CURSO DE DIREITO

SAMARA BARBOSA SILVA

A LEI GERAL DE PROTEÇÃO DE DADOS E O SISTEMA BANCÁRIO

Cuiabá/MT

2025

CURSO DE DIREITO

SAMARA BARBOSA SILVA

A LEI GERAL DE PROTEÇÃO DE DADOS E O SISTEMA BANCÁRIO

Monografia apresentado à Banca Avaliadora do Departamento de Direito, da Faculdade FASIPE-Cuiabá, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador(a): Me. Bruno Felipe Monteiro Coelho

Cuiabá/MT

2025

SAMARA BARBOSA SILVA

A LEI GERAL DE PROTEÇÃO DE DADOS E O SISTEMA BANCÁRIO

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito – da Faculdade Fasipe Cuiabá como requisito para a obtenção do título de Bacharel em Direito.

Aprovado em ___/___/____

_____

Professor Orientador: Me. Bruno Felipe Monteiro Coelho

Departamento de Direito– FASIPE

_____

Professor(a) Avaliador(a):

Departamento de Direito – FASIPE

_____

Coordenador do Curso de Direito

Cuiabá/MT

2025

DEDICATÓRIA

A todos meus amigos e familiares e as pessoas que em minha caminhada demonstraram paciência e carinho.

Em especial, àquelas que me incentivaram a seguir sempre em frente.

SILVA, Samara Barbosa. **A Lei Geral de Proteção de Dados e o Sistema Bancário**. 2025. 44 fls. Trabalho de Conclusão de Curso – Faculdade Fasipe Cuiabá.

RESUMO

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece diretrizes para o tratamento de dados pessoais no Brasil, com o objetivo de resguardar a privacidade, a liberdade e os direitos fundamentais dos cidadãos. No sistema bancário, a LGPD tem papel central, considerando o volume expressivo de informações sensíveis que as instituições financeiras coletam, processam e armazenam diariamente. O objetivo da pesquisa foi investigar como a LGPD tem influenciado os processos de gestão de dados nas instituições bancárias, com foco na proteção da privacidade dos clientes. A pesquisa utiliza abordagem descritiva e qualitativa, baseada em revisão de literatura e análise de normas jurídicas. Com a vigência da LGPD, é obrigatório que as instituições bancárias adotem medidas técnicas e administrativas para garantir a segurança dos dados e prevenir acessos não autorizados, vazamentos ou usos indevidos. A responsabilização em casos de violação pode envolver sanções administrativas, inclusive multas. Dessa forma, a LGPD é um marco de mudança cultural e operacional no setor bancário. Mais do que uma obrigação legal, ela exige novo olhar sobre o valor dos dados pessoais, promove a atuação ética, segura e responsável das instituições financeiras frente aos avanços da tecnologia e às exigências da sociedade contemporânea.

Palavras-chave: Lei Geral de Proteção de Dados; Autoridade Nacional de proteção de Dados; Banco Central do Brasil

SILVA, Samara Barbosa. **The General Data Protection Law and the Banking System**. 2025. 44 fls. Completion of course work – Faculdade Fasipe Cuiabá.

ABSTRACT

Law No. 13,709/2018, known as the General Personal Data Protection Law (LGPD), establishes guidelines for the processing of personal data in Brazil, with the aim of protecting the privacy, freedom and fundamental rights of citizens. In the banking system, the LGPD plays a central role, considering the significant volume of sensitive information that financial institutions collect, process and store daily. The objective of the research was to investigate how the LGPD has influenced data management processes in banking institutions, with a focus on protecting customer privacy. The research uses a descriptive and qualitative approach, based on a literature review and analysis of legal standards. With the LGPD in force, banking institutions are required to adopt technical and administrative measures to ensure data security and prevent unauthorized access, leaks or misuse. Liability in cases of violation may involve administrative sanctions, including fines. Thus, the LGPD is a milestone of cultural and operational change in the banking sector. More than a legal obligation, it requires a new look at the value of personal data, promotes ethical, safe and responsible actions by financial institutions in the face of technological advances and the demands of contemporary society.

Keywords: General Data Protection Law; National Data Protection Authority; Central Bank of Brazil

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
BCB	Banco Central do Brasil
DPO	Encarregado de Proteção de Dados
FEBRABAN	Federação Brasileira de Bancos
LGPD	Lei Geral de Proteção de Dados
OCDE	Organização para Cooperação e Desenvolvimento Socioeconômicos

SUMÁRIO

1 INTRODUÇÃO

Com a expansão das tecnologias digitais e a crescente presença da internet no cotidiano, praticamente todas as nossas ações, desde uma simples compra online até uma transferência bancária deixam rastros. Nesse cenário, cresceu a preocupação com a forma como essas informações são coletadas, armazenadas e utilizadas pelas empresas, sobretudo por aquelas que lidam com dados altamente sensíveis, como os bancos.

O sistema bancário brasileiro é um dos mais desenvolvidos do mundo em termos tecnológicos. As instituições financeiras investem em inovação, oferecem serviços digitais que facilitam a vida dos clientes, como aplicativos, *internet banking* e pagamentos por aproximação. Assim, toda essa praticidade exige um volume enorme de dados sendo processados em tempo real, o que levanta uma questão essencial: como garantir que essas informações sejam tratadas com responsabilidade e segurança?

Foi para responder a essa preocupação que surgiu a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018 e em vigor desde 2020. Inspirada em legislações internacionais, como o GDPR da União Europeia, a LGPD estabelece regras sobre o uso dos dados pessoais no Brasil. Ela determina que os dados só podem ser utilizados com consentimento do titular ou por alguma base legal específica, além de exigir transparência e medidas de proteção por parte das empresas.

No contexto bancário, a LGPD trouxe uma série de desafios e adaptações, os bancos passaram a ter que revisar seus processos internos, repensar suas estratégias de marketing e fortalecer ainda mais a segurança digital. Mais do que seguir uma lei, foi preciso mudar a cultura organizacional, reconhecendo que os dados dos clientes não são apenas informações técnicas, mas parte da identidade e da vida de cada pessoa. Esse movimento abriu espaço para um relacionamento ético e transparente com os consumidores.

Essa nova realidade gera debates importantes: os bancos estão preparados para lidar com a responsabilidade de proteger tantos dados? Os clientes compreendem seus direitos nesse processo? A LGPD não veio somente como um conjunto de regras, mas como um convite para

refletir sobre a forma como é tratada a privacidade em um mundo conectado. Compreender como a legislação tem sido aplicada no setor bancário é essencial para avaliar seus efeitos e caminhos possíveis.

O objetivo geral da pesquisa foi investigar como a LGPD tem influenciado os processos de gestão de dados nas instituições bancárias, com foco na proteção da privacidade dos clientes. Os objetivos específicos foram:

Para chegar ao objetivo, utilizar-se-á uma pesquisa de caráter descritivo, qualitativo, onde serão empregados a revisão de obras literárias físicas e eletrônicas juntamente com os artigos científicos e normas jurídicas, que serão utilizados como embasamento desse trabalho.

Este trabalho está estruturado em capítulos, sendo que no primeiro capítulo foi abordado seu funcionamento, fundamentos e contexto histórico, incluindo escândalos internacionais que impulsionaram a criação. Sendo explorado o percurso da legislação no Brasil até a sanção definitiva, além dos princípios fundamentais da LGPD, como boa-fé, liberdade, privacidade e o livre desenvolvimento da personalidade. Apresentados os direitos dos titulares de dados, a responsabilidade de controladores e operadores, as sanções para o descumprimento das normas e o impacto da LGPD nos negócios, sobretudo no meio digital, onde empresas utilizam dados pessoais para estabelecer padrões de consumo.

No segundo capítulo foi abordado o tratamento de dados pelas instituições financeiras e a Lei Geral de Proteção de Dados, tratando a segurança das informações pessoais, a obrigação de seguir essa lei para não haver nenhuma irregularidade, pois se caso houver descumprimento na lei, pode haver sanções administrativas. Assim, foi apresentado as boas práticas sobre como tratar as informações pessoais, transparência e consentimento. Sendo elencado o consentimento do titular de dados, a segurança de dados, a proteção das informações e o impacto das sanções sobre como essas sanções impactam as empresas públicas e privadas.

No terceiro capítulo, versa sobre o *open finance* e a LGPD, seu surgimento e sua evolução, os impactos, os direitos dos titulares de dados, qual a proteção que os titulares de dados têm com as relações as instituições financeiras. Também se apresentou os desafios e oportunidades, as dificuldades, as possibilidades que esses elementos trouxeram ao mercado financeiro e os casos de sucesso onde foi abordado a causa para o sucesso.

2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO ORDENAMENTO JURÍDICO BRASILEIRO

As discussões que ocorreram após a sanção da LGPD trouxeram algumas dúvidas com relação a sua efetividade. E conforme Palhares (2020, p. 529), os questionamