FACULDADES INTEGRADAS DE BAURU- FIB

DIREITO

Gabriel Alves de Assis

FRAUDES EM CONTRATOS BANCÁRIOS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Bauru

2025

Gabriel Alves de Assis

FRAUDES EM CONTRATOS BANCÁRIOS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Monografia apresentada às Faculdades Integradas de Bauru para obtenção do título de Bacharel em Direito, sob a orientação da Prof.ª **Márcia Regina Negrisoli Fernandez Polettini**

Bauru
2025

Assis, Gabriel Alves de.

Fraudes em contratos bancários e a lei geral de proteção de dados (LGPD)

Assis, Gabriel Alves de. Bauru, FIB, 2025.

43f.

Monografia, Bacharel em Direito. Faculdades Integradas de Bauru - Bauru

Orientador: Prof.ª Márcia Regina Negrisoli Fernandez Polettini

1. Fraudes bancárias. LGPD. Proteção de dados. Segurança da informação. Responsabilidade.

CDD 340

Gabriel Alves de Assis

FRAUDES EM CONTRATOS BANCÁRIOS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Monografia apresentada às Faculdades Integradas de Bauru para obtenção do título de Bacharel em Direito,

Bauru, xx de xxxxxxx de 2025.

Banca Examinadora:

Presidente/ Orientador: Prof.ª Márcia Regina Negrisoli Fernandez Polettini

Professor 1: Prof. Paulo Henrique Silva Godoy

Professor 2: César Augusto Michelli

Bauru
2025

Dedico este trabalho à minha família, pelo apoio incondicional, incentivo constante e paciência durante toda a minha trajetória acadêmica. Às amizades que me motivaram e estiveram presentes nos momentos de desafio, oferecendo palavras de encorajamento e confiança. Sem esse suporte, a realização deste TCC não teria sido possível.

AGRADECIMENTOS

Agradeço a Deus pela força e sabedoria ao longo desta jornada.

À minha família, pelo apoio, paciência e incentivo em todos os momentos.

À minha orientadora, Prof.ª Márcia Regina Negrisoli Fernandez Polettini, pela atenção, orientação e dedicação.

E a todos que, de alguma forma contribuíram para a realização deste trabalho, deixo aqui minha gratidão.

“A injustiça num lugar qualquer é uma ameaça à justiça em todo o lugar”.

(Martin Luther King)

ASSIS, Gabriel Alves de. **Fraudes em contratos bancários e a lei geral de proteção de dados (LGPD)**. 2025. 43f. Monografia apresentada às Faculdades Integradas de Bauru, para obtenção do título de Bacharel em Direito. Bauru, 2025.

RESUMO

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, tem sido considerada em instrumento fundamental para a prevenção das fraudes bancárias. Com o avanço das tecnologias digitais e o aumento das transações eletrônicas, as instituições financeiras passaram a lidar com grandes volumes de informações pessoais e sensíveis, tornando-se alvos frequentes de fraudes e vazamentos de dados. A pesquisa evidencia que a LGPD estabelece diretrizes claras sobre o tratamento, armazenamento e compartilhamento de dados, impondo às instituições o dever de adotar medidas técnicas e administrativas que assegurem a proteção das informações. Observa-se que a aplicação efetiva da lei contribui para a redução de vulnerabilidades, reforçando a transparência e a confiança entre bancos e consumidores. Além disso, a legislação atua de forma preventiva, educativa e sancionatória, responsabilizando agentes que não garantem a segurança necessária. Conclui-se que a conformidade com a LGPD é indispensável para o fortalecimento da segurança digital, para a proteção dos direitos dos titulares de dados e para a construção de um ambiente financeiro mais ético, seguro e confiável frente aos desafios impostos pelas fraudes bancárias no contexto atual.

Palavras-chave: Fraudes bancárias. LGPD. Proteção de dados. Segurança da informação. Responsabilidade.

ASSIS, Gabriel Alves de. **Fraud in banking contracts and the general data protection law (LGPD)**. 2025. 43f. Monografia apresentada às Faculdades Integradas de Bauru, para obtenção do título de Bacharel em Direito. Bauru, 2025.

ABSTRACT

The General Data Protection Law (LGPD), Law No. 13.709/2018, has been considered a fundamental instrument for preventing bank fraud. With the advancement of digital technologies and the increase in electronic transactions, financial institutions have begun to handle large volumes of personal and sensitive information, becoming frequent targets of fraud and data breaches. Research shows that the LGPD establishes clear guidelines on the processing, storage, and sharing of data, imposing on institutions the duty to adopt technical and administrative measures that ensure the protection of information. It is observed that the effective application of the law contributes to the reduction of vulnerabilities, reinforcing transparency and trust between banks and consumers. Furthermore, the legislation acts in a preventive, educational, and punitive manner, holding accountable agents who fail to guarantee the necessary security. It is concluded that compliance with the LGPD (Brazilian General Data Protection Law) is indispensable for strengthening digital security, protecting the rights of data subjects, and building a more ethical, secure, and reliable financial environment in the face of the challenges posed by banking fraud in the current context.

Keywords: Banking fraud. LGPD. Data protection. Information security. Responsibility.

SUMÁRIO

1 INTRODUÇÃO

As fraudes bancárias têm se tornado um dos principais desafios enfrentados pelas instituições financeiras e pelos consumidores, considerando especialmente, o contexto e realidade dos avanços tecnológicos e da transformação digital que cada dia mais, faz parte do cotidiano da sociedade.

O aumento das transações eletrônicas e o uso intenso de dados pessoais ampliaram as possibilidades de ataques cibernéticos que não raramente, surgem acompanhados de manipulações indevidas de informações, apontando para a indispensabilidade de haver atenção expressa e consistente em relação à segurança e privacidade desses dados.

Na observância dessas afirmativas, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, surge como um marco regulatório essencial, visando primordialmente, assegurar garantias de transparência, responsabilidade e a proteção dos dados pessoais, determinando diretrizes para o tratamento e a manejo dessas informações.

Em se tratando de operações bancárias, tem-se que a aplicação da LGPD é de relevância indiscutível, acentuando o entendimento de que o setor financeiro lida diariamente com dados sensíveis e estratégicos de seus clientes, cabendo o dever de primar pela privacidade dos mesmos. Compreende-se que seja fundamental que como as políticas de privacidade, protocolos de autenticação e mecanismos de monitoramento, sejam pensadas e colocadas em prática no propósito de fomentar a construção de uma cultura organizacional validada pela proteção de dados e prevenção de fraudes.

Interessa pontuar que uma correta implementação dos princípios dessa lei, envolvendo aspectos como a finalidade e a necessidade de segurança, requer que as instituições bancárias, busquem adotar práticas mais rigorosas no tratamento das informações, para fins de combater as vulnerabilidades existentes, promovendo maior controle sobre o fluxo de dados.

Estabelecendo regras claras inerentes ao uso e compartilhamento de informações pessoais, a LGPD, pode contribuir para promover maior conscientização sobre o valor e a sensibilidade dos dados, incentivando comportamentos mais seguros no ambiente digital. Além disso, a referida lei, pode ainda comportar um caráter educativo e preventivo, sinalizando a redução da prática

ilícita, ajudando no fortalecimento da confiança entre instituições e consumidores, promovendo um ambiente digital mais seguro.

Dessa forma, compreender a relação entre as fraudes bancárias e a LGPD é fundamental para identificar mecanismos de prevenção, mitigação de riscos e responsabilização diante de incidentes de segurança, capazes de comprometer de forma significativa a vida financeira das pessoas e o desenvolvimento produtivo das instituições.

Assim observado, a partir de uma revisão de literatura com base em pesquisa bibliográfica, este trabalho, discorreu sobre a importância da LGPD na prevenção e no combate às fraudes bancárias, destacando os principais aspectos legais, tecnológicos e éticos, envolvidos na proteção da informação e na garantia dos direitos dos titulares de dados.

2 FRAUDES BANCÁRIAS NO CENÁRIO ECONÔMICO

As instituições bancárias ocupam uma posição de suma importância na sociedade contemporânea e respondem por atuação incisiva nas ações e intermediações financeiras, abarcando uma diversidade de negócios, operações e transações que são necessárias no dia a dia das pessoas (físicas ou jurídicas), movimentando o sistema econômico como um todo (Lima, 2023).

Neste enfoque, a Lei n°4.595 de 31 de dezembro de 1964 que trata sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, dispõe que:

> Art. 17. Consideram-se instituições financeiras, para os efeitos da legislação em vigor, as pessoas jurídicas públicas ou privadas, que tenham como atividade principal ou acessória a coleta, intermediação ou aplicação de recursos financeiros próprios ou de terceiros, em moeda nacional ou estrangeira, e a custódia de valor de propriedade de terceiros (Brasil, 1964, art. 17).

Sobre as atividades e ou prestação de serviços realizada pelas instituições bancárias, na observância de direitos e obrigações que cabem aos envolvidos, as relações estabelecidas entre um sujeito ativo (credor) e um sujeito passivo (devedor), são determinantes para o alcance dos propósitos pretendidos por ambas as partes (Costa, 2013).

A partir destes apontamentos, cabe considerar que os contratos bancários têm papel relevante nessas relações firmadas entre os Bancos e seus clientes. Segundo Coelho (2016), trata-se de instrumentos jurídicos que documentam as atividades e as intermediações de recursos monetários, incluindo a captação e o fornecimento financeiro.

Segundo Tartuce (2013), os contratos são tidos como formas de acordos que contemplam a concordância dos interesses envolvidos e de fatores secundários. A validação de um contrato depende da legalidade do conteúdo e do seu propósito, devendo estar fundamentado na legislação, considerando a sua utilidade social, econômica, respeitando a honestidade.

Acompanhando o crescimento econômico e a adesão tecnológica pela sociedade como um todo, os Bancos tradicionais foram se rendendo à concepção e implementação de novas tecnologias com a validação funcional de Bancos Digitais, favorecendo o acesso aos serviços, impulsionando o as operações financeiras (Moura *et al.*, 2023), colaborando para o aumento de clientes e dos diferentes

contratos que são firmados entre as partes interessadas.

> A inovação tecnológica, com promoção da inclusão digital, foi uma aliada para diversificar a oferta de serviços e melhorar o acesso ao sistema financeiro. Ela permitiu que os *players* tradicionais e os novos entrantes melhorassem a eficiência do sistema [...] (Sperancini; Alexandre, 2024, p.137).

A princípio este cenário parece estar repleto de positividade e de possibilidades de desenvolvimento mais satisfatório das atividades bancárias. No entanto e conforme Santos (2023), os Bancos e seus correntistas têm vivenciado constantes experiências decorrentes de fraudes em contratos bancários que seguem crescendo de modo assustador.

Por outro lado, as facilidades de acesso à *internet* e aos meios de comunicação, inerentes ao mundo contemporâneo, vem colaborando para evidenciar divulgações que têm se tornado cada vez mais frequentes em relação a ocorrência de fraudes (Pereira; Silva, 2020).

Na percepção de Wells (2014), o conceito de fraude refere-se a qualquer benefício conquistado por meio ilícito, usando o erro como elemento central do *modus operandi.* Ressalta-se que o atrelamento entre fraude e erro não significa que todo erro, corresponde a uma fraude.

Práticas fraudulentas utilizam de forma criminosa as informações confidenciais das pessoas, gerando inúmeros prejuízos financeiros a todos os envolvidos (Santos, 2023). No caso de fraudes bancárias, podem representar transtornos substanciais para os Bancos e clientes, configurando: “[...] qualquer ato enganoso, de má-fé, com o intuito de lesar ou ludibriar alguém, ou de não cumprir determinado dever” (Bacigalupo, 2005, p.109).

Outros conceitos apresentados trazem com mais clareza o sentido de fraude, explicitando que este tipo de ação impacta negativamente nas atividades bancárias, especialmente no que tange aos contratos. De acordo com Ribeiro; Fermentão (2023), os efeitos da prática fraudulenta podem levar a anulação do contrato, se for demonstrado que uma das partes interessadas foi induzida ao erro.

Diante destas circunstâncias, considerando os campos empresariais e de negócios ativos e atuantes no meio comercial, o setor bancário é o que mais vem sofrendo com as fraudes em contratos. Pesquisas realizadas no segundo semestre de 2022, mostraram que nos últimos 12 meses um número aproximado de 8,4

milhões de pessoas foi vítima de fraudes bancárias. Esses golpes financeiros incluíram produtos, serviços, créditos e diferentes contratos (Sakamoto, 2023).

Importante enfatizar que as instituições financeiras têm firmado contratos eletrônicos com seus clientes, possibilitando uma otimização e maior agilização do tempo para ambas as partes. Os contratos eletrônicos são então interpretados como providencial ferramenta para o comércio, mas também, estão elencados como um dos alvos das fraudes (Matheus; Nocetti, 2023).

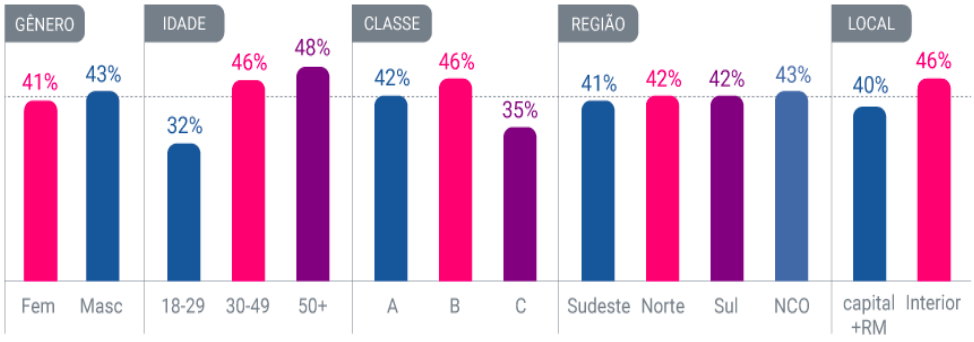
As fraudes bancárias acontecem de diferentes maneiras e conforme Janeri Filho (2023), as práticas fraudulentas podem envolver desde a falsificação de assinaturas eletrônicas simples ou através da invalidação de assinaturas digitais avançadas e ou por meio de certificados digitais de terceiros.

A questão das fraudes bancárias é tema de preocupação e atenção justificável com impactos que repercutem na sociedade como um todo:

> No panorama atual as fraudes mais comuns envolvem clientes que tem relacionamento com alguma instituição financeira ou que, sem ligação com qualquer instituição financeira, tiveram fragilizados seus dados bancários pessoais. Em qualquer das situações, diante da sagacidade dos criminosos, eles acreditam estar em um ambiente seguro, e acabam sendo manipulados e realizando transações financeiras (Veloso, 2024, p.133).

As vítimas, estão mais concentradas nas regiões do interior do país, em comparação com as metropolitanas e esse crime não exclui pessoas com menor renda, embora priorizem aquelas com maior poder aquisitivo nas variadas faixas-etárias, com índices crescentes para os 50+ (Serasa *Experian*, 2024), como pode ser verificado na representação a seguir (Figura 1):

Figura 1: Representação gráfica do perfil das vítimas de fraudes bancárias



Fonte: Serasa *Experian*, 2024.

Partindo deste ponto, as fraudes bancárias podem abarcar registro de situações descritas por:

> [...] condutas de terceiros que buscam alterar, com o uso de tecnologia, a finalidade de algumas transações bancárias, dentre elas, o pagamento, transferências, contratações de empréstimos ou serviços, bem como obtenção indevida de dados sigilosos. É nessa condição que entendemos as fraudes bancárias, como sendo aquela que de qualquer sorte buscam alterar a finalidade das atividades envolvendo as relações entre correntistas (consumidores) e instituição bancária (Ribeiro *et al*., 2023, p.3).

Em se tratando de Bancos Digitais e o grande número de clientes deste tipo de instituição financeira, o aumento de fraudes é contínuo e persistente e segundo é destacado pela Federação Brasileira de Bancos (Febraban), os fraudadores têm aplicado técnicas de engenharia social para realizar os golpes digitais (Campêlo, 2024), elevando de forma assustadora as taxas dessas ocorrências, ainda que condenáveis pela legislação.

Faz-se, pois saber, que a prática do crime de fraude está tipificada no Código Penal brasileiro, artigo 171: “Obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento” (Brasil, 1940), portanto entende-se que essas práticas precisam ser combatidas em prol da proteção da sociedade como um todo.

Conforme pesquisas realizadas pela Federação Brasileira de Bancos (Febraban), a repercussão das fraudes financeiras nas instituições bancárias totalizaram entre 2022 e 2024, um valor estimado em R$ 10,1 bilhões de prejuízos (De Luca, 2025) e infelizmente essas práticas vêm se tornando cada vez mais sofisticadas e não raramente, são assustadoras na ousadia e na dimensão dos impactos que causam.

Sob este prisma, as fraudes bancárias podem ser desafiadoras, tanto para as instituições como para os clientes e saber de fato se uma pessoa está intencionada a cometer este crime é praticamente impossível. As variadas formas de fraudes seguem dificultando cada vez mais, a identificação dos golpes (Campos *et al.* 2023).

Considerando a interconexão digital presente no mundo contemporâneo não se pode negar que te ficado evidente “[...] o aumento de golpes e fraudes financeiras que se utilizam de técnicas cada vez mais sofisticadas de um campo denominado “engenharia social” (Câmpelo, 2024, n.p).

Engenharia social está associada à tecnologia da informação e ao uso de

técnicas de manipulação psicológica que são aplicadas na intenção de conseguir dados privados de pessoas, alcançando vantagens financeiras (Monteiro, 2022).

Uma diversidade de mecanismos é usada pela engenharia social para praticar golpes e fraudes. Além de interações presenciais, são muito comuns as ligações telefônicas, redes sociais e os *phishing* e ou mensagens falsas enviadas via *e-mails.* Geralmente os engenheiros sociais usam informações coletadas por meio da *internet* e com base nesses dados, constroem planejamentos de abordagens personalizadas e de técnicas psicológicas para fazer vítimas (Campêlo, 2024).

Outro meio usado pelos criminosos é o *pharming* que vem sendo considerado um formato mais evoluído do *phishing*, em que o fraudador:

> [...] ataca diretamente o Sistema de Nomes e de Domínio, mais conhecido pela nomenclatura em inglês *Domain Name System* ou DNS, qual o possibilita redirecionar automaticamente o consumidor do *site* legítimo do banco para uma versão falsificada, *site* espelho, que normalmente é construída de forma extremamente similar a página da instituição financeira. Desta forma, apesar do consumidor digitar o URL correto da instituição este é redirecionado ao *site* falso fazendo acreditar estar no endereço eletrônico legítimo do banco, disponibilizando seus dados pessoais e bancários sem suspeita alguma de estar sendo vítima de uma fraude (Gonçalves, 2021, p. 66).

Utilizando engenharia social, os criminosos aproveitam do desconhecimento sobre os golpes existentes ou da falta de entendimento de como identificá-los, usando de persuasão e até mesmo, abusando da confiança que as pessoas depositam em determinado sistema para a obtenção de dados bancários e senhas de acesso. Em muitas situações, induzem a vítima a realizar a instalação de *malwares* em seus dispositivos, abrindo acesso às informações privadas dessas vítimas (Monteiro, 2022).

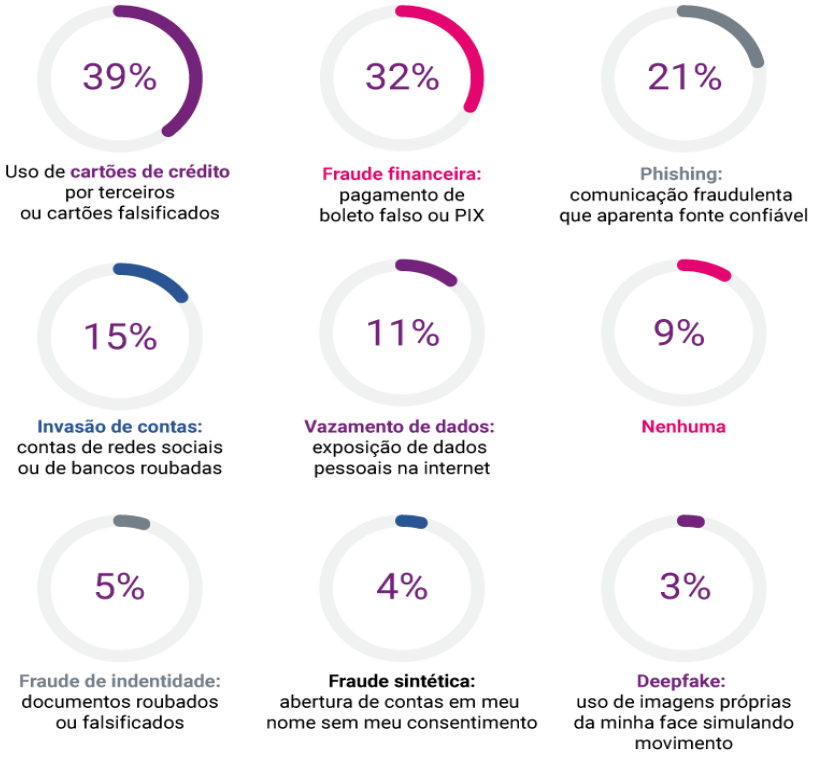
Neste segmento, cabe salientar que existe uma diferença dos ataques cibernéticos que se fundamentam em falhas técnicas, haja vista que a engenharia social acontece a partir da exploração das vulnerabilidades humanas com o foco maios centrado nos aspectos psicológicos (Câmpelo, 2024).

A partir desta concepção, as espécies de fraudes no âmbito bancário podem estar relacionadas com o golpe do pix, perfil falso do *whatsapp*, golpe com QR Code, golpe da mão fantasma, *phising smishing* bancário, golpe da falsa central de atendimento, golpe da troca de cartão, *site, link* ou perfil/página de rede social falsa das instituições bancárias, capturador de sessões, SMS fraudulento, clonagem de

whatsapp, golpe do *motoboy*, golpe do boleto falso e golpe do depósito prévio para liberação de empréstimo, entre outros (Campos *et al.* 2023).

Dentre os vários registros de fraudes, a Serasa *Experian,* divulgou conforme pesquisa realizada em 2024, os tipos que mais afetam a população (Figura 2):

Figura 2: Tipos mais comuns de fraudes bancárias em 2024



Fonte: Serasa *Experian*, 2024.

Embora tenha seus favorecimentos enquanto ferramenta centrada principalmente na criação de conteúdos e imagens (EVG, 2024), a inteligência generativa (IA Generativa) também tem colaborado para o aumento das fraudes.

Nas mãos de criminosos fraudadores a IA generativa tem sido um mecanismo poderoso e sofisticado para vitimar pessoas, empresas e instituições bancárias. Através dos algoritmos de IA generativa, ocorre a manipulação de dados privados, criando-se identidades e aberturas de contas bancárias falsificadas com resultantes de fraudes que seguem crescendo em escala sem precedentes, além de manipulações de vídeos e imagens falsas que não despertam qualquer desconfiança e até mesmo, a geração de áudios artificiais utilizados para romper sistemas tradicionais de segurança e de autenticação, sendo que essas ações

criminosas podem ser executadas em poucos minutos a partir de comandos digitais (Serasa *Experian*, 2025).

A constância desses eventos vem impactando na economia e cooperando com o aumento de reclamações e principalmente tem levado os clientes das instituições bancárias, vítimas de fraudes, a buscarem pelo Poder Judiciário para fins de que as responsabilidades em relação aos prejuízos sejam apuradas (Martins; Kim; Stavropoulos, 2023).

3 O SISTEMA BANCÁRIO, *FINTECHS* E AS FRAUDES BANCÁRIAS

As instituições financeiras que compõem o sistema bancário tradicional no Brasil seguem uma regulamentação rigorosa, formada por um grande número de agências que estão aportadas sobre uma consistente infraestrutura (Pereira *et al*., 2025). Esta realidade demarcada tradicionalmente por longa trajetória do domínio de agências bancárias físicas vem se modificando de maneira consistente, desde a pandemia de 2020, em razão do crescimento dos Bancos digitais (Moreira, 2023).

Não se pode negar que o cenário econômico está sob evolução constante, passando por transformações, instabilidades e inovações que colaboram na construção de reformulações em amplitude global (Moreira, 2023). Neste sentido, as *fintechs,* surgem e configuram elementos de potencial influência sobre os sistemas bancários, vistas como "[...] agente da sexta onda de inovação bancária, tendo como principal novidade a exploração criativa e disrupta das oportunidades negligenciadas pelos bancos no mercado de atuação" (Cernev; Diniz, 2019, p. 6),

O sentido de *Fintech* está contextualizado pelo termo "*financial technology*", trazendo uma combinação de tecnologia e finanças com o propósito de possibilitar soluções financeiras inovadoras (Pazarbasioglu *et al*.,2020).

Conceituando *Fintechs,* "são empresas que introduzem inovações nos mercados financeiros através do uso intenso de tecnologias e com potencial de criar novos modelos de negócios [...]" (Falcão, 2022, p.5). Sob esta ótica e em se tratando de serviços financeiros digitais disponibilizados pelas instituições bancárias, o surgimento das *fintechs* é destaque no mercado econômico *e* referenciada como:

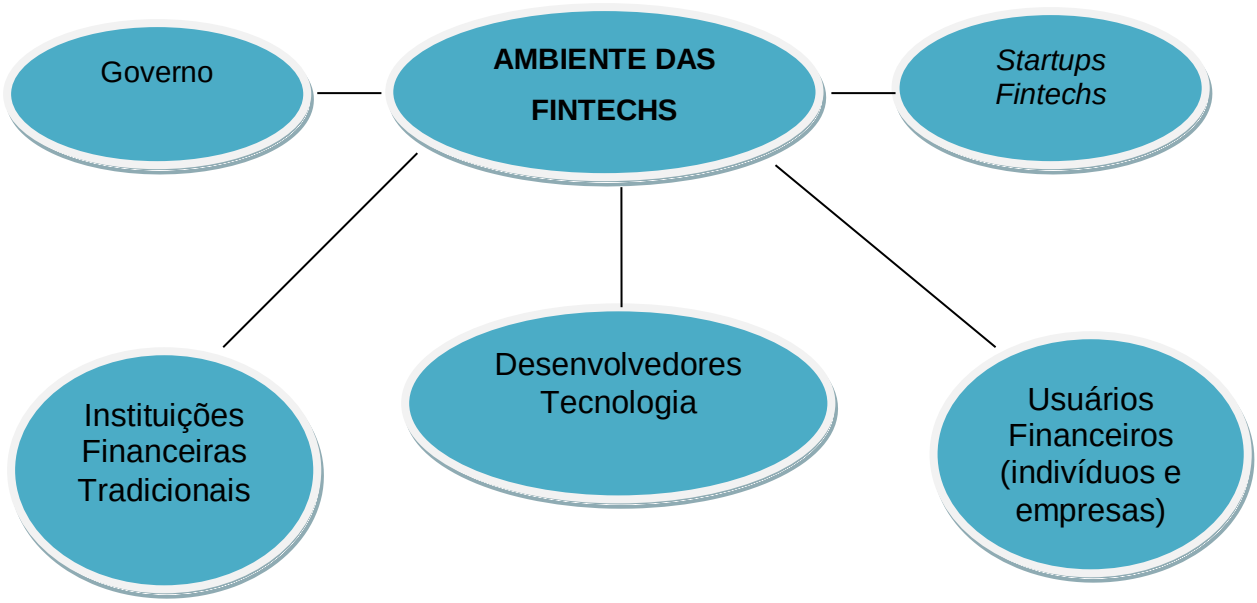
> [...] tecnologias digitais com potencial para transformar a prestação de serviços financeiros, estimulando o desenvolvimento de novos modelos de negócios, aplicativos, processos e produtos existentes ou modificando-os. Na prática, o termo "*fintech*" também é amplamente utilizado para denotar a onda contínua de novos DFS. Exemplos dessas tecnologias incluem *web*, dispositivos móveis, serviços em nuvem, aprendizado de máquina, identidade digital e Interfaces de Programação de Aplicativos (APIs) (Pazarbasioglu *et al*.,2020, p.1).

A partir de plataformas *online*, diversos recursos tecnológicos e aplicativos, as *fintechs* imprimem atuação diferenciada no mercado, voltada para oferta de produtos e serviços financeiros totalmente digitais que podem ser acessados pelos usuários e clientes por meio de *smartphones* ou *desktops* de forma ágil e facilitada. É possível dizer que as *fintechs* seguem revelando possibilidades positivas consolidação no

mercado, principalmente quando se trata de questões envolvendo a solução de democratização do acesso aos bancos (CNN Brasil, 2023).

O ambiente das *fintechs* é dinâmico e pode-se dizer que está composto por cinco elementos principais: *startups fintechs;* desenvolvedores de tecnologia; governo; usuários financeiros; instituições financeiras tradicionais, conforme demonstrado (figura 3), a seguir:

Figura 3 – Ambiente das *Fintechs*: agentes participantes



Fonte: Adaptado de Leee e Shin, 2018.

Partindo dessa representação e para melhor delineamento da realidade do ambiente das *Fintechs* e seus agentes participantes, considera-se que:

- ✓ *Startups fintechs* que comportam os processos relacionados com os pagamentos e gestão dos valores, empréstimos, *crowdfunding*, mercado de capitais, além de *fintechs* de seguros;
- ✓ Desenvolvedores de tecnologia: Realizam a análise *big* data, computação em nuvem, moedas criptográficas, desenvolvedores de mídias sociais;
- ✓ Governo: Respondem pela regulamentação de ordem financeira e legislação;
- ✓ Usuários financeiros: Pessoas físicas e jurídicas (empresas);
- ✓ Instituições financeiras tradicionais: Bancos, financeiras e *venture*

capitalists, companhias de seguros, corretoras de ações (Araújo, 2018; Lee; Shin, 2018).

Tem se que uma empresa *Fintech* é especializada em oferecer serviços financeiros digitais que incluem mecanismos e serviços como provedores de pagamento digital e plataformas de empréstimos *peer-to-peer*, que favorecem e vão de encontro à realidade contemporânea em que o tempo é fator valioso (Pazarbasioglu *et al*., 2020).

Através das *fintechs*, os usuários podem se conectar em uma variedade de serviços móveis, tais como fazer pagamentos, transferir dinheiro, fazer solicitações de empréstimo, compra de seguros, gerenciamento de ativos e realização de investimentos (Ryu, 2018) entre outros.

Fintechs são recentes no Brasil, no entanto já ganharam espaço no mercado financeiro nacional com suas inovações, facilidades de consumo e baixo custo (Cordeiro, 2019; Nakashima, 2018) e em tal perspectiva, importa salientar que os bancos digitais que se enquadram na categoria das *fintechs* estão experimentando um crescimento significativo, evidenciando as transformações do mercado financeiro bancário em função dessa inovação em tecnologia (Vido, 2020).

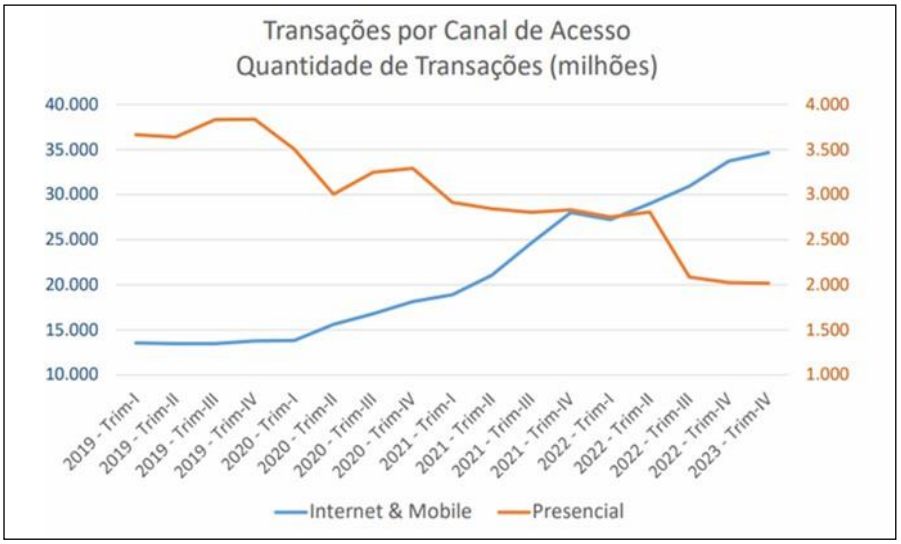
Pesquisa feita pelo banco digital N26 juntamente com a *Accenture*, o Brasil está posicionado entre os três países que registram maior número de clientes na adesão do modelo de bancos digitais e com participação ativa no crescimento da *fintechs* (CNN, 2020). Validando o uso de canais eletrônicos, as *fintechs,* conseguem inovar o relacionamento com clientes, viabilizando atendimento a uma demanda que invariavelmente não estava sedo atendida por bancos tradicionais. Assim, pode-se afirmar que as *fintechs* conseguem proporcionar:

> Inovações para pessoas e empresas. Isso se reflete em: melhores jornadas de utilização de produtos e serviços que trazem melhores experiências de uso; geração de inteligência a partir de volumes inimagináveis de dados e do conhecimento coletivo para otimizar as decisões; e integração dos diferentes elos do mercado de maneira muito mais eficiente, com menos falhas operacionais, aumentando a velocidade de transações e reduzindo custos (Fintech Lab, 2016, p. 3).

Estudo realizado pelo Banco Central do Brasil (2020) mostra que as *fintechs* estão revelando potencial crescimento no mercado bancário, disponibilizando produtos e serviços mais acessíveis, seguros e direcionados a atender às necessidades dos clientes sob diferentes aspectos.

Esta realidade permite constatar que a ascensão das *fintechs* tem impactado nos atendimentos presenciais e em influenciado a queda das transações nas agências bancárias físicas, como mostra a figura 2:

Figura 4: Aumento das transações bancárias via aplicativo



Fonte: Gomes, 2023.

Em vista deste panorama, o sistema bancário, atento à necessidade de atender aos novos comportamentos e hábitos dos usuários e clientes e relação às inovações digitais, vem investindo fortemente em tecnologias (Febraban, 2023)

Não é difícil encontrar comentários e conceituações que traçam entendimentos sobre as *fintechs*, acentuando a relação e as influências na economia e sistemas bancários. Segundo alguns posicionamentos: “As *fintechs* têm sido apresentadas pela grande mídia internacional como revolucionárias e uma ameaça à indústria bancária tradicional” (Rocha; Christopoulos, 2023, p.1) e esta concepção pode reforçar a ideia e tendência à diminuição do número de que agências físicas: “62% das pessoas têm preferência por um banco digital que pode ser uma *fintech* [...]” (CNN Brasil, 2023, n.p).

Consideradas as soluções e plataformas que estão relacionadas com as *fintechs,* a automatização das operações financeiras se consagra como uma das possibilidades convergentes em benefícios para os clientes. Além disso, citam-se as contas digitais, os pagamentos, serviços de transferência e a verificação de recebimentos que são serviços que especialmente atendem as demandas da

população em geral, favorecendo nas mais diferentes regiões do país, a acessibilidade para diversos públicos (BACEN, 2020).

A concepção sobre o uso das *Fintechs* tem demarcado benefícios e riscos que devem ser conhecidos e compreendidos, de forma que seja possível construir uma visão mais apurada em relação a estas empresas, no que tange a sua movimentação no mercado, adesão e realidades inerentes as fraudes (Quadro1).

Quadro1: Benefícios e riscos relacionados às *fintechs*

FINTECHS	
BENEFÍCIOS ECONÔMICOS	Redução de custos ou vantagens financeiras
	Facilidade de transação – velocidade e simplicidade
	Conveniência - uso dos serviços (qualquer lugar/hora)
RISCOS	Perda financeira por fraudes/ataques cibernéticos
	Perda financeira - problemas operacionais
	Perda financeira - problemas e processos internos (insolvência)
	Insegurança jurídica – falta de regulamentação

Fonte: Adaptado Ryu, 2018.

Independente dos riscos, os benefícios das *fintechs,* parecem ocupar um patamar mais elevado, fazendo com que os brasileiros sinalizem uma adesão cada vez maior, considerando a flexibilidade dos serviços digitais ofertados por essas empresas (CNN, 2023). Cabe lembrar, conforme esclarecem pesquisadores que atuam pela Serasa *Experian*:

> Por não existir uma bala de prata que blinde toda e qualquer transação, apenas a proteção em camadas é capaz de garantir a segurança de todos. Alguns exemplos são a biometria facial, a análise de risco de dispositivo, a verificação de documentos, o Cadastro *Know Your Costuer* (KYC), entre outros (Rocha, 2024, n.p).

Outros mecanismos que também vem sendo de grande valia, é o monitoramento contínuo e a autenticação multifator, sendo interessante consagrar que a utilização inteligente das tecnologias é indispensável para que a segurança e integridade das operações e ou transações sejam contempladas, prevenindo e evitando fraudes (Serasa *Experia*n, 2024).

3.1 Estratégias *Fintechs* – reforço à segurança

Na busca por mecanismos que tragam maior segurança para o usuário em relação à utilização dos serviços bancários digitais, têm sido criadas estratégias diferenciadas e novas formas de potencializar a proteção das informações dos usuários, fomentando o crescente uso das tecnologias *fintechs* (Trigo, 2024). Seguindo esta afirmativa, elencam-se algumas possibilidades aplicáveis em segurança para as *fintechs* (Quadro 2):

Quadro 2: Estratégias *Fintechs* contra fraudes

SEGURANÇA *FINTECHS*	
ESTRATÉGIAS	DESENVOLVIMENTO
Autenticação robusta	Empresas utilizam diversos métodos de autenticação para garantir que o usuário seja quem ele diz ser. Além do *login* e senha tradicionais, podem solicitar documentos, biometria facial e outras informações para validar a identidade do usuário.
Análise de comportamento	Plataformas monitoram constantemente o comportamento dos usuários para identificar atividades suspeitas. Alterações repentinas no padrão de consumo, acessos de diferentes dispositivos ou transações em locais incomuns podem gerar alertas e bloquear a conta, caso necessário.
Inteligência artificial	Inteligência artificial: a tecnologia é utilizada para analisar grandes volumes de dados e identificar padrões de fraude. Permite detectar novas ameaças e aprimorar os sistemas de segurança de forma contínua.
Equipe especializada	Equipe especializada: especialistas em segurança cibernética monitoram as ameaças 24 horas por dia, 7 dias por semana. A equipe é responsável por analisar alertas, investigar incidentes e tomar as medidas necessárias para proteger os dados dos usuários.
Atendimento personalizado	Atendimento personalizado: em caso de dúvidas ou problemas, os usuários contam com um atendimento personalizado e eficiente. Diversos canais de atendimento, como chat, telefone e e-mail auxiliam os clientes a resolverem qualquer tipo de problema.

Fonte: Adaptado Terra, 2024.

Em observância aos itens supracitados, as estratégias que vêm sendo adotadas para evitar possíveis fraudes bancárias contextualizam uma preocupação ativa com a proteção dos dados dos clientes e das transações financeiras realizadas no ambiente digital das *fintechs.* Segundo Diazero (2023), especialmente pelas particularidades inerentes a uma combinação de tecnologia e finanças, não se pode ignorar a indispensabilidade de passar para os clientes confiabilidade no mundo das

fintechs, sendo importante observar alguns pontos, como:

- ✓ Dados sensíveis: as *fintechs* estão diretamente atreladas com informações críticas de ordem pessoal e financeira (dados dos clientes, dados bancários, históricos de transações) que demandam proteção incisiva contra ciberataques, posto que alteradas ou expostas, podem trazer sérios danos ao indivíduo, afetando a segurança, privacidade e a integridade das operações;
- ✓ Identidade digital segura: essencial que as *fintechs* garantam a segurança das identidades digitais dos clientes, utilizando meios de proteção eficazes para evitar golpes e fraudes;
- ✓ Compartilhamento seguro de informações: as *fintechs,* devem considerar a necessidade de assegurar garantias de que o compartilhamento de dados é realizado de forma segura e eficiente, sendo fundamental, validar mecanismos de consentimento do cliente e o uso de tecnologias avançadas de criptografia que convertem informações sensíveis em códigos indecifráveis por qualquer pessoa ou sistema não autorizado;
- ✓ Segurança X *Malwares*: é quesito indispensável que as plataformas utilizadas pelas *fintechs* estejam protegidas contra *malware*s, confirmando a finalidade de evitar que a integridade dos dados e do sistema seja comprometida;
- ✓ Segurança contra vazamento de dados: no ambiente das *fintechs*, o uso do recurso da nuvem é fundamental para diminuir riscos de vazamento de dados, aumentando a segurança e a acessibilidade, contribuindo para a fidelização dos clientes e o crescimento aplicações (Diazero, 2023).

Estando as *fintechs* comprometidas com a segurança e proteção dos dados sensíveis, conseguem fomentar a confiança dos clientes, elevando as chances de alcançar com maior êxito, o crescimento sustentável do negócio (Diazero, 2023).

Considerando que tornar o ambiente das *fintechs* mais seguro é extremamente necessário, a valoração da segurança cibernética segue ganhando espaço neste cenário (Dieu, 2024), lembrando que o uso das tecnologias digitais é um chamariz para que as instituições bancárias se tornem alvos de cibercrimes, portanto: “A proteção dos dados dos clientes, dos ativos financeiros e da integridade das transações é essencial para manter a confiança e a credibilidade no setor de *fintech”* (Dieu, 2024, n.p).

Neste contexto, o combate às fraudes bancárias são desafios constantes e persistentes que invariavelmente sinalizam complexidades devido à crescente

sofisticação dos golpes e a rapidez que caracteriza a evolução tecnológica, acenando para a necessidade de haver uma ação coordenada e aprimorada das instituições financeiras com a implementação de estratégias que colaborem para garantir a confidencialidade e a proteção dos dados dos clientes (Santos, 2023). Para fins didáticos, vale ressaltar que:

> A confidencialidade está diretamente relacionada ao sigilo dos dados. O princípio básico é que as informações serão “tratadas” apenas pelas pessoas para as quais o acesso foi fornecido. Geralmente adotamos a “necessidade de conhecer” para definir quais informações podem ser acessadas por um colaborador. A confidencialidade pode ser comprometida quando fornecer intencionalmente ou não informações a uma pessoa que não deveria ter acesso, ou quando a informação é roubada durante um ataque (LNCC, 2024, n.p).

Sob esta ótica e especialmente pelos riscos evidentes de ações fraudulentas, compreende-se que a relação entre as estratégias de segurança e a legislação voltada para o setor bancário deve ser expressamente observada.

Através da legislação são determinados padrões mínimos de segurança que devem ser concebidos e adotados pelas instituições bancárias, incluindo as *fintechs,* protegendo os dados, prevenindo e evitando lavagem de dinheiro e outros crimes financeiros. Estar em conformidade com as leis vigentes, configura um dos caminhos mais seguros para um ambiente financeiro digital confiável (Rocha *et al*., 2024).

As normas para a proteção de dados é uma forma de também contemplar a proteção da própria pessoa humana (Santos 2021). Seguindo esta afirmativa, interessa o entendimento de que:

> Os dados pessoais têm como por definição representar algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa titular destes dados, podendo ser considerados uma extensão de sua personalidade, o que merece adequado tratamento (Santos, 2021, p.8).

A relevância das regulamentações e legislações direcionadas para o setor das *fintechs*, confirma normas e regras para combater ameaças digitais, crimes e fraudes bancárias. No ordenamento jurídico brasileiro, entre as legislações em destaque, encontram-se: a Resolução CMN 4.893/2021, Resolução CVM 35/2021, Resolução n° 119/2021, Resolução BCB n° 85 e a Resolução Conjunta n°6/2023, com ênfase para a Lei n°13.709/2018 (LGPD), assinalando que cada qual, traz especificações demarcadas por diretrizes, critérios e dispositivos que concorrem no

mesmo propósito de consolidar no complexo mundo das operações e transações bancárias, maior efetividade da segurança, privacidade e proteção dos dados.

A Resolução CMN 4.893/2021, trata dos quesitos para a contração de serviços de processamento, armazenamento de dados e de computação em nuvem estabelecendo as diretrizes referentes à implementação da política de cibersegurança nas instituições bancárias (BACEM, 2021).

Por sua vez, a Resolução CVM 35/2021 estabelece diretrizes que consagram a mediação de operações relacionadas com valores mobiliários em mercados regulamentados (DOU, 2021). Dentre outras determinações, o artigo 43 desta Resolução estabelece que as regras e procedimentos para o tratamento e controle de dados de clientes, devem validar: “I – a proteção das informações de cadastro e de operações realizadas pelo cliente, contra acesso ou destruição não autorizados, vazamento ou adulteração” (Resolução CVM, 2021, art.43).

A Resolução n° 119/2021 dispõe sobre as diretrizes referentes às políticas, procedimentos e controles internos que devem ser observados e seguidos pelas instituições que te o seu funcionamento autorizado pelo Banco Central do Brasil, sinalizando principalmente a finalidade de promover a prevenção do uso do sistema financeiro para a lavagem de dinheiro.

Quanto a Resolução BCB n° 85, as disposições previstas, referem-se:

> [...] a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024) (DOU, 2021, Seção 1, p. 66).

A Resolução Conjunta, n°6/2023, define critérios para o compartilhamento de dados e informações envolvendo suspeitas de fraudes que precisam ser observadas pelas instituições financeiras e instituições de pagamento, assim como outras que tenham autorização do Banco Central do Brasil, de modo a evitar ações fraudulentas, culminando no vazamento de dados sensíveis (Diazero, 2023).

Neste contexto, entre as citadas legislações, a Lei n°13.709/2018 (LGPD) é pontuada como sendo de extrema relevância quando se trata de prevenção às fraudes bancárias. É consagrada como a lei geral de proteção de dados vigente em nosso país, desde 18 de setembro de 2020.

4 LGPD NA PREVENÇÃO DAS FRAUDES

Considera-se como medida essencial que a política de tratamento dos dados pessoais esteja sob a devida proteção e regulamentação. No Brasil, a Lei n° 13.709/2018, Lei Geral de Proteção de Dados (LGPD), consagra o propósito central de proteger os direitos fundamentais de liberdade e privacidade no que tange ao tratamento de dados pessoais, seja em ambiente físico ou digital (Santos, 2021). Nestes termos, com o objetivo de proteger os dados pessoais, a LGPD:

> [...] dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018, p. 59).

A referida Lei foi sancionada em 14 de agosto de 2018, mas somente entrou em vigor e 18 de setembro de 2020. Este período de 24 meses ocorreu com base no entendimento da necessidade e importância de garantir a possibilidade de adaptação das organizações e empresas (Santos, 2022), lembrando que essa adequação envolveu dentre outros:

> [...] processos de captação das informações pessoais, ou melhor, a releitura da comunicação e da transparência com os indivíduos acerca das informações captadas e as razões para tal. Avaliação da natureza do tratamento, a finalidade e a utilização das informações em contexto e em concreto, conduzindo testes e proporcionalidade, adequação e necessidade (Araújo, 2019, p.23).

A LGPD colocou o Brasil em consonância com outras legislações internacionais como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Salienta-se que em sua essência, esta Lei, define o que são dados pessoais, estabelecendo cuidados fundamentais que devem ser usados para com o tratamento dos dados sensíveis. Em seu artigo 2°, esta Lei também, mostra-se fundamentada nos direitos humanos, na dignidade e no direito que cada pessoa deve ter de exercer a cidadania (Oliveira, 2021).

Visando proteger o cidadão de forma a mais completa possível, seja no âmbito de sua autonomia pública ou privada, a LGPD “[...] “busca estabelecer regras de coleta, uso, armazenamento e compartilhamento de dados de um cidadão por outra pessoa natural ou jurídica” (Oliveira, 2021, p.24).

A LGPD estabelece princípios e diretrizes para o tratamento adequado de dados pessoais, com especial atenção à segurança, à prevenção e à responsabilização dos agentes de tratamento. A principal contribuição da LGPD no combate às fraudes está na exigência de medidas técnicas e administrativas capazes de proteger os dados contra acessos não autorizados, destruição, perda, alteração e qualquer forma de tratamento inadequado ou ilícito (Silva; Oliveira, 2022)

Conforme previsto no artigo 6º da LGPD, a segurança deve ser entendida como um dever contínuo das organizações, o que implica na constante atualização de sistemas, treinamento de equipes e auditorias periódicas. A negligência na adoção dessas práticas pode acarretar sérias consequências, como multas administrativas, danos à reputação institucional e até ações judiciais por parte dos titulares dos dados (Damião; Novais, 2024).

A aplicabilidade da LGPD contempla os governos e as empresas, sempre com enfoque em garantir maior segurança aos dados pessoais, observando determinações e princípios legais conferidos pela legislação brasileira, acentuando atenta validação de regras que envolvem transparência, segurança, prevenção, responsabilização e a prestação de contas de tudo que se refere aos dados pessoais (Santos, 2021).

A LGPD pode ser tida como um relevante mecanismo legal que prima pelos direitos de proteção de dados dos indivíduos contribuindo para também protegê-los contra possíveis violações de suas informações, posto que: “os riscos que envolvem a violação à privacidade e à personalidade dos cidadãos na sociedade da informação crescem exponencialmente, como a possibilidade de uso indevido de dados pessoais” (Finkelstein, Finkelstein, 2019, p. 285).

Sob esta perspectiva, a realidade dos desafios que as instituições bancárias, têm vivenciado é intensa, na busca combater crimes que afetam a privacidade das informações dos clientes. Conforme Toledo (2021), que a relação entre a LGPD e a prevenção de fraudes deve ser cada vez mais consolidada para fins de prevenir e garantir maior proteção dos dados sensíveis.

A LGPD impõe às instituições financeiras a obrigação de adotar medidas técnicas e organizacionais robustas para garantir a segurança dos dados pessoais sob sua responsabilidade. Nesse sentido, falhas na implementação dessas medidas, que resultem em fraudes, ensejam a responsabilização da instituição por não ter assegurado o tratamento adequado das informações, conforme estabelecido na

legislação (Ribeiro; Fermentão, 2023). Recursos como a autenticação biométrica, protocolos de segurança avançados e o compartilhamento de dados sobre atividades suspeitas entre instituições tornam-se essenciais para evitar vazamentos e acessos indevidos.

Nesta linha de pensamento, de acordo com Damião e Novais (2024), a LGPD pode impactar de forma significativa na prevenção de fraudes, considerando os seguintes aspectos:

- ✓ Direito à segurança dos dados: A segurança é reconhecida como um dos pilares fundamentais da LGPD, exigindo das instituições financeiras o emprego de medidas técnicas e administrativas capazes de evitar acessos não autorizados e vazamentos de dados.
- ✓ Responsabilidade institucional: Quando uma fraude decorre de falhas na segurança da informação ou de procedimentos ineficazes, a instituição pode ser responsabilizada por descumprimento da lei, o que pode acarretar desde sanções administrativas até a obrigação de indenizar os titulares dos dados pelos danos causados.
- ✓ Prevenção de crimes: A utilização adequada de dados pessoais, inclusive sensíveis, como dados biométricos, pode contribuir significativamente para a identificação de padrões suspeitos e a autenticação de usuários, mecanismos fundamentais na detecção e prevenção de fraudes.
- ✓ Compartilhamento de informações: A legislação, em consonância com as normas do Banco Central, incentiva o intercâmbio de informações entre instituições financeiras sobre indícios de fraudes. Essa cooperação visa fortalecer os sistemas de controle e prevenção no âmbito do Sistema Financeiro Nacional (SFN).
- ✓ Eficiência aliada à segurança: A LGPD busca equilibrar a eficiência proporcionada pelos avanços tecnológicos com a proteção efetiva dos dados dos consumidores, assegurando que o desenvolvimento digital das operações bancárias ocorra sem comprometer a privacidade e a segurança das informações.

Preponderante salientar que a responsabilidade legal estabelecida pela LGPD desempenha papel relevante na prevenção de fraudes no ambiente digital. Em caso de incidentes envolvendo vazamento de dados que resultem em prejuízos aos consumidores, a organização pode ser obrigada a reparar os danos causados,

inclusive com indenizações por danos morais e materiais. De acordo com a legislação, em especial os artigos 42 a 45, os controladores e operadores de dados, podem ser responsabilizados civil, administrativa e até criminalmente quando houver falhas no tratamento dos dados que resultem em danos aos titulares, incluindo vazamentos de informações pessoais ou sua utilização para fins fraudulentos (Doneda, 2021).

Tal responsabilização não apenas visa à reparação, mas também atua como incentivo para que as empresas invistam em medidas robustas de segurança da informação, implementem políticas de governança de dados e adotem boas práticas para o tratamento adequado das informações pessoais (Monteiro, 2020).

A responsabilização prevista pela LGPD funciona como um mecanismo jurídico de dissuasão, forçando as organizações a tratarem os dados com zelo e a implementarem práticas de *compliance* digital, o que contribui diretamente para a redução dos riscos de fraudes, extorsões e outras condutas ilícitas relacionadas ao uso indevido de dados pessoais (Bioni, 2021).

Cabe ressaltar que a LGPD define dado pessoal como qualquer informação que possa identificar, direta ou indiretamente, uma pessoa natural (art. 5º, I), e estabelece regras claras para o tratamento dessas informações, fundamentadas nos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (art. 6º). Esses princípios visam garantir que os dados sejam tratados com respeito à privacidade, à liberdade e à dignidade do titular (Brasil, 2018).

A responsabilidade objetiva, prevista na LGPD, impõe que as empresas respondam independentemente da existência de culpa, bastando que se comprove o dano e o nexo com a falha no tratamento dos dados. Essa responsabilização tem como finalidade estimular uma cultura organizacional de prevenção e respeito à privacidade dos dados, essencial em um cenário crescente de crimes cibernéticos e uso indevido de informações sensíveis (Moraes, 2022).

Pode-se assim entender que a LGPD promove uma cultura de proteção de dados, tornando o tratamento responsável das informações pessoais um diferencial competitivo no mercado. Segundo Toledo (2021), à medida que os consumidores se tornam mais conscientes de seus direitos, cresce a exigência por parte deles em relação à transparência e à segurança das instituições que utilizam seus dados.

Embora a LGPD não elimine por completo a possibilidade de fraudes, ela estabelece um padrão rigoroso de segurança e responsabilidade para o tratamento de dados pessoais nas instituições financeiras. Ao impor diretrizes claras e mecanismos de responsabilização, a lei visa minimizar os riscos de acesso indevido e uso fraudulento de informações sensíveis, contribuindo para um ambiente financeiro mais seguro e transparente (Bioni, 2021).

Sob esta ótica, consagra-se que sob a perspectiva da relevância da LGPD, o tratamento adequado dos dados, aliado à responsabilidade legal pelo seu uso, transforma a privacidade em um ativo estratégico para o setor financeiro, ao mesmo tempo em que reforça a confiança dos consumidores e previne práticas fraudulentas (Monteiro; Oliveira, 2020).

4.1 Conceito privacidade LGPD

A privacidade é um direito fundamental assegurado pela Constituição Federal de 1988, em seu artigo 5º, incisos X, XI e XII, que tratam da inviolabilidade da intimidade, da vida privada, do domicílio e das comunicações (Brasil, 1988). Com o avanço das tecnologias da informação e a crescente digitalização das relações sociais, econômicas e jurídicas, compreende-se que seja necessário ampliar a compreensão desse direito, incluindo a proteção dos dados pessoais como dimensão essencial da privacidade.

Nesse cenário, a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, representa um marco regulatório que visa assegurar o direito à privacidade e à proteção dos dados pessoais dos indivíduos, conforme disposto em seu artigo 1º. A LGPD reconhece que o controle sobre os próprios dados é uma manifestação da autodeterminação informativa, ou seja, o direito do titular de decidir como, por quem e para que finalidade suas informações, serão tratadas (Doneda, 2021).

No contexto da LGPD, o conceito de privacidade é ampliado para além da esfera íntima, abarcando também a privacidade informacional e conforme Solove (2008) que consiste no controle que o indivíduo exerce sobre o fluxo de suas informações pessoais. Tal abordagem é compatível com o entendimento de que, em uma sociedade conectada, a exposição excessiva ou não autorizada de dados pode

comprometer a liberdade individual, a autodeterminação e até mesmo a igualdade de oportunidades.

A privacidade no contexto da LGPD, não se resume ao sigilo ou a não divulgação de informações, mas refere-se a um conjunto de prerrogativas que garantem ao titular a liberdade de construir sua identidade sem interferências indevidas por parte de instituições públicas ou privadas. Esse entendimento é alinhado às tendências internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, que influenciou diretamente a redação da LGPD (Bioni, 2021).

Com a promulgação da Emenda Constitucional nº 115/2022, a proteção de dados pessoais passou a ter status constitucional, sendo expressamente reconhecida como direito fundamental autônomo no artigo 5º, inciso LXXIX. Essa alteração reforça a centralidade da privacidade informacional no Estado Democrático de Direito e consolida a LGPD como uma das principais ferramentas normativas para sua efetivação (Mendes; Branco, 2023).

A LGPD transforma a privacidade em uma norma de conduta para agentes de tratamento, impondo deveres de cuidado, responsabilidade e prestação de contas no uso de dados pessoais. Esse novo paradigma jurídico exige das organizações uma mudança de cultura, pautada na transparência, ética digital e respeito aos direitos fundamentais, especialmente em setores que lidam com grandes volumes de dados, como o financeiro, o de saúde e o de tecnologia (Monteiro, 2020).

Assim, o conceito de privacidade na LGPD está intimamente ligado à proteção da liberdade individual em ambientes cada vez mais interconectados. A lei busca equilibrar os benefícios da inovação tecnológica com a necessidade de preservar a integridade, a autonomia e os direitos dos titulares de dados, promovendo um ambiente de maior confiança, responsabilidade e segurança jurídica (monteiro; Moraes, 2020).

A LGPD rompe com a lógica meramente patrimonialista dos dados, adotando abordagem centrada nos direitos fundamentais. O tratamento de dados pessoais não pode ocorrer de forma arbitrária, devendo respeitar princípios como a finalidade, a necessidade, a transparência e a segurança (art. 6º da LGPD). A privacidade, portanto, é concebida como um direito multifacetado, que se projeta sobre os processos de coleta, armazenamento, uso e compartilhamento de dados, impondo limites jurídicos à atuação de empresas e do Estado (Doneda, 2021).

5 JURISPRUDÊNCIA: FRAUDES BANCÁRIAS X DESOBEDIÊNCIA A LGPD

A vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) introduziu um novo regime jurídico de responsabilização para agentes que tratam dados pessoais, especialmente no setor bancário, onde o volume e a sensibilidade das informações são significativos. A violação dos princípios da LGPD como a segurança, a finalidade e a necessidade, pode ensejar não apenas sanções administrativas, mas também responsabilidade civil por danos causados a titulares de dados, inclusive nos casos de fraudes bancárias decorrentes de vazamentos de dados (Bioni, 2021).

A jurisprudência brasileira tem se consolidado no sentido de responsabilizar instituições financeiras por fraudes ocorridas após vazamentos de dados pessoais, ainda que não esteja comprovada sua culpa direta, com base na teoria do risco da atividade e na responsabilidade objetiva prevista no Código de Defesa do Consumidor (CDC). A LGPD e o CDC se complementam na proteção do consumidor, exigindo das instituições padrões elevados de cuidado e segurança no tratamento de dados (Tartuce, 2023).

A jurisprudência dos tribunais superiores e estaduais tem reconhecido que a falha na proteção de dados pessoais, ainda que sem prova de vazamento intencional ou dolo, pode caracterizar violação aos deveres legais e ensejar indenização por danos materiais e morais. Uma das decisões paradigmáticas nesse sentido foi proferida pelo Tribunal de Justiça de São Paulo (TJSP):

> É objetiva a responsabilidade da instituição financeira por falhas no sistema de segurança que permitem a ocorrência de fraudes bancárias, especialmente quando evidenciado que os dados do autor foram utilizados indevidamente. A LGPD impõe padrões mínimos de segurança que não foram observados (TJSP – Apelação Cível nº 100XXXX-56.2022.8.26.0100, j. 27/06/2023).

Neste julgado, o tribunal reconheceu a correlação entre a ineficiência dos mecanismos de segurança e a falha na prestação do serviço bancário, mesmo diante da alegação da instituição de que a fraude foi causada por terceiros. A responsabilização foi fundamentada tanto no artigo 14 do CDC quanto nos princípios da LGPD, como segurança, prevenção e responsabilização e prestação de contas (art. 6º, incisos VII, VIII e X) (Brasil, 2018).

