a maneira como as instituições operam e como os consumidores interagem com os serviços financeiros. Inovações nos sistemas de pagamentos, gestão de investimentos e a ascensão das *FinTechs*, desafiaram os modelos tradicionais e trouxeram também, desafios em relação à segurança e ao aumento potencial das fraudes bancárias (Neto, 2021).

À título de exemplo, têm-se a criação do Pix, lançado em 2020, um recurso ágil de transferências instantâneas, que de acordo com o coordenador do laboratório de segurança cibernética da Federação Brasileira de Bancos (Febraban), Valdir Assef Jr., explodiu o número de transações realizadas no sistema financeiro nacional, sendo que, de 2020 à 2022 houve um aumento de 87%. Para logo, essa crescente culminou ao aumento das fraudes bancárias, de modo que os valores são rapidamente dispersados, dificultando a mitigação, diligenciamento e recuperação de recursos (OPovo, 2023).

Com isso, de acordo com estatísticas publicadas em O GLOBO, o Banco Central registrou um aumento de 57,7% de fraudes bancárias de 2020 para 2021 e 55,8% de 2021 a 2022 (Bretas, 2023). Outro número exorbitante foi discutido pela Comissão de Defesa do Consumidor da Câmara dos Deputados em audiência pública para discutir medidas de prevenção a fraudes no sistema financeiro, vez que, apenas no primeiro trimestre de 2023 foram registradas mais de 2,8 mil tentativas de fraude por minuto no Brasil (Anadep,2023).

Por conseguinte, infere-se que a responsabilidade civil das instituições financeiras em casos de fraudes está diretamente relacionada à obrigação de garantir a segurança e integridade das transações financeiras de seus clientes. Com isso, o Banco Central do Brasil intensificou a normatização de procedimentos e controle para a prevenção e combate às fraudes, a serem adotadas pelas instituições financeiras.

Através da Resolução n°142/2021, o Banco Central do Brasil definiu medidas para a realização de transações de pagamento e transferências de valores, os quais passaram a ter um valor máximo de limite pré-estabelecido. Com isso, após a instituição do normativo, os bancos passaram a possuir uma tabela nacional, e os valores que excedam o limite estipulado passou a ser facultado ao cliente e podem ser adequados ao perfil de cada um, de acordo com sua capacidade, risco e padrão de consumo, auxiliando na identificação de movimentações atípicas que fujam desse padrão, reduzindo riscos e possíveis perdas (Brasil, 2021).

Outrossim, no mesmo ano de 2021, o MED - Mecanismo Especial de Devolução, foi instituído com intuito de recuperação de valores e possibilita a comunicação entre instituições financeiras. No momento em que é identificada uma suposta fraude a vítima contacta sua instituição, que se cabível, aciona o MED e os recursos são bloqueados na conta recebedora (do fraudador). Vale ressaltar que esse dispositivo atua de forma devolutiva somente após a ocorrência do infortúnio, de modo que a devolução desses valores está condicionada a existência ou não de saldo disponível na conta destino durante um prazo de 90 dias (Brasil, 2021).

Similarmente, em 2023 entrou em vigor a Resolução Conjunta n°6, que dispõe regras para o compartilhamento de dados entre instituições financeiras, sobre indícios de transações fraudulentas. Essa medida, possibilita o enriquecimento de informação entre os bancos, como a identificação de quem teria executado ou tentado executar a fraude, indícios de ocorrência, identificação da instituição responsável pelo

registro e dados das contas recebedoras de recursos, portanto, reduz a chance de um golpista aplicar a mesma fraude em várias entidades diferentes (Brasil, 2023).

Além disso, para cumprir com essas obrigações e atuar como uma barreira de proteção dentro do sistema de cada instituição financeira, essas entidades implementam diversos mecanismos de segurança além dos dispositivos já estipulados pelo Bacen, os quais chegam a gerar um custo anual de cerca de R$2 bilhões em tecnologia. Conforme disposto e exemplificado pela FEBRABAN (2019), tem-se a tecnologia de *analytics* se baseia numa análise detalhada do perfil de cada cliente; a biometria, que atua como uma barreira de segurança no login ou confirmação de operações realizadas em aplicativos bancários; os avisos e notificações enviadas pelos bancos através de SMS ou nos próprios aplicativos; os cartões virtuais; o *QR Code* ou autenticação multifatorial (MFA), os quais permitem que uma movimentação só seja realizada quando utilizados dois equipamentos habilitados pelos clientes e os módulos de segurança, que protegem e identificam programas espiões ou vírus instalados em aparelhos celulares para invasão de máquina e aplicativos.

Todavia, nenhuma ferramenta é capaz de barrar todo e qualquer tipo de fraude. Em uma pesquisa realizada com consumidores em 16 países do mundo, incluindo o Brasil, a "*Faces of Fraud: Consumer Experiences With Fraud and What It Means for Businesses*" do SAS, empresa de inteligência artificial e analytics, revelou que 70% dos entrevistados relatam terem sido vítimas de fraude pelo menos uma vez e 40% duas ou mais vezes, e afirmam que mudariam de prestador de serviços se oferecidas melhores condições de segurança. Nessa perspectiva, os interrogados também manifestaram vontade de partilhar mais dados pessoais aos detentores de suas contas de modo a serem utilizados para aprimoramento de mecanismos de segurança antifraudes, bem como se dispuseram a abrir mão de certas inovações, como as transações instantâneas, a fim de evitar perdas (SAS, 2023).

Em atenção à isso, a implementação de mecanismos cada vez mais eficazes contribuem com a redução de perdas financeiras, danos à reputação e consequente impacto negativo aos clientes, além da proteção dos direitos dos consumidores. É impreterível que as organizações aprimorem esses mecanismos para enfrentar os desafios no cenário de segurança contra fraudes e golpes bancários.

# CAPÍTULO II – ENGENHARIA SOCIAL E GOLPES

Busca-se no presente capítulo abordar o conceito, métodos e principais estratégias envolvidas nas práticas de engenharia social e golpes aplicados em fraudes bancárias. A evolução das técnicas utilizadas, caminham junto à evolução do sistema financeiro e seus produtos, o que exprime uma análise minuciosa das vulnerabilidades e desafios tecnológicos, a fim de compreender, entender e mitigar os riscos de golpes bancários.

## 2.1 Conceito de engenharia social, métodos e estratégias.

Engenharia social é uma prática que envolve a manipulação psicológica de pessoas para obter informações úteis, acessar sistemas protegidos ou realizar ações relacionadas. Ao contrário dos métodos tradicionais de invasão, que se concentram na exploração de vulnerabilidades técnicas, a engenharia social direciona-se à exploração das fraquezas humanas, buscando persuadir ou enganar indivíduos para atingir seus objetivos (Kaspersky, 2024).

O termo “engenharia social” surgiu em 1894, com um estudo mais aprofundado do tema pelo industrial holandês JC Van Marken, com intuito de resolver os problemas das indústrias relacionadas à força de trabalho, em virtude da ocorrência de descontentamento de funcionários. Posteriormente, em 1911, com o livro *“Social Engineer”* de Edward L. Earp, foi apresentada a ideia de que na Engenharia Social, as pessoas deveriam lidar com as relações sociais assim como abordam as máquinas (Escobar, 2022).

Com relação aos dias atuais, essa nomenclatura é utilizada para definir estratégias de práticas ilegais, de manipulação humana, popularizada em 2013 com a execução de diversos crimes de roubo de informações e acessos não autorizados

por Kevin Mitnick, detalhados em seu livro *“The Art of Deception: Controlling the Human Element of Security”*. Neste, Kevin afirma que o ciclo da Engenharia Social possui 4 fases, sendo elas: pesquisar; desenvolver uma relação de confiança com a vítima; explorar essa confiança e utilizar a informação, utilizada, principalmente, por fraudadores e hackers que não possuem conhecimento em tecnologia e sistemas (Escobar, 2022).

Em 2017, o Brasil foi alvo de 205 milhões de ciberataques, aproximadamente um para cada brasileiro (Rocha, 2018). Vale ressaltar que, no país, os crimes de engenharia social são relacionados à crimes cibernéticos, embasados na Lei 12.737/2012, também conhecida como Lei Carolina Dieckmann, após invasão de fotos íntimas e dados pessoais da atriz. A pena varia de acordo com a gravidade da ação e pode chegar a dois anos de reclusão para casos mais graves (Fachini, 2023).

Salienta-se que a engenharia social envolve vários métodos e estratégias de manipulação da vítima, como: *phishing, vishing, dumpster diving, quid pro quo, sextorsion, tailgating, pretexting, baiting,* entre outros. No contexto em que estão inseridas as fraudes bancárias, os principais métodos utilizados são o *phishing*, *vishing*, *pretexting* e *quid pro quo*, os quais estão entre as principais ameaças à segurança da informação financeira (Stefanini, 2022).

Entre os principais golpes, o *Phishing*, que pode ser traduzido como “pescaria” é o mais habitual e periculoso. Conforme pesquisa realizada pela *Psafe, dfndr security e dfndr enterprise,* esse método representou mais de 5 milhões de ataques nos primeiros sete meses de 2022 e 100% de aumento em comparação à 2021. (Diniz, 2022). Essa estatística permanece em crescente, já que em 2023 registrou-se 134 milhões de tentativas de *phishing* em um ano, representa um aumento de 463% em comparação ao visto nos anos anteriores. Vale ressaltar que, dos ataques realizados, 42,8% se tratam de golpe do falso funcionário bancário (O Globo, 2023).

Nessa técnica, normalmente, os criminosos se passam por empresas confiáveis, bancos, familiares ou pessoas conhecidas, através de e-mail, WhatsApp ou SMS, assim, recorre à emoções como curiosidade, medo e presteza, ao apresentar algum problema, induz a vítima a entrar em um link que a encaminha à um site de *phising/*falso site, ludibriados a apresentar informações pessoais sigilosas e seus dados confidenciais são roubados (Serasa, 2023).

No cenário bancário, esses ataques ocorrem principalmente via e-mail, nestes, é relatado algum problema que pode ter acontecido com a suposta conta mantida no banco em questão, bem como, mensagens de aprovação de limites de cartão de crédito, de empréstimos ou solicitações de atualizações cadastrais. Dessa forma, a vítima acessa o falso site e dispõe aos fraudadores seus dados pessoais, contas, senhas e números de cartões de crédito (Rocha, 2018).

Em contrapartida, o *vishing,* que é a junção de “voice” e “*phishing”,* é uma prática semelhante ao *phishing,* contudo, exercida através de telefonemas, onde é possível forjar a identidade da ligação, o que faz com que o número da chamada recebida aparente ser de fonte legítima, como exemplo, número de telefone de bancos e 0800. Com isso, as vítimas são induzidas ao repasse de informações pessoais, senhas de acesso, a realizar transferências ou realizar depósito de determinado valor para liberação de falso empréstimo, acreditando estar falando com alguém de confiança (Rocha, 2018).

Em 2023, o Banco do Brasil, assim como outros bancos, intensificou a disseminação de alertas de cuidado aos golpes de *phishing* e *vishing.* Em matéria publicada em seu site, o Banco sobreavisa sobre o golpe da falsa central de atendimento ou 0800, golpe este que tomou grandes proporções, onde os criminosos se passam por atendentes bancários, com gravações que simulam as URAs (Unidade de Resposta Audível) persuadem a vítima, que acaba por resultar em perdas financeiras (Banco do Brasil, 2023).

Sob outra perspectiva, ao recorrer ao *pretexting,* os golpistas tomam forma de assumir uma nova identidade ou um personagem, o qual está inserido em uma falsa história a fim de comover a vítima. Para isso, são colhidas informações acessíveis em redes sociais, como data de nascimento, familiares, amigos, local de residência, entre outros, para a familiarização com quem irá sofrer o golpe. Assim, os criminosos se passam por um conhecido do meio de trabalho ou pessoal e coagem ao fornecimento de informações, acessos ou valores (Rocha, 2018).

Por outro lado, o *quid pro quo*, também definido como “isso por aquilo” acontece quando há o requerimento de informações em troca de algo. Um exemplo é o fornecimento de formulários a serem preenchidos com informações pessoais, para concorrer à brindes ou premiações (Serasa, 2023). No mesmo sentido, também ocorre com o golpe do falso especialista em segurança, onde, os criminosos oferecem atualizações de software antivírus, mas solicitam que sejam desinstalados os já

existentes, dessa forma, a vítima é induzida a instalar programas maliciosos sem restrições no computador ou celular, o que permite acesso a todos seus dados, aplicativos e contas (KPMG, 2019).

Tem-se, portanto, que a engenharia social emerge como uma prática sofisticada que se utiliza de artifícios psicológicos para manipular indivíduos e obter informações confidenciais. Esta abordagem destaca a importância da compreensão das vulnerabilidades humanas para proteger contra ataques cibernéticos e fraudes, uma vez que, os métodos e estratégias empregados na engenharia social incluem a exploração de confiança, criação de pretextos convincentes e a utilização de técnicas persuasivas. Assim, a compreensão desses aspectos é fundamental para o desenvolvimento de medidas eficazes de prevenção e conscientização, que visa fortalecer a segurança digital e proteger organizações e indivíduos contra ameaças sociais.

## 2.2 Principais golpes bancários e *modus operandi* dos fraudadores

Nos últimos anos, o avanço tecnológico proporcionou inúmeras facilidades na gestão financeira, tornando as transações bancárias mais acessíveis e eficientes. No entanto, esse progresso também abriu portas para uma crescente ameaça: os golpes bancários. Desde ataques cibernéticos até métodos mais tradicionais, como a clonagem de cartões, as estratégias dos fraudadores evoluíram, o que exige uma atenção constante por parte dos consumidores e das instituições financeiras (Santiago, 2024).

A Federação Brasileira de Bancos – FEBRABAN - tem intensificado os esforços e investimentos na busca de eficientes medidas de prevenção a golpes e fraudes bancárias. Em 2021, foi criada a Campanha de prevenção a fraudes “Pare e Pense: Pode ser Golpe”, que ficou conhecida com a disseminação em formato de paródia da música “Pare” dos cantores Zezé Di Camargo e Luciano, com intuito de divulgar os principais golpes aplicados por criminosos e formas de proteger os clientes e consumidores do país, de forma didática e chamativa (Febraban, 2023).

Em 2023, já na 3° edição da Campanha, em conjunto com a iD\TBWA, agência que combina criatividade e dados para acelerar o crescimento de marcas e negócios, elencando o informativo de fraudes com músicas atuais, passaram a expandir os canais de divulgação, também utilizando as principais emissoras do país

para divulgação dos alertas. Além desse e outros meios, a Febraban implantou a Semana da Segurança Digital, para promover a conscientização da sociedade e divulgar dicas de proteção aos principais golpes, as quais utilizam ações similares desenvolvidas nos Estados Unidos em 2003 e na Europa em 2012 (Febraban, 2023).

Transmitidos na Campanha, a Federação Brasileira de Bancos elencou os principais golpes ou mais comuns em doze, sendo eles: Golpe da falsa central de atendimento, golpe do falso motoboy, golpe do falso leilão, golpe no *whatsapp*, golpe da troca de cartão, cuidado com as senhas, golpe do link falso, golpe do delivery maquininha quebrada, golpe do falso boleto, proteção de dados no celular ou dispositivo, golpe do falso presente, golpe do falso empréstimo e por fim, acesso remoto ou mão fantasma. Sendo, 06 deles os mais comuns e diretamente ligados ao contexto de fraudes bancárias (Febraban, 2023).

O Golpe da falsa central de atendimento, é uma prática de *vishing*, na qual um fraudador se passa por um representante legítimo de uma instituição financeira ou empresa para obter informações confidenciais da vítima. O *modus operandi* do fraudador envolve um contato inicial com a vítima, geralmente por meio de telefonemas ou mensagens eletrônicas, onde se faz passar por um funcionário do banco ou empresa, alega problemas de segurança, como invasão ou clonagem de conta, o fraudador cria um senso de urgência e preocupação na vítima. Ademais, instrui para que a vítima ligue para a suposta central do banco, utilizando o número presente no verso do cartão. No entanto, o fraudador permanece na linha durante a chamada simulada, agindo como se fosse um atendente legítimo, para continuar a coleta de dados sensíveis, como números de conta, informações de cartões e, especialmente, senhas (Febraban, 2023).

O Golpe do falso motoboy, destaca uma técnica mais elaborada, envolvendo uma série de etapas para persuadir a vítima a entregar seu cartão e informações, permitindo que os golpistas realizem transações fraudulentas. O golpe começa com uma ligação telefônica para o cliente, na qual o golpista se apresenta como um funcionário do banco, alega que cartão do cliente foi fraudado, então, solicita a senha do cartão e instrui o cliente a cortar o cartão, mas sem danificar o chip. Em seguida, os fraudadores informam que um representante do banco irá até a casa da vítima para retirar o cartão cortado. Essa manobra permite que os fraudadores tenham acesso ao chip e, consequentemente, realizem transações fraudulentas em nome da vítima, mesmo após o corte do cartão (Banco Master, 2023).

O golpe da troca de cartões, aborda estratégias de golpistas que atuam como vendedores ou prestadores de serviços, aproveitando-se de situações cotidianas para obter informações sensíveis, como senhas e cartões, para realizar transações fraudulentas. Esses vendedores observam atentamente quando os clientes digitam suas senhas em máquinas de compra. Após a transação, esses golpistas trocam o cartão do cliente por outro, mantendo consigo o cartão original e, consequentemente, a senha. Esse golpe também pode ocorrer em caixas eletrônicos, onde, os criminosos oferecem ajuda sob o pretexto de auxiliar em dificuldades no terminal eletrônico, assim, durante o suposto auxílio, esses golpistas se atentam à senha de acesso, rapidamente pegam o cartão da vítima, devolvendo um cartão falso no lugar (Banco Master, 2023).

No caso do Golpe do falso boleto, o emissor do boleto fraudado possui informações detalhadas sobre os dados pessoais da vítima, tornando a situação bastante convincente. Esse tipo de golpe é uma forma de fraude financeira que pode ser disseminada de diversas maneiras, tanto em formato físico como correspondências bancárias ou de lojas, quanto eletrônico, por meio do Whatsapp, e-mail ou SMS. Uma característica crucial desse golpe é a semelhança entre os boletos falsos e os originais, o que torna a fraude difícil de ser identificada, e, ao realizar o pagamento do boleto o valor é direcionado para a conta do fraudador, ao invés do verdadeiro credor (Febraban, 2023).

Já no Golpe do falso empréstimo, quadrilhas atuam sob a fachada de falsas instituições financeiras, utilizando anúncios online para atrair potenciais vítimas com promessas de crédito vantajoso. O *modus operandi* dessas quadrilhas começa com a veiculação de anúncios na internet, oferecendo crédito com condições extremamente atrativas, que, ao atrair a atenção de interessados, os fraudadores conduzem as vítimas a preencher cadastros em sites falsos que simulam serem de instituições financeiras legítimas. Posteriormente, os fraudadores entram em contato com os interessados, muitas vezes enviando um suposto contrato que, de forma deliberada, contém cláusulas com multas expressivas para desencorajar qualquer tentativa de desistência. Diante disso, os fraudadores solicitam o pagamento de taxas e impostos sob a alegação de que é necessário para a liberação do suposto empréstimo, como condição prévia para concessão do crédito, embora na realidade seja apenas uma forma de extorquir a vítima (Febraban, 2023).

Por fim, tem-se o golpe do acesso remoto ou mão fantasma, o fraudador entra em contato e se identifica falsamente como um funcionário do banco, alega que há movimentações suspeitas na conta da vítima, informando-a de uma possível invasão ou clonagem da conta. Para resolver o suposto problema, o fraudador propõe a solução de instalar um aplicativo no celular da vítima. No entanto, o golpe reside no fato de que o aplicativo oferecido pelo fraudador é, na verdade, malicioso, que permite ao golpista acesso a todos os dados armazenados no celular invadido (Febraban, 2023).

Com isso, fica elucidado a diversidade de estratégias enganosas empregadas para obter acesso indevido a informações financeiras e pessoais. Com o emprego de técnicas de engenharia social e com o avanço da tecnologia, os golpes tomaram proporções significantes. Assim, a conscientização dos usuários sobre práticas de segurança digital, a verificação rigorosa de solicitações suspeitas e a adoção de medidas preventivas são essenciais para mitigar os riscos e proteger os consumidores contra a crescente complexidade dos golpes bancários.

## 2.3 Vulnerabilidades, desafios e soluções tecnológicas no combate à fraudes

Na atual era digital, onde a tecnologia permeia quase todos os aspectos da vida moderna, o combate às fraudes tornou-se um desafio cada vez mais complexo e crucial. À medida que as organizações adotam sistemas e processos tecnológicos avançados para otimizar suas operações, os fraudadores também se tornam mais sofisticados em suas abordagens, explorando vulnerabilidades e lacunas nos sistemas de segurança. Com isso, o setor bancário tem sido significativamente impactado pela rápida transformação digital, especialmente com o surgimento e sucesso das *fintechs* e bancos digitais (Tchilian, 2022).

Conforme revelado pela Pesquisa Febraban de Tecnologia Bancária 2023, conduzida pela Deloitte, líder global na prestação de serviços de *audit & assurance, consulting, financial advisory, risk advisory, tax* e serviços relacionados, quase 80% das transações bancárias no Brasil são feitas por meio de canais digitais, como o mobile banking e o internet banking. Ademais, divulgado durante o Febraban Tech 2023, esse dado destaca a preferência crescente dos brasileiros por serviços bancários online, sendo que, no ano de 2022 foram realizados 163,3 bilhões de transações, um aumento significativo de 30% em relação a 2021, impulsionado

principalmente pelo crescimento de 54% no mobile banking, que registrou 107,1 bilhões de transações (Febraban, 2023).

Esse levantamento revelou um prejuízo nas transações realizadas por brasileiros nas agências bancárias, de 3,3 bilhões para 3,2 bilhões, representando hoje apenas 2% do total. Da mesma forma, as operações em caixas eletrônicos, central de atendimentos e correspondentes também reduziram. Isto evidencia o aumento contínuo da adesão aos canais digitais, o qual o presidente da Febraban, Isaac Sidney, atribui essa tendência ao investimento anual de R$ 45 bilhões em tecnologia pelos bancos, tornando o acesso aos serviços financeiros mais democrático e estreitando o relacionamento com os clientes (Febraban, 2023).

No mesmo viés, a pandemia do COVID-19, caracterizada em março de 2020, intensificou a necessidade de oferecer soluções financeiras simples e acessíveis por meio da tecnologia bancária, facilitando a adesão de milhões de brasileiros aos serviços digital, o que justifica o aumento expressivo na utilização desses serviços, destacada pela pesquisa da Febraban (Tchilian, 2022). No entanto, essa mudança também trouxe desafios de segurança, desde a autenticação de identidade até a aprovação de crédito sem documentos financeiros, o que explica a crescente em 165% de fraudes e golpes contra clientes de bancos em 2021 em comparação a 2020. Assim, evidencia a necessidade que os bancos têm de inovar, sem desconsiderar a segurança, responder com soluções tecnológicas robustas, ao mesmo tempo em que oferecem uma experiência sem atrito aos clientes (O Popular, 2021).

Como já amplamente discutido, os bancos têm implementado diversos mecanismos de segurança para combater fraudes financeiras, desde sistemas de autenticação em duas etapas até o monitoramento de transações suspeitas em tempo real. No entanto, tais mecanismos ainda se mostram insuficientes para barrar transações espúrias oriundas de golpes sofridos por meio da engenharia social. Por conseguinte, à medida que as tecnologias avançam, surge uma nova fronteira na batalha contra atividades fraudulentas: a inteligência artificial (IA), que pode oferecer aos bancos a capacidade de detectar padrões complexos de comportamento fraudulento com uma precisão muito maior do que os métodos tradicionais, além de personalizar suas medidas de segurança, adaptando-as às necessidades individuais de cada cliente e proporcionando uma experiência mais segura e conveniente (TI Inside, 2023).

Estima-se que, Alan Turing, renomado matemático que concebeu o famoso Teste de Turing em 1950, o qual envolvia uma máquina capaz de simular a comunicação escrita humana, é considerado pioneiro na Inteligência Artificial após a publicação de seu artigo *Computing Machinery and Intelligence* (Barbosa; Bezerra, 2020, p. 94). Posteriormente, em 1956 ocorreu um marco fundamental na história da IA, durante a Conferência do Dartmouth College, realizada em New Hampshire, nos Estados Unidos. Foi nesse caso que o termo “inteligência artificial” foi formalmente introduzido, delineando um novo campo de estudo (Barbosa; Bezerra, 2020, p. 93).

Contemporaneamente, durante os anos 2000, a inteligência artificial começou a ser investigada para sua aplicação em carros independentes, uma tecnologia que agora está disponível no mercado. A partir de 2008, o processamento de linguagem natural, ressurgiu como foco nas pesquisas de IA resultando no desenvolvimento de novos assistentes virtuais, como a Siri, lançada pela Apple em 2011, Alexa, da Amazon, Cortana, da Microsoft e Google Assistente (Barbosa; Bezerra, 2020, p. 95).

No cenário bancário, com o aprimoramento e surgimento de novas ferramentas de uso da Inteligência Artificial, segundo o estudo *State of AI in Financial Services,* 2022, realizado pela Nvidia, empresa multinacional de tecnologia incorporada, 78% dos profissionais que atuam no setor financeiro utilizam a Inteligência Artificial (IA), por meio de tecnologias aplicadas, que dá aos computadores a capacidade de identificar padrões em dados massivos e fazer previsões (análise preditiva), com o objetivo de melhorar suas operações e lidar com problemas relacionados a fraudes. Essa preferência dos profissionais do setor financeiro pela IA, é esclarecida por Eduardo Daghum, CEO da Horus Group, empresa que atua no ciclo completo da prevenção à fraude e planejamento estratégico corporativo, o qual afirma que um dos principais motivos é a capacidade da IA em fornecer soluções eficazes para o gerenciamento de riscos, as quais têm impacto potencial em toda a organização (TI Inside, 2023).

No mesmo viés, Eduardo Daghum examina e exemplifica algumas das aplicações da Inteligência Artificial, sendo elas, a detecção de anomalias em tempo real, a análise de padrões de comportamento, a verificação biométrica e o aprendizado por reforço, as quais têm revolucionado a prevenção à fraudes bancárias e redução de perdas financeiras (TI Inside, 2023).

Na tecnológica por análise de padrões de comportamento, as ferramentas de Inteligência Artificial analisam o padrão de transações e comportamentos costumeiros dos clientes, com base na análise de perfil individual, sendo que, transações detectadas fora do que é comumente realizado, são disparados alertas. Outro mecanismo utilizado, é a verificação biométrica, que associada à IA aperfeiçoa consideravelmente a ferramenta, a qual utiliza padrões complexos na detecção biométrica, aliada contra variações que podem ocorrer ao longo do tempo (Crypto ID, 2024).

A detecção de anomalias em tempo real, permite que instituições financeiras monitorem operações simultaneamente e identifique, por exemplo, gastos atípicos ou localizações suspeitas, bloqueando as transações antes de efetivadas. Essa ferramenta também foi apresentada em palestra realizada na Febraban Tech 2023, pelo CEO e Cofundador da Incognia, André Ferraz, empresa na qual já atua em parceria com bancos e aplicativos de delivery na prevenção e mitigação de fraudes com o auxílio da Inteligência Artificial (Incognia, 2023).

Por fim, no aprendizado por reforço, o método de inteligência artificial é desenvolvido para aprimorar de forma contínua os sistemas de detecção de fraudes, os algoritmos de reforço têm a capacidade de se aperfeiçoar através da experiência, aumentando sua eficácia na detecção de novas formas de fraudes à medida que estas surgem. Isso se assemelha ao processo de aprendizado de máquina, também conhecido como *machine learning,* uma subárea de inteligência artificial na qual os sistemas são treinados para garantir padrões e realizar tarefas sem necessidade de programação explícita (Crypto ID, 2024).

Em síntese, à medida que as ameaças de fraudes continuam a evoluir e se sofisticar, soluções tecnológicas se tornam indispensáveis no combate a esses problemas. A inteligência artificial surge como aposta do futuro nesse contexto, oferecendo capacidades únicas de aprendizado e adaptação que permitem aprimorar continuamente os sistemas de detecção de fraudes, com a utilização de algoritmos de aprendizado para reforço e outras técnicas avançadas, a IA pode identificar e responder a novos tipos de fraudes de maneira rápida e eficiente, oferecendo uma linha de defesa robusta contra atividades fraudulentas. Assim, investir no desenvolvimento e melhoria de soluções baseadas em IA tem sido crucial para fortalecer a segurança e proteger organizações e usuários contra ameaças cada vez mais sofisticadas no mundo digital.

# CAPÍTULO III – ANÁLISE JURÍDICA E PERSPECTIVAS DE PROTEÇÃO AO CONSUMIDOR

No vasto cenário jurídico das fraudes bancárias, emerge a necessidade premente de uma análise jurisprudencial minuciosa e abrangente. A evolução das práticas delituosas no âmbito financeiro, aliada à constante atualização das leis e regulamentos, desafia tanto os operadores do Direito quanto os próprios sistemas judiciais. Com isso, através da análise criteriosa de decisões judiciais e da confrontação com a legislação vigente, compreende-se as nuances que permeiam as fraudes bancárias, suas repercussões sociais e econômicas, bem como as respostas do Poder Judiciário diante de tais desafios.

## 3.1 Vulnerabilidades do consumidor nas relações bancárias

Nas relações de consumo, o consumidor se encontra sempre em uma posição de fragilidade em relação ao fornecedor. Para o sistema jurídico brasileiro, isso significa que o consumidor é considerado vulnerável no mercado de consumo, o que exige proteção por meio de normas jurídicas. Assim, a legislação brasileira estabeleceu o Princípio da Vulnerabilidade como um dos fundamentos do Código de Defesa do Consumidor (Silveira, 2022).

A origem e o desenvolvimento da noção jurídica de vulnerabilidade estão associados, no direito, especialmente após as mudanças no direito constitucional com a consolidação dos direitos fundamentais, possibilitou a admissão de uma proteção especial e diferenciada para grupos de pessoas com base em qualidades ou situações específicas que justifiquem essa distinção (Miragem, 2020).

O Código de Defesa do Consumidor reconhece o consumidor como a parte mais fraca nas relações de consumo, em conformidade com a Resolução 39/248 da

ONU de 1985. Esta resolução, em seu artigo 1º, destaca que o consumidor é a parte mais vulnerável, um reconhecimento que é aceito mundialmente (Silveira, 2022). Assim, Silvia Fernandes Chaves (2015, p.150) conceitua essa vulnerabilidade como:

> o princípio pelo qual o sistema jurídico positivado brasileiro reconhece a qualidade ou condição daquele (s) sujeito (s) mais fraco (s) na relação de consumo, tendo em vista a possibilidade de que venha (m) a ser ofendido (s) ou ferido (s), na sua incolumidade física ou psíquica, bem como âmbito econômico, por parte do (s) sujeito (s) mais potente (s) da mesma relação.

A vulnerabilidade é o conceito central que sustenta todo o sistema de defesa do consumidor, visando proteger a parte mais frágil na relação de consumo para promover o equilíbrio contratual. Esse princípio está previsto no art. 4º, I da Política Nacional das Relações de Consumo, Lei n°8.078 de 11 de setembro de 1990, porém com sua concepção no art. 5°, XXXII da Constituição Federal, ou seja, é reconhecida constitucionalmente, podendo ser técnica, jurídica, fática ou informacional (Estado de Minas, 2016).

A vulnerabilidade fática (ou socioeconômica) decorre da relação de superioridade e do poder que o fornecedor exerce no mercado de consumo em comparação ao consumidor. Geralmente, há uma disparidade nas relações de consumo, refletindo o maior poder econômico do fornecedor em confronto ao consumidor, o que costuma resultar em uma posição contratual privilegiada para o fornecedor. Vale ressaltar que, a vulnerabilidade fática não pode ser confundida com a hipossuficiência (Silveira, 2022).

No ponto de vista de Bruno Miragem (2008, p.63) “a vulnerabilidade fática é espécie ampla, que abrange genericamente, diversas situações concretas de reconhecimento da debilidade do consumidor”. Ao analisar a relação entre cliente e instituição financeira, fica claro que o cliente está em uma posição de desvantagem devido à enorme disparidade de poder entre as partes, devido não somente da comparação com o poder econômico do banco, como também a essencialidade de manter relacionamento com alguma dessas instituições financeiras nos dias atuais. Essa necessidade, em certa medida, obriga o correntista a aceitar as regras contratuais impostas pelos bancos, que geralmente são contratos de adesão, sem espaço para negociação (Monteiro, 2022).

Além da pressão social, a vulnerabilidade do consumidor obriga-o a aceitar as formas de operação dessas instituições, como métodos de atendimento não presenciais, contatos telefônicos frequentes, recebimento constante de e-mails, além de mensagens por SMS e aplicativos de celular. Esses meios expõem os clientes a riscos significativos, como a exploração de canais de comunicação por criminosos que se passam por bancários e fazem com que esses consumidores fiquem suscetíveis à golpes e fraudes bancárias (Monteiro,2022).

A vulnerabilidade técnica, refere-se à situação em que o consumidor se encontra em desvantagem devido à sua falta de conhecimento técnico ou especializado em comparação ao fornecedor de produtos ou serviços. Esta vulnerabilidade é reconhecida como uma das justificativas para a proteção especial concedida ao consumidor, pois ele geralmente não possui as informações, a expertise ou os recursos necessários para avaliar de forma crítica e segura as características técnicas, riscos e condições dos produtos ou serviços que adquire (Estado de Minas, 2016).

Os produtos bancários, como investimentos, seguros, empréstimos e cartões de crédito, muitas vezes envolvem termos técnicos, condições contratuais complexas e riscos que não são imediatamente evidentes para o consumidor médio. Além disso, com a crescente dependência de canais de atendimento não presenciais podem ocasionar na dificuldade por parte do consumidor dificuldade em avaliar a segurança e a legitimidade dessas comunicações, o que os torna alvos fáceis para fraudes e golpes financeiros (Monteiro, 2022).

A vulnerabilidade jurídica, refere-se à situação de desvantagem do consumidor em relação ao fornecedor devido à sua falta de conhecimento e compreensão das normas e procedimentos legais que regem as relações de consumo. Esse princípio reconhece que o consumidor, muitas vezes, não possui o entendimento necessário sobre seus direitos e deveres legais, bem como sobre os mecanismos de proteção disponíveis, o que pode dificultar a defesa de seus interesses em disputas com fornecedores. Além disso, se manifesta de várias maneiras, incluindo a dificuldade do consumidor em interpretar contratos, compreender cláusulas contratuais complexas ou perceber práticas abusivas e ilegais, sendo que, muitos consumidores não têm acesso fácil a assistência jurídica especializada, o que agrava essa desvantagem frente aos fornecedores que, geralmente, contam com recursos legais e consultoria jurídica (Benjamin, 2008).

No contexto das fraudes bancárias, a carência de compreensão jurídica pode ser explorada por fraudadores que se aproveitam da confiança que os consumidores depositam nas instituições financeiras para realizar golpes sofisticados, como por exemplo, na engenharia social por meio do *phishing*, onde consumidores recebem e-mails ou mensagens fraudulentas que parecem ser de seus bancos, a falta de conhecimento jurídico pode impedir que eles reconheçam a falsidade dessas comunicações e seus direitos de contestar transações originadas de golpes (Monteiro, 2022).

Por conseguinte, a vulnerabilidade informacional refere-se à desvantagem do consumidor decorrente da assimetria de informações entre ele e o fornecedor, isto é, se manifesta quando o consumidor não possui acesso às mesmas informações que o fornecedor sobre os produtos ou serviços, ou quando as informações disponíveis são insuficientes, confusas, incompletas ou técnicas demais para serem compreendidas facilmente (Marques, 2014).

Essa assimetria informacional coloca o consumidor em uma posição desfavorável e pode levá-lo a escolhas inadequadas, insatisfatórias ou até prejudiciais, visto a incapacidade de avaliar corretamente a qualidade, segurança, condições de uso e os riscos associados ao produto ou serviço. Nesse viés, Sérgio Cavalieri Filho diz que “o direito à informação é um reflexo ou consequência do princípio da transparência (...) e encontra-se umbilicalmente ligado ao princípio da vulnerabilidade. Daí é possível dizer que o direito à informação é, primeiramente, um instrumento de igualdade e de reequilíbrio da relação de consumo” (Cavalieri Filho, 2011).

Em suma, pode-se afirmar que as vulnerabilidades do consumidor nas relações bancárias destacam a desigualdade inerente entre os clientes e as instituições financeiras. Para mitigá-las o Código de Defesa do Consumidor (CDC) garante a obrigatoriedade do fornecimento de informações transparentes e compreensíveis, além de garantir a proteção contra práticas abusivas e enganosas. Essas medidas são fundamentais para fortalecer a posição do consumidor, permitindo que ele tome decisões informadas e seguras e se proteja, inclusive, contra fraudes bancárias.

## 3.2 Interpretação das leis e regulamentos aplicáveis

No que diz respeito às operações realizadas pelas instituições financeiras, é indiscutível que elas carregam um risco inerente, ou seja, risco do negócio, que surge pelas atividades desenvolvidas pela entidade e precisa de controle para mitigação. Isso se deve tanto à própria natureza de sua atividade, que envolve a guarda de recursos financeiros, quanto à relação contratual estabelecida com o cliente, que exige o acesso a informações altamente específicas, como documentos e dados pessoais (Monteiro, 2022).

Parte-se do princípio de que a relação jurídica entre as instituições financeiras e seus clientes está regida e firmada pelo Código de Defesa do Consumidor em seu artigo 3°, § 2º:

> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
> [...]
>
> § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, **inclusive as de natureza bancária, financeira, de crédito e securitária**, salvo as decorrentes das relações de caráter trabalhista.

Do mesmo modo, o STJ se posicionou através da Súmula 297, sustentando a relação consumerista expressa no CDC, quando diz que “o Código de Defesa do Consumidor (CDC) é aplicável às instituições financeiras”. Assim, resta configurado que o cliente lesado por casos de fraudes bancárias está expressamente respaldado por esse dispositivo.

No mesmo âmbito da relação consumerista, o CDC em seu artigo 14 aduz sobre a responsabilidade pela reparação de danos causados aos seus consumidores, independentemente da existência de culpa, ou seja, a responsabilidade civil objetiva. Por outro lado, no § 3° do mesmo artigo, expõe as excludentes dessa responsabilidade que se consubstanciam em culpa exclusiva do consumidor e defeito inexistente da prestação de serviços (Villar, 2015).

Contudo, conforme elucidado pela Ministra Nancy Andrighi “Segundo a doutrina e a jurisprudência do STJ, o fato de terceiro só atua como excludente da responsabilidade quando tal fato for inevitável e imprevisível”. Portanto, a culpa exclusiva de terceiros, que pode excluir a responsabilidade objetiva do fornecedor, é

um tipo de evento fortuito externo. Isso se refere a um acontecimento que não tem nenhuma relação de causalidade com a atividade do fornecedor, isto é, completamente alheio ao produto ou serviço (Resp n. 685.662/RJ, julgado em 10/11/2005, DJ 05/12/2005).

O Tema Repetitivo n°466/STJ fixou a responsabilidade objetiva das instituições financeiras em casos de fraudes bancárias e delitos praticados por terceiros como fortuito interno. Concomitante à isso, em 2012 originou-se a Súmula 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” (REsp n. 1.197.929/PR, Segunda Seção, julgado em 24/8/2011, DJe 12/9/2011).

No entanto, conforme entendimento da Relatora Ministra Nancy Andrighi, para estabelecer a relação causal entre a ação de terceiros/golpistas e o vazamento de dados pessoais pelo responsável por seu tratamento, é essencial investigar com precisão quais dados estavam em posse dos criminosos. Isso se faz necessário para determinar a origem do vazamento e, consequentemente, a responsabilidade dos envolvidos (REsp 2.077.278-SP, Terceira Turma, por unanimidade, julgado em 3/10/2023, DJe 9/10/2023). Essa responsabilidade por vazamento de dados se dá pelo amparo e correlação à Lei Geral de Proteção de Dados n°13.709/2018 (LGPD), a qual pontua em seu artigo 6° o tratamento de dados pessoais deve observar o princípio da segurança com a utilização de medidas técnicas e administrativas para proteger os dados pessoais (Giovanini, 2021).

Dessa forma, tendo em vista a responsabilidade civil objetiva das instituições financeiras, resta comprovar que seus mecanismos e procedimentos de segurança são eficientes no combate à fraudes bancárias. Outrossim, não demonstrada prática adequada e constatada a ineficiência dos mecanismos, certifica a aplicação da LGPD, bem como a reparação de danos materiais e morais em consonância com as Súmulas correspondentes (Giovanini, 2021).

Sob a mesma perspectiva, comprovada a participação ativa do consumidor na fraude contestada, ou seja, a culpa exclusiva da vítima, como é o caso do golpe do motoboy, onde a vítima entrega voluntariamente seu cartão nas mãos do golpista, ou a instalação de aplicativos *rackers*, como o AnyDesk, em que o cliente baixa o aplicativo em seu aparelho celular e dispõe livre acesso aos fraudadores à contas bancárias e dados pessoais, os tribunais voltam-se a julgar em favor dos bancos ou à

divisão de prejuízos, o que se mostra relativo e depende da análise do magistrado (Strang, Raffa e Amorim, 2024).

Por fim, é válido ressaltar sob o viés da penalização dos criminosos, que o senador Mecias de Jesus (Republicanos-RR), propôs o Projeto de Lei (PL 650/2022) que altera o Decreto-Lei nº 2848, de 07 de dezembro de 1940 – Código Penal, para dispor sobre fraude bancária. A medida está em tramitação e, estabelece pena de reclusão de 4 a 8 anos para quem dispõe sua conta bancária para que criminosos dinheiro fruto de roubo, sequestro relâmpago, e golpes cometidos após o desvio de aparelhos celulares para posterior transferência bancária via PIX (Agência Senado, 2022).

A tipificação específica do crime de fraude bancária no Código Penal cria um mecanismo legal mais robusto para combater práticas criminosas que envolvem o uso indevido de contas bancárias, incluindo o aluguel de contas para movimentação de dinheiro obtido ilicitamente e traz mais segurança ao consumidor no que diz respeito às relações bancárias.

## 3.3 Casos emblemáticos e análise das decisões judiciais

### 3.3.1 Recurso Especial nº 2.077.278 - SP (2023/0190979-8)

O Recurso Especial nº 2.077.278 - SP (2023/0190979-8), relatado pela Ministra Nancy Andrighi, trata de uma ação declaratória de inexigibilidade de débito devido a vazamento de dados bancários, cumulada com indenização por danos morais e repetição de indébito. Parte-se dos fatos, em que a recorrente argumentou que, devido ao tratamento inadequado de seus dados pessoais pela instituição financeira, o que facilitou a aplicação do golpe do falso boleto, causando-lhe prejuízos financeiros e morais.

Nesse contexto, conforme também citado pela Ministra, já havia sido decidido pela Terceira Turma que “se comprovada a hipótese de vazamento de dados por culpa da instituição financeira, será dela, em regra, a responsabilidade pela reparação integral de eventuais danos. Caso contrário, inexistindo elementos objetivos que comprovem esse nexo causal, não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários

para a aplicação de golpes de engenharia social” (REsp n. 2015732, Re. Ministra Nancy Andrighi, DJe 20/06/2023).

Diante disso, para estabelecer a responsabilidade, faz-se necessário verificar com precisão quais dados estavam em posse dos criminosos e determinar a origem do vazamento, sendo que, a análise dos nexos de causalidade e imputação depende da situação concreta apresentada. Nesse sentido, conforme a Lei Complementar 105/2001, os dados bancários são de tratamento exclusivo das instituições financeiras, que têm a obrigação de manter o sigilo e a segurança dessas informações, sendo que, o armazenamento inadequado que permite acesso por terceiros constitui um defeito na prestação do serviço, previsto no art. 14 do CDC e art. 44 da LGPD.

A decisão do recurso se apoia na Súmula 479 do STJ, assim como no Tema Repetitivo 466/STJ, reforçando a responsabilidade objetiva das instituições financeiras em casos de falha na prestação de serviços e, reconhece também, o princípio do reconhecimento da vulnerabilidade no mercado de consumo, consagrando a aplicação do CDC às relações bancárias, como expresso na Súmula 297/STJ.

Diante de tal fato, a Terceira Turma, por unanimidade, reconheceu e deu provimento ao recurso especial, reformando a decisão do Tribunal de Justiça de São Paulo (TJSP) que havia julgado improcedentes os pedidos da inicial.

### 3.3.2 Recurso Especial nº 1.995.458 – SP (2022/0097188-3)

O Recurso Especial Nº 1.995.458 - SP envolve uma vítima do golpe do motoboy, onde, o recorrente buscava a declaração de inexigibilidade de débitos decorrentes de transações fraudulentas realizadas após ele entregar seu cartão e senha ao estelionatário, além de indenização por danos morais. O REsp questiona a decisão do Tribunal de Justiça do Estado de São Paulo (TJSP), que julgou improcedente a ação, afastando a responsabilidade dos bancos.

A princípio, a primeira instância julgou parcialmente procedente, reconhecendo a inexigibilidade de parte dos débitos e condenando os bancos a restituir os valores das transações fraudulentas. Posteriormente, o Tribunal de Justiça de São Paulo (TJSP) reformou a sentença de primeira instância, julgando

improcedente a ação, alegando que o consumidor foi negligente ao entregar o cartão e fornecer a senha ao golpista.

No entanto, o recurso especial se baseou na violação do artigo 14 do Código de Defesa do Consumidor (CDC), que trata da responsabilidade objetiva dos fornecedores de serviços e trouxe consigo as falhas na adoção de medidas adequadas, por parte da instituição financeira, para proteger os dados e transações, falha na prestação de serviços e a responsabilidade objetiva, independente de culpa.

Nesse sentido, a Ministra Nancy Andrighi reforçou a responsabilidade objetiva das instituições financeiras, previstas na Súmula 479/STJ, no dever de segurança dos serviços prestados, o qual inclui a implementação de mecanismos eficazes para prevenir fraudes e proteger os dados dos consumidores. No caso em questão, a falha na prestação de serviço foi evidenciada pela ausência de medidas preventivas que poderiam ter impedido o golpe. Do mesmo modo, foi estabelecido o nexo causal, o qual se baseou no sentido de que mesmo que o consumidor tenha fornecido o cartão e a senha ao estelionatário, a responsabilidade da instituição financeira prevalece, pois ela deveria ter sistemas de segurança que detectassem e evitassem transações fraudulentas.

Nesse cenário, a Ministra também abordou o princípio da vulnerabilidade, vez que o caso em questão envolvia uma vítima idosa, razão pela qual a imputação de responsabilidade é pautada sob o Estatuto do Idoso (Lei 10.741/2003) e a Convenção Interamericana sobre a Proteção dos Direitos Humanos, e assim, exige um nível mais elevado de cuidado por parte das instituições financeiras.

Nesse sentido, ressaltou-se quanto ao comportamento atípico do uso do cartão, o qual cabe à instituição financeira adotar medidas de segurança que verifiquem a idoneidade das transações por meio da análise do padrão de comportamento do cliente. Justificou-se que, do mesmo modo em que cabe ao consumidor a guarda e segurança de seu cartão, cabe ao banco identificar transações e movimentações que destoam do perfil costumeiro de seu cliente, o qual permeia a responsabilidade do fornecedor, que responde pelo risco da atividade. Vale ressaltar que, conforme entendimento do STJ, essa responsabilidade recai independente de qualquer ato do consumidor, tenha sido ou não decorrido de roubo ou furto (REsp 1.058.221/PR, Terceira Turma, DJe de 14/10/2011; REsp n. 970.322/RJ, Quarta Turma, DJe de 19/3/2010.).

Por fim, a Terceira Turma decidiu por unanimidade dar provimento ao recurso especial, reconhecendo a responsabilidade objetiva do banco pelas transações fraudulentas decorrentes do golpe do motoboy, baseada na falha de segurança do serviço prestado e a vulnerabilidade do consumidor idoso. A decisão do STJ fortalece a proteção dos consumidores, especialmente os hipervulneráveis, e impõe às instituições financeiras a obrigação de adotar medidas mais rigorosas na prevenção à fraudes.

### 3.3.3 Recurso Especial nº 1.197.929 - PR (2010/0111325-0)

O Recurso, julgado pelo Superior Tribunal de Justiça (STJ) e relatado pelo Ministro Luís Felipe Salomão, trata da responsabilidade civil das instituições bancárias por fraudes ou delitos praticados por terceiros, onde, o recorrente ajuizou uma ação declaratória de inexistência de dívida cumulada com pedido de indenização por danos morais, alegando que nunca teve relação jurídica com o banco, mas teve seu nome negativado em cadastros de proteção ao crédito por uma dívida que jamais contraiu, resultante de uma fraude.

O Juízo de Direito da Vara Cível da Comarca de Alto Paraná/PR julgou improcedente o pedido, concluindo que havia uma relação contratual entre as partes, justificando a negativação, sentença essa que foi mantida na apelação, que afirmou que o banco agiu cautelosamente e de boa-fé, afastando a responsabilidade objetiva devido à culpa exclusiva da vítima ou de terceiro. No mesmo sentido, a Federação Brasileira de Bancos – FEBRABAN, parte interessada, argumentou que a instituição financeira não deve ser responsabilizada em caso de fraude por terceiros, destacou falta de nexo causal e que a negativação foi um exercício regular de direito.

Contrariamente, o recorrente sustenta que a prova documental apresentada pelo banco não era suficiente para comprovar a autenticidade das assinaturas, sem a realização de perícia técnica. Do mesmo modo que, a responsabilidade da instituição financeira deveria ser objetiva, baseada no risco do empreendimento, sem possibilidade de culpa exclusiva de terceiros.

O STJ deu provimento ao recurso e estabeleceu que as instituições bancárias são objetivamente responsáveis pelos danos causados por fraudes e delitos praticados por terceiros, isso inclui a abertura de contas correntes ou obtenção de empréstimos mediante documentos falsos. A decisão sublinha que tais fraudes são

inerentes ao risco do negócio bancário (fortuito interno). Portanto, os bancos devem arcar com os prejuízos decorrentes dessas fraudes, independentemente de prova de culpa.

A decisão foi baseada no artigo 14 do Código de Defesa do Consumidor, a qual fez menção à Súmula 28/STF, da década de 60, na qual já responsabilizava os bancos pelo pagamento de cheques falsos, a menos que houvesse culpa concorrente do correntista e, com a vigência do CDC, a responsabilidade objetiva foi reforçada.

Em suma, o REsp em questão é emblemático na jurisprudência brasileira, no que diz respeito a responsabilidade civil das instituições financeiras. Para mais, estabelece que os bancos respondem objetivamente por fraudes praticadas por terceiros e protege os consumidores, ao ponto que impõe um maior rigor à prevenção a fraudes.

# CONCLUSÃO

A responsabilidade civil das instituições financeiras em casos de fraudes bancárias é um tema complexo e de suma importância no contexto da era digital. Este trabalho buscou analisar de maneira abrangente as obrigações legais dessas instituições na prevenção, detecção e mitigação de fraudes, com uma atenção especial às consequências jurídicas e aos mecanismos de proteção ao consumidor.

A digitalização dos serviços financeiros, embora tenha proporcionado maior conveniência e acessibilidade, também trouxe desafios significativos em termos de segurança e regulação. As fraudes bancárias, que se tornaram mais sofisticadas, exigem uma resposta robusta tanto por parte das instituições financeiras, quanto das entidades reguladoras. A legislação brasileira, especialmente o Código de Defesa do Consumidor e o Código Civil, oferece um arcabouço normativo essencial para a proteção dos consumidores, mas é a aplicação prática dessas normas e a jurisprudência que realmente moldam a responsabilidade das instituições financeiras.

A análise detalhada da literatura jurídica, aliada ao estudo de casos concretos, demonstrou que a responsabilidade objetiva das instituições financeiras, conforme estabelecida pela Súmula 479 do Superior Tribunal de Justiça (STJ), é fundamental para assegurar a proteção aos consumidores. Este princípio, que dispensa a prova de culpa, é vital para garantir que os bancos adotem todas as medidas necessárias para prevenir fraudes e ressarcir os clientes prejudicados.

Os mecanismos de prevenção e detecção de fraudes se mostraram essenciais para a proteção dos consumidores e para a manutenção da integridade do sistema financeiro. As instituições financeiras têm a obrigação legal de adotar medidas eficazes de segurança e de gerenciamento de riscos, conforme determinado pela legislação brasileira, incluindo o Código de Defesa do Consumidor, o Código Civil e as diretrizes do Banco Central do Brasil. No entanto, a responsabilidade dessas instituições não se limita à implementação de medidas preventivas, vez que, a prontidão e a eficácia na resposta a incidentes de fraude, transparência na comunicação e adequado suporte são igualmente cruciais.

Ademais, as excludentes de responsabilidade, tais como a culpa exclusiva do consumidor ou de terceiros, foram discutidas detalhadamente, demonstrando que, embora essas excludentes possam ser aplicáveis em determinadas situações, a

responsabilidade primária pela segurança das transações bancárias recai sobre as instituições financeiras. No mais, a aplicabilidade do Código de Defesa do Consumidor à essas entidades reforça a necessidade de uma abordagem centrada na proteção do consumidor, garantindo que as instituições sejam responsáveis por falhas em seus sistemas de segurança.

Em conclusão, a responsabilidade civil das instituições financeiras em casos de fraudes bancárias é um campo dinâmico e em constante evolução, impulsionado pelas mudanças tecnológicas e pelas novas formas de criminalidade. A proteção eficaz dos consumidores exige não apenas um marco regulatório robusto, mas também a implementação de práticas de segurança rigorosas e a manutenção de um diálogo contínuo entre instituições financeiras, reguladores e consumidores.

Assim, espera-se que este estudo contribua para um entendimento mais profundo das responsabilidades envolvidas e para o desenvolvimento de estratégias mais eficazes na prevenção e mitigação de fraudes bancárias e, consequentemente, maior proteção ao consumidor.

# REFERÊNCIAS


**7 tipos de ataques de engenharia social que você precisa se proteger**. STEFANINI GROUP**,** 2022. Disponível em: https://stefanini.com/pt-br/insights/artigos/tipos-de-ataques-de-engenharia-social. Acesso em: 18 abr. 2024.

AGUIAR JÚNIOR, Ruy Rosado de. O Novo Código Civil e o Código de Defesa do Consumidor: pontos de convergência. **Revistas EMERJ**, Rio de Janeiro, v. 6, n. 24, 2003.

ALVES, Cássio B. **Segurança da Informação vs. Engenharia Social:** como se proteger para não ser mais uma vítima. 2010. Sistemas de Informação - Centro Universitário do Distrito Federal – UDF, Brasília, 2010.

**ANÁLISE JURISPRUDENCIAL DA FRAUDE BANCÁRIA: Decisões dos Tribunais e Proteção ao Consumidor.** Strang, Raffa e Amorim, 2024. Disponível em: https://advocaciasra.com.br/analise-jurisprudencial-da-fraude-bancaria-decisoes-dos-tribunais-e-protecao-ao-consumidor-. Acesso em: 6 jun. 2024.

ARAÚJO JÚNIOR, Vital Borba de. **Excludentes de Responsabilidade Civil**. 2014. Graduação Direito – Faculdade IESP, 2014.

ARAÚJO, Eduardo E. **A Vulnerabilidade Humana na Segurança da Informação**. 2005. Licenciatura Sistemas de Informação - Faculdade de Ciências Aplicadas de Minas, Uberlândia, 2005.

**As principais aplicações de IA no combate às fraudes financeiras**. TI INSIDE, 2023. Disponível em: https://tiinside.com.br/12/12/2023/as-principais-aplicacoes-de-ia-no-combate-as-fraudes-financeiras/. Acesso em: 18 abr.2024.

BARBOSA, Xênia de Castro; BEZERRA, Ruth Ferreira. **BREVE INTRODUÇÃO À HISTÓRIA DA INTELIGÊNCIA ARTIFICIAL**. UFAC. v.4, n.2, 2020.

BARONE, Dante. Sociedades Artificiais: **A Nova Fronteira da Inteligência nas Máquinas**. 1. ed. Porto Alegre: Bookman, 2003.

BENJAMIN, Antônio Herman. V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual de Direito do Consumidor**. São Paulo: Revista dos Tribunais, 2008.

**Brasil teve 134 milhões de tentativas de phishing em um ano**. OGLOBO, 2023. Disponível em:

https://oglobo.globo.com/patrocinado/dino/noticia/2023/09/19/brasil-teve-134-milhoes-de-tentativas-de-phishing-em-um-ano.ghtml. Acesso em: 18 abr.2024.

BRASIL. Banco Central do Brasil. **Resolução BCB N°142**. 23 set. 2021. Disponível em: Https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=142. Acesso em: 24 nov. 2023.

BRASIL. Banco Central do Brasil; Conselho Monetário Nacional. **Resolução Conjunta n°6.** 23 mai.2023. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-conjunta-n-6-de-23-de-maio-de-2023-485299560. Acesso em: 24 nov. 2023.

BRASIL. Banco Central do Brasil; Conselho Monetário Nacional. **Resolução BCB n°103.** 08 jun.2021. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-bcb-n-103-de-8-de-junho-de-2021-324759269. Acesso em: 24 nov. 2023.

BRASIL. **Código Civil dos Estados Unidos do Brasil de 1916**. Rio de Janeiro, RJ: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l3071.htm. Acesso em 24 de nov. 2023.

BRASIL. **Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 2002. 11 jan. 2002.

BRASIL. **Lei Nº 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 1990. 12 set. 1990.

BRASIL. Senado Federal. **Projeto de Lei nº 650**, de 21 de março de 2022. Altera Decreto-Lei nº 2848/1940 - Código Penal. São Paulo: Senado Federal, 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/05/03/proposta-cria-crime-de-fraude-bancaria-com-4-a-8-anos-de-reclusao. Acesso em: 06 jun. 2024.

BRASIL. Superior Tribunal de Justiça. **RECURSO ESPECIAL 1.197.929/PR.** Relator: Ministro Luis Felipe Salomão. DJe: 12/9/2011. STJ, 2011. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?cod_doc_jurisp=1130626. Acesso em: 6 jun. 2024.

BRASIL. Superior Tribunal de Justiça. **RECURSO ESPECIAL 1.995.458/SP**. Relatora: Ministra Nancy Andrighi. DJe 18/08/2022. STJ, 2022. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202200971883&dt_publicacao=18/08/2022#:~:text=SRA.-,MINISTRA%20NANCY%20ANDRIGHI%20(Relatora)%3A,v%C3%ADtima%20do%20golpe%20do%20motoboy. Acesso em: 6 jun. 2024.

BRASIL. Superior Tribunal de Justiça. **RECURSO ESPECIAL 2.077.278/SP**. Relatora: Ministra Nancy Andrighi. DJe 9/10/2023. STJ, 2023. Disponível em:

https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301909798&dt_publicacao=09/10/2023. Acesso em: 6 jun. 2024.

BRASIL. Superior Tribunal de Justiça. **RECURSO ESPECIAL 685.662/RJ**. Relatora: Ministra Nancy Andrighi. DJ: 05/12/2005. STJ, 2005. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?cod_doc_jurisp=657510. Acesso em: 6 jun. 2024.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 297**. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Brasília, DF: Superior Tribunal de Justiça, [2004]. Disponível em: https://scon.stj.jus.br/SCON/sumstj/toc.jsp?livre=%27297%27.num.&O=JT. Acesso em: 7 jun. 2024.

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: Superior Tribunal de Justiça, [2012]. Disponível em: https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=479.num. Acesso em: 7 jun. 2024.

BRETAS, Pollyanna. **Fraudes bancárias: veja como funciona novo sistema de rastreamento do BC: bancos terão 24h para avisar**. OGlobo, 2023. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/noticia/2023/11/12/fraudes-bancarias-veja-como-funciona-novo-sistema-de-rastreamento-do-bc-bancos-terao-24h-para-avisar.ghtml. Acesso em: 19 nov.2023.

CAVALIERI FILHO, Sergio. **Programa de direito do consumidor**. 3ª ed. São Paulo: Atlas, 2011.

CAVALIERI FILHO, Sergio. **Responsabilidade Civil no Novo Código Civil**. Revistas EMERJ. v. 6, n. 24, 2003.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil.** 9° ed. rev. e ampl. São Paulo: Atlas, 2010.

CHAVES, Silvia Fernandes. **A vulnerabilidade e a hipossuficiência do consumidor nas contratações eletrônicas**. Barueri: Manole, 2015.

**Comissão dos Direitos do Consumidor da ANADEP participa de audiência pública na Câmara dos Deputados**. ANADEP, 2023. Disponível em: https://www.anadep.org.br/wtk/pagina/materia?id=55990. Acesso em: 22 nov. 2023.

**Como a engenharia social funciona e 4 dicas para se proteger.** SERASA EXPERIAN, 2023. Disponível em: https://www.serasaexperian.com.br/conteudos/prevencao-a-fraude/como-funciona-engenharia-social-e-como-se-proteger/. Acesso em: 18 abr. 2024.

CORREA, Alexandre Augusto de Castro. Introdução ao Direito Romano das obrigações, aplicado ao Direito Civil. **Revistas USP**, n. 2, p. 45–66, 1973.

COSTA, Leandro Silva; PADILHA, Marcelos Fróes; CARNEIRO, Auner Pereira. A Responsabilidade Civil - Origens e evolução do objeto científico. **Revistas FaCJSA**, Conexão acadêmica, n.5, 2014.

DINIZ, Danielly. **Golpes financeiros**: mais de mil tentativas por hora, neste ano. PSAFE, 2022. Disponível em: https://www.psafe.com/blog/golpes-financeiros/. Acesso em: 18 abr. 2024.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro – Responsabilidade Civil**. 19 ed. São Paulo: Saraiva, 2005.

ESCOBAR, Matheus Garcia. **Origem, anatomia e perigos da Engenharia Social no mundo Digital.** UFSM, 2022. Disponível em: https://www.ufsm.br/pet/sistemas-de-informacao/2022/11/14/origem-anatomia-e-perigos-da-engenharia-social-no-mundo-digital#:~:text=COMO%20SURGIU%3F,industrial%20holand%C3%AAs%20JC%20Van%20Marken. Acesso em: 18 abr. 2024.

ESTADO, Agência. **Pix leva a explosão em transações bancárias desde 2021, e também aumenta fraudes, diz Febraban**. OPovo, 2023. Disponível em: https://www.opovo.com.br/noticias/economia/2023/10/26/pix-leva-a-explosao-em-transacoes-bancarias-desde-2021-e-tambem-aumenta-fraudes-diz-febraban.html. Acesso em: 19 nov. 2023.

FACHINI, Thiago. **Lei Carolina Dieckmann**: Tudo o que você precisa saber sobre. PROJURIS, 2023. Disponível em: https://www.projuris.com.br/blog/lei-carolina-dieckman-tudo-o-que-voce-precisa-saber-sobre/#:~:text=A%20Lei%20Carolina%20Dieckmann%20disp%C3%B5e,sem%20a%20autoriza%C3%A7%C3%A3o%20da%20mesma. Acesso em: 18 abr. 2024.

**Febraban Tech 2023: Como proteger seus clientes de golpes sem que sejam experts no tema**. INCOGNIA, 2023 Disponível em: https://www.incognia.com/pt/conteudos/assista-palestra-febraban-tech-2023. Acesso em: 18 abr. 2024.

**Fraudes contra clientes de bancos crescem 165% em 2021**. O POPULAR, 2021. Disponível em: https://opopular.com.br/economia/fraudes-contra-clientes-de-bancos-crescem-165-em-2021-1.2345543. Acesso em: 18 abr. 2024.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil–Responsabilidade Civil**. 10. ed. São Paulo: Saraiva, 2012.

GILISSEN, John. **Introdução histórica ao direito**. Tradução de António Manuel Hespanha e Manuel Macaísta Malheiros. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 2001. p. 751.

GIOVANINI, Karen Silva. **A lei geral de proteção de dados e as fraudes bancárias.** JUSBRASIL, 2021. Disponível em: https://www.jusbrasil.com.br/artigos/a-lei-geral-de-protecao-de-dados-e-as-fraudes-bancarias/1278379901. Acesso em: 6 jun. 2024.

**Golpe da falsa central de atendimento ganha nova versão: saiba como se proteger**. BANCO DO BRASIL, 2023. Disponível em: https://blog.bb.com.br/golpe-0800/#:~:text=Como%20se%20proteger%20do%20golpe,-%E2%80%93%20Liga%C3%A7%C3%B5es%20recebidas%20por&text=%E2%80%93%20O%20BB%20n%C3%A3o%20realiza%20chamadas,por%20SMS%20ou%20outras%20mensagens. Acesso em: 18 abr. 2024.

**Golpes Bancários: quais os principais e como se prevenir**. BANCO MASTER, 2023. Disponível em: https://www.bancomaster.com.br/blog/golpes-bancarios-principais-como-prevenir. Acesso em: 18 abr. 2024.

GONÇALVES, Carlos Roberto. **Direito Civil**. São Paulo: Saraiva, 2020.

HIRONAKA, Giselda Maria Fernandes Novaes. **Responsabilidade pressuposta**. Belo Horizonte: Del Rey, 2005. p. 53- 57.

LIMA, Alvino. **Culpa e risco**. 2. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 1999.

LOPES, Silvana. **Sistemas Especialistas na Educação**. Ariquemes: Universidade Federal de Rondônia, 2008.

MARQUES, Claudia Lima. **Contratos no código de defesa do consumidor: o novo regime das relações contratuais.** 7° ed. São Paulo: Revista dos Tribunais, 2014.

MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 8. Ed. São Paulo: Revista dos Tribunais, 2020.

MIRAGEM, Bruno. **Direito do consumidor:** fundamentos dos direitos do consumidor; direito material e processual do consumidor; proteção administrativa do consumidor; direito penal do consumidor. São Paulo: Revista dos Tribunais, 2008.

MIRAGEM, Bruno. Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo. In: MIRAGEM, Bruno; MARQUES, Claudia Lima; MAGALHÃES, Lucia Ancona Lopez de. (Org.). **Direito do Consumidor: 30 anos do CDC**. 1ª. Ed. São Paulo: Forense, 2020.

MIRAGEM, Bruno. **O direito privado e a proteção dos vulneráveis**. 2. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014.

MONTEIRO, André de Oliveira. **A RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS EM CASOS DE GOLPES CONTRA CORRENTISTAS.** 2022. Monografia (Graduação em Direito) – Curso de Direito – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2022.

MONTENEGRO, Rosa Livia Gonçalves; *et al*. Influência da crise financeira de 2008: uma análise sobre a tecnologia da informação dos maiores bancos do consolidado financeiro brasileiro. **Revista do Desenvolvimento Regional**. n.2, p. 2454-2476, 2020.

NETO, Roberto Campos. **Com a digitalização, o sistema financeiro do futuro começa a ser desenhado**. InfoMoney, 2021. Disponível em: https://www.infomoney.com.br/especiais/ed01/com-a-digitalizacao-o-sistema-financeiro-do-futuro-comeca-a-ser-desenhado/. Acesso em: 19 nov.2023.

**O que é engenharia social?**. KAPERSKY. Disponível em:https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 18 abr. 2024.

**Pare e pense, pode ser golpe**. FEBRABAN, 2023. Disponível em: https://antifraudes.febraban.org.br/#golpe-da%20falsa%20central%20de%20atendimento. Acesso em: 18 mar. 2024.

PEREIRA, Júlia Sulzbach Fichtner. **A RESPONSABILIDADE CIVIL DO FORNECEDOR PELOS RISCOS DO DESENVOLVIMENTO**. 2018. Monografia (Graduação em Direito) – Curso de Direito – Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS, Rio Grande do Sul, 2018.

**Pesquisa global sobre fraude bancária**. KPMG. Disponível em: https://assets.kpmg.com/content/dam/kpmg/br/pdf/2019/08/br-pesquisa_global_de_fraude.pdf. Acesso em: 18 abr.2024.

REZENDE, Luiz Paulo Fontes de. **Inovação tecnológica e a funcionalidade do sistema financeiro:** uma análise de balanço patrimonial dos bancos no Brasil. 2012. Tese de Doutorado. Universidade Federal de Minas Gerais – UFMG, Minas Gerais, 2012.

ROCHA, Douglas. **ENGENHARIA SOCIAL: COMPREENDENDO ATAQUES E A IMPORTÂNCIA DA CONSCIENTIZAÇÃO**. UOL, 2018. Disponível em: https://meuartigo.brasilescola.uol.com.br/atualidades/engenharia-social-compreendendo-ataques-importancia-conscientizacao.htm. Acesso em: 18 abr. 2024.

SANTIAGO, Abinoan. **Se liga: estes são os 20 golpes mais manjados de fraude bancárias.** UOL, 2024. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2024/01/03/golpes-online-fraude-bancaria-mais-comuns-brasil.htm. Acesso em: 18 mar. 2024.

**Seis tecnologias usadas pelos bancos na prevenção e combate a fraudes**. FEBRABAN, 2019. Disponível em: https://portal.febraban.org.br/noticia/3385/pt-br/. Acesso em: 21 nov. 2023.

SILVA NETO, Orlando Celso da. **Comentários ao Código de Defesa do Consumidor**. Rio de Janeiro: Forense, 2013.

SILVA, Bianca Ruiz; KALASSA, Renata S. Longo; CALLEGARO, Ciro José. **As fraudes bancárias e a responsabilidade civil das instituições financeiras.** Falletti Advogados, 2022. Disponível em: https://fallettiadvogados.com.br/artigos/as-fraudes-bancarias-e-a-responsabilidade-civil-das-instituicoes-financeiras/. Acesso em: 19 nov. 2023.

SILVA, De Plácido e. **Vocabulário jurídico conciso**. Rio de Janeiro. Forense, 2008.

SILVEIRA, Neil Alessandro Medeiros. **O Princípio da Vulnerabilidade perante o Código de Defesa do Consumidor.** JUSBRASIL, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/o-principio-da-vulnerabilidade-perante-o-codigo-de-defesa-do-consumidor/1577310506. Acesso em: 03 jun.2024.

SOUZA, Wendell Lopes Barbosa de. **A perspectiva histórica da responsabilidade civil**. 2009. Tese (Mestrado em Direito) – Curso de Direito – Pontifícia Universidade Católica de São Paulo, PUC-SP, São Paulo, 2009.

STOCO, Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência**. São Paulo: Editora Revista dos Tribunais, 2007.

TARTUCE, Daniel Amorim Assumpção Neves. **Manual de Direito do Consumidor**. São Paulo: Método, 2018.

TCHILIAN, Felipe. **Tecnologia Bancária: tendências e desafios de segurança.** CLEARSALE, 2022. Disponível em: https://blogbr.clear.sale/tecnologia-bancaria-tendencias-e-desafios-de-seguranca. Acesso em: 18 abr. 2024.

**Tentativas de fraudes e golpes mais comuns com o Pix: conheça quais são e saiba como evitá-los.** FEBRABAN, 2023. Disponível em: https://portal.febraban.org.br/noticia/3903/pt-br/. Acesso em: 18 mar. 2024.

VENOSA, Silvio de Salvo. **Código Civil Interpretado**. São Paulo: Atlas, 2010.

VILLAR, Alice Saldanha. **A responsabilidade civil dos bancos por fraudes e delitos praticados por terceiros em operações bancárias**. JUSBRASIL, 2015. Disponível em: https://www.jusbrasil.com.br/artigos/a-responsabilidade-civil-dos-bancos-por-fraudes-e-delitos-praticados-por-terceiros-em-operacoes-bancarias/241116662. Acesso em 03 jun. 2024.

**Vulnerabilidade no CDC.** ESTADO DE MINAS, 2016. Disponível em: https://www.em.com.br/app/noticia/direito-e-justica/2016/10/03/interna_direito_e_justica,828595/vulnerabilidade-no-cdc.shtml. Acesso em: 18 mai. 2024.

**b**