Outro exemplo relevante está na jurisprudência do Superior Tribunal de Justiça (STJ) que, embora ainda esteja consolidando entendimentos específicos com base na LGPD, já reconheceu que a instituição financeira responde objetivamente por falhas na segurança de seus sistemas, especialmente quando tais falhas resultam em prejuízos aos clientes, conforme jurisprudência consolidada no tema da responsabilidade bancária por fraudes eletrônicas (Brasil, 2023).

Neste segmento, em decisão emblemática o Tribunal de Justiça de São Paulo (TJSP), responsabilizou um banco por fraude bancária ocorrida após vazamento de dados pessoais, com base na ausência de segurança adequada para proteger as informações do titular. Foi considerado que o banco, réu, não adotava medidas de proteção dos dados, colaborando para com o comprometimento da segurança e, portanto, não observou as determinações da LGPD. Essa postura permitiu que houvesse falhas na prestação dos serviços (TJSP, 2022).

Essa decisão está em consonância com o artigo 42 da LGPD, que prevê a responsabilidade do controlador ou operador que, em razão de tratamento inadequado de dados, cause danos patrimoniais, morais, individuais ou coletivos.

A LGPD exige dos agentes de tratamento uma postura proativa de governança de dados, o que implica adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação. A ausência dessas medidas pode ser interpretada como negligência, ainda que o banco alegue ser vítima de terceiros (Bioni, 2021).

A privacidade e a proteção de dados são direitos fundamentais que integram a autodeterminação informativa do indivíduo. Assim, qualquer violação decorrente de omissão ou falha de controle tecnológico impõe a responsabilização do agente de tratamento, mesmo na ausência de dolo (Doneda, 2021).

Em outra decisão recente, o Tribunal Regional Federal da 3ª Região (TRF-3) reforçou esse entendimento ao julgar procedente pedido de indenização contra instituição bancária por fraude eletrônica resultante de suposto vazamento de dados: “Cabe à instituição financeira adotar todos os meios disponíveis de proteção de dados dos clientes, conforme os princípios da LGPD. A ocorrência de fraude, por si só, revela falha na segurança” (TRF-3, Apelação Cível nº 500XXXX-39.2021.4.03.6100).

A jurisprudência nacional tem se consolidado no sentido de reconhecer a responsabilidade das instituições financeiras em casos de fraudes bancárias facilitadas pelo uso indevido de dados pessoais, sobretudo quando há descumprimento dos deveres previstos na Lei Geral de Proteção de Dados Pessoais LGPD – Lei nº 13.709/2018 (Bioni, 2021).

Um dos precedentes mais emblemáticos é o REsp 2.077.278/SP, julgado pela Terceira Turma do Superior Tribunal de Justiça (STJ), sob relatoria da Ministra Nancy Andrighi. O cliente solicitou, via e-mail, informações para quitar um financiamento e posteriormente, recebeu um boleto falso com aparência legítima, que continha, dados corretos do contrato. Após o pagamento, constatou-se que o valor fora destinado a fraudadores. O STJ entendeu que houve falha no dever de segurança por parte da instituição financeira, que permitiu o vazamento ou a exposição indevida de dados pessoais e contratuais do cliente. Assim, reconheceu-se a responsabilidade objetiva do banco, com fundamento nos artigos 42, 44 e 46 da LGPD (Brasil, 2018).

Em decisão semelhante, o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) também responsabilizou, uma instituição financeira por fraude bancária praticada mediante o golpe do boleto. O caso envolveu a emissão de um boleto falso por terceiros, com uso de dados contratuais legítimos da cliente, obtidos indevidamente. A corte entendeu que houve violação dos princípios da segurança, prevenção e responsabilização (art. 6º, incisos VII, VIII e X, da LGPD), além de falha na prestação do serviço bancário. A sentença determinou a restituição dos valores pagos, além de indenização por danos morais (TJDFT, 2023).

Outro caso relevante envolveu a prática de empréstimo consignado fraudulento, julgado por Vara Cível no Distrito Federal. A autora da ação teve seu nome e dados pessoais utilizados indevidamente para a contratação de um empréstimo junto a uma instituição financeira. O banco, ao ser demandado, não conseguiu comprovar a adoção de mecanismos eficazes de proteção de dados nem medidas de verificação de identidade. O juiz concluiu pela violação do dever de segurança previsto na LGPD, determinando a extinção da dívida e a devolução dos valores indevidamente descontados do benefício da autora (Conjur, 2025).

Essas decisões revelam uma tendência clara dos tribunais brasileiros no sentido de exigir das instituições financeiras um padrão elevado de diligência no tratamento de dados pessoais. O descumprimento das obrigações legais

estabelecidas pela LGPD, especialmente quanto à segurança da informação, tem sido interpretado como fator determinante para a ocorrência de fraudes bancárias, ensejando reparação integral dos danos patrimoniais e extrapatrimoniais sofridos pelos titulares de dados (Doneda, 2021).

Observável que a jurisprudência tem sinalizado a desobediência à LGPD, ainda que indireta, como um fator de responsabilização civil, principalmente em fraudes que envolvam o uso indevido de dados pessoais. A responsabilização não está condicionada à comprovação de que o banco realizou diretamente o vazamento, mas sim à demonstração de que houve falha na adoção de medidas preventivas, conforme os princípios de *accountability e privacy by design* (Brasil, 2018; Doneda, 2021).

Dessa forma, a LGPD introduziu um novo paradigma de proteção jurídica, elevando o padrão de diligência exigido das instituições financeiras e permitindo aos titulares de dados, a busca por reparação em casos de fraudes bancárias originadas de falhas de segurança e governança informacional.

6 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste trabalho permitiu constatar que as fraudes bancárias, representam um dos maiores desafios enfrentados pelas instituições financeiras e pela sociedade contemporânea, especialmente em um cenário marcado pela digitalização dos serviços e pelo uso massivo de dados pessoais. A expansão das operações eletrônicas trouxe agilidade e comodidade, mas também ampliou as vulnerabilidades relacionadas à segurança da informação, tornando indispensável a adoção de mecanismos de proteção mais robustos e transparentes.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) assume papel essencial na prevenção e mitigação das fraudes bancárias. Ao estabelecer princípios e obrigações específicas sobre o tratamento e a segurança de dados, a LGPD reforça a responsabilidade das instituições financeiras quanto à guarda, uso e compartilhamento das informações de seus clientes. A norma, além de promover a proteção da privacidade, também fortalece a confiança nas relações de consumo e fomenta uma cultura de responsabilidade digital, indispensável para o funcionamento ético e seguro do sistema financeiro.

Verificou-se ainda que a aplicação efetiva da LGPD contribui não apenas para a responsabilização das instituições que negligenciam a segurança das informações, mas também para a prevenção de condutas ilícitas, uma vez que exige a implementação de medidas técnicas e administrativas adequadas. Dessa forma, a legislação atua de forma preventiva e educativa, incentivando a conformidade e a adoção de boas práticas de governança de dados.

Conclui-se que a importância da LGPD transcende o aspecto jurídico, alcançando dimensões sociais, econômicas e éticas. A sua observância é indispensável para o fortalecimento da segurança digital, para a redução dos índices de fraudes e para a consolidação de um ambiente financeiro mais confiável e sustentável. Assim, a efetiva integração entre a proteção de dados pessoais e as políticas de segurança bancária, constitui não apenas uma exigência legal, mas um compromisso essencial com a integridade, a transparência e a confiança nas relações que envolvem o tratamento de informações no sistema financeiro.

REFERÊNCIAS

ARAÚJO, Marcos Venicius Mourão de. **Investimento em tecnologia nas instituições financeiras e a influência das fintechs**. Dissertação [Mestrado em Economia]. 83f. São Paulo: Fundação Getúlio Vargas – FGV, 2018.

BACIGALUPO, H. **Direito penal**: parte geral. São Paulo: Malheiros, 2005.

BIONI, B. R. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Comissão de Valores Mobiliários. **Resolução CVM Nº 35, de 26 de maio de 2021**. Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários.Brasília,DF, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**.Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 maio 2025.

BRASIL. Banco Central do Brasil. **Resolução nº 4.658, de 26 de abril de 2018**. Dispõe sobre a política de segurança cibernética, sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e sobre a política de segurança cibernética para as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Diário Oficial da União, Brasília, DF, seção 82, 2018.

BRASIL. **Lei n°4.595, de 31 de dezembro de 1964**. Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, cria o Conselho Monetário Nacional e dá outras providências. Brasília, DF,1964.

BRASIL. Código Penal. **Decreto – Lei n° 2.848, De 7 de dezembro de 1940**. Brasília, DF, 1940.

CABLE NEWS NETWORK. **Fintechs**: entenda o que são, onde atuam e os impactos no mercado. CNN Brasil. 2023. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/fintechs-o-que-sao-e-onde-atuam/. Acesso em: 2 maio 2025.

CAMPÊLO, M. A. Engenharia Social: como aspectos psicológicos podem se relacionar com golpes e fraudes. **Portal do Investidor**.2024. https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1

CONJUR. **Banco é responsável por vazamento de dados que levaram a falso consignado**. 2025. Disponível em: [https://www.conjur.com.br/2025-jan-25/banco-e-responsavel-por-vazamento-de-dados-que-levaram-a-falso-

consignado/](https://www.conjur.com.br/2025-jan-25/banco-e-responsavel-por-vazamento-de-dados-que-levaram-a-falso-consignado/). Acesso em: 13 set. 2025.

CERNEV, A. K.; DINIZ, E. H. **Fintech**: a sexta onda de inovações no sistema financeiro. In CERNEV, A. K.; DINIZ, E. H. Inovação em serviços na economia do compartilhamento. São Paulo: Saraiva, 2019.

COELHO, F. U. **Curso de Direito Comercial**: direito de empresa. 17ª ed., rev. atual. e ampl.. São Paulo: Saraiva, 2016.

COSTA, M. J. A. **Direito das obrigações**. 12ª ed**.** rev. e atual. Coimbra: Almedina, 2013.

CORDEIRO, J. P. DE V. **Fintechs e inclusão financeira no Brasil**: uma abordagem Delphi. 2019. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/28667. Acesso em: 2 jun. 2025.

DAMIÃO, A. S.; NOVAIS, T. G. consequências jurídicas da LGPD para os crimes virtuais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**; v. 10, n. 11, nov. 2024.

DIAZERO, Security. Fintechs e segurança de dados: importância, desafios e estratégias. 2023. Disponível em: https://www.diazerosecurity.com.br/pt/blog/fintechs-e-seguranca-de-dados-importancia-desafios-e-estrategias. Acesso em: 22 jul. 2025.

DIEU, Linh Chu. **Os mares cibernéticos das fintechs: desafios e soluções para uma navegação segura**. SmartDev. 2024. Disponível em: https://smartdev.com/thefintech-cyber-seas-challenges-and-solutions-for-secure%20navigation/. Acesso em: 16 set. 2025.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. 3º ed. Ribeirão Preto: RT, 2021.

ESCOLA VIRTUAL DO GOVERNO – EVG. Inteligência artificial generativa**. Portal do Governo. 2024**. Disponível em: https://www.escolavirtual.gov.br/curso/1091. Acesso em: 22 mar. 2025.

FINKELSTEIN, M. E.; FINKELSTEIN, C. Privacidade e Lei Geral De Proteção de Dados Pessoais. **Revista de Direito Brasileira**; v. 23, n. 9, p. 284-301, 2019.

GONÇALVES, L. M. A. **Responsabilidade civil em casos de fraudes digitais no setor bancário**. 2021. 34f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Curitiba. Curitiba, PR, 2021.

JANERI FILHO, O. **Fraude em Contratos com Assinatura Eletrônica Tipos de Assinatura, Aspectos Legais e Jurídicos, Principais Tipos de Fraudes e Relatos de Casos Reais**. Jusbrasil. 2023. Disponível em: https://www.jusbrasil.com.br/artigos/fraude-em-contratos-com-assinatura-eletronica/1764921870. Acesso em: 13 mar. 2025.

LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA – LNCC**. Os quatro pilares da segurança da informação: Confidencialidade, Disponibilidade, Integridade e Autenticidade**. Ministério da Ciência, Tecnologia e Inovações. 2024. Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/os-quatro-pilares-da-seguranca-da-informacao-2013-confidencialidade-disponibilidade-integridade-e-autenticidade. Acesso em: 22 jul.2025.

LEE, In; SHIN, Yong Jae. Fintech: ecosystem, business models, investment decisions, and challenges. **Business Horizons**; v. 61, n. 1, p. 35-46, 2018. Disponível em: https://www.researchgate.net/publication/320365249_Fintech_Ecosystem_business_models_investment_decisions_and_challenges. Acesso em: 2 jun. 2025.

LIMA, M. R. **A evolução e a democratização do sistema de pagamento no Brasil**. 38f. 2023. Monografia (Ciências Econômicas) - Pontifica Universidade Católica de Goiás. Goiânia, GO, 2023.

MARTIS, P. H. M.; KIM, H. S. P.; STAVROPOULOS, R.M. **Novo olhar do judiciário para as fraudes financeiras**. Consultor Jurídico. 2023. Disponível em: https://www.conjur.com.br/2023-dez-12/novo-olhar-do-judiciario-para-as-fraudes-financeiras/. Acesso em: 2 maio 2025.

MATHEUS, L. H.; NOCETTI, R. de C. P. A segurança jurídica dos contratos onlines de consumo das instituições financeiras.**Revista ft**; 2023. https://revistaft.com.br/a-seguranca-juridica-dos-contratos-onlines-de-consumo-das-instituicoes-financeiras/

MENDES, G. F.; BRANCO, P. G. G. **Curso de direito constitucional**. 18. ed. São Paulo: Saraiva, 2023.

MONTEIRO, A. de O. **A responsabilidade civil das instituições financeiras em casos de golpes contra correntistas**. 2022. 51f. Monografia (Direito) - Universidade Federal do Rio de Janeiro. Rio de Janeiro, RJ, 2022.

MOREIRA, J. E. **Fatores que influenciam no uso de bancos digitais**: uma revisão da literatura de 2013 a 2023. 30 f. 2023. Trabalho de Conclusão de Curso (Administração) - Universidade Federal de Ouro Preto – UFOP. Mariana, MG, 2023.

MOURA, J.S.M. *et al.* Análise das demonstrações contábeis dos bancos digitais. **Revista Conhecimento Contabil**; v. 13, n. 1, 2023.

OLIVEIRA, B. H. D. **Lei geral de proteção de dados adaptação das empresas para proteção e privacidade dos dados de seus clientes, fornecedores, colaboradores e outros**. 2021. 29f. Monografia Jurídica (Direito) - Pontifícia Universidade Católica de Goiás. Goiânia, GO, 2021.

PAZARBASIOGLU, C., A. *et al*. **Digital Financial Services**. 2020. Disponível em: https://thedocs.worldbank.org/en/doc/305a39cbb6f35567db78bda6709c5cd8-0430012025/original/World-Bank-DFS-Whitepaper-DigitalFinancialServices.pdf. Acesso em: 5 set. 2025.

PEREIRA, C. F. de A.; SILVA, R. da. As fraudes bancárias e a responsabilidade civil das instituições financeiras. **Revista JurisFIB**; v. XI, ano XI, 2020.

RIBEIRO, M. M.; FERMENTÃO, C. A. G. R. Proteção de dados pessoais na era do capitalismo de vigilância em defesa dos direitos personalíssimos da pessoa : uma possibilidade ou mero devaneio?. **Virtuajus**, Belo Horizonte, v. 8, n. 15, p. 245–252, 2023.

ROCHA, C. **Prevenção à fraudes**.Serasa Experian.2024. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/relatorio-de-fraude-da-serasa-experian-4-em-cada-10-brasileiros-ja-foram-vitimas-de-golpes-e-preocupacao-de-empresas-aumentou-58-em-um-ano/. Acesso em: 2 maio 2025.

ROCHA, J.; Christopoulos, T. P. A visão da grande mídia sobre a revolução Fintech. **Rev. Bras. Ciênc. Comun**.; v. 46, e2023203, 2023. Disponível em: https://www.scielo.br/j/interc/a/X95Rw5NMfd7CbZRgXN8bqJG/?format=pdf&lang=pt. Acesso em: 23 abr. 2025.

RYU, H. S. What makes users willing or hesitant to use Fintech?: the moderating effect of user type. **Industrial Management & Data Systems**; v.118, n. 3, p. 541-569, 2018. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/imds-07-2017-0325/full/html. Acesso em: 3 abr. 2025.

SAKAMOTO, D. **8 milhões de consumidores sofreram golpes finaceiros nos últimos 12 meses**: aponta CNDL/SPC Brasil. Políticas Públicas 4.0 Institucional CNDL. 2025. Disponível em: https://cndl.org.br/politicaspublicas/8-milhoes-de-consumidores-sofreram-golpes-financeiros-nos-ultimos-12-meses-aponta-cndl-spc-brasil/. Acesso em: 10 mar. 2023.

SANTOS, K. O. D. dos. **As fraudes bancárias e a responsabilidade civil das instituições financeiras**. 2023. 61f. Monografia (Bacharel em Direito) - Pontifícia Universidade Católica de São Paulo. São Paulo, SP, 2023.

SANTOS, L. S. **A lei 13.709/18**: Lei geral de proteção de dados o direito à privacidade e os princípios que asseguram a proteção de dados. 2021. 36f. Trabalho de Curso (Direito) - Pontifícia Universidade Católica de Goiás. Goiânia, GO. 2021.

SERASA EXPERIAN. **Maiores tendências em fraudes e crimes financeiros em 2025**. 2025. Disponível em: https://www.serasaexperian.com.br/conteudos/prevencao-a-fraude/as-5-maiores-tendencias-em-fraudes-e-crimes-financeiros-da-atualidade/. Acesso em: 2 maio 2025.

SERASA EXPERIAN. **Relatório de fraude da Serasa experian**: e em cada 10 brasileiro já foram vítimas de golpes e preocupação de empresas aumentou 58%.2024. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/relatorio-de-fraude-da-serasa-experian-4-em-cada-10-brasileiros-ja-foram-vitimas-de-golpes-e-preocupacao-de-empresas-aumentou-58-em-um-ano/. Acesso em: 13 abr. 2025.

SILVA, N. L. da.; UEHARA, M. A evolução da tecnologia digital: seus impactos no setor bancário. Goiânia: **Enciclopédia Biosfera/Centro Científico Conhecer**;v.16, n.29, p.2241, 2019.
Disponível em: https://www.conhecer.org.br/enciclop/2019a/apli/a%20evolucao.pdf. Acesso em 15 mar. 2025.

SOLOVE, D. J. **Compreendendo a Privacidade**. Cambridge, Massachusetts: Harvard University Press. 2008.

TARTUCE, F. **Manual de Direito Civil**. 13ª ed. Rio de Janeiro: Método. 2023.

TARTUCE, F. **Responsabilidade Civil**. 3. ed. Rio de Janeiro: Forense, 2013.

TOLEDO, M. **Manual da LGPD Descomplicado**: Guia Completo. Belo Horizonte, MG: Empreendedorismo Legal, 2021.

TRIGO, B. **Por que *fintechs* são tão seguras quanto bancos tradicionais**.Terra. 2024. Disponível em:https://www.terra.com.br/economia/por-que-fintechs-sao-tao-seguras-quanto-bancos-tradicionais,27436cff5fa40893cf2585e054df3ed499gj8vpu.html. Acesso em: 13 abr. 2025.

VELOSO, L. F. F. O limite da responsabilidade dos bancos nas fraudes de terceiros contra os consumidores. **Revista do Curso de Direito da Unimontes**; v. 1, n. 1, 2024. Disponível em: file:///C:/Users/PC/Downloads/11.+Artigos+cient%C3%ADficos+8.+Revista+de+Direito+da+Unimontes.+v.+1.+n.+1.+2024.pdf. Acesso em: 13 abr. 2025.

VIDO, N.; GUTIERREZ, V. **Crescimento das fintechs Nubank, Guia bolso e Creditas no Brasil e as ameaças ao sistema bancário tradicional**. 2020. Disponível em: http://ric.cps.sp.gov.br/handle/123456789/7071. Acesso em: 13 jun. 2025.

WELLS, J. T. **Corporate fraud handbook**: prevention and detection. 5. ed. Wiley, 2017.

WELLS, J. T. **Principles of Fraud Examination**. 4. ed. United States of America: John Wiley & Sons, 2014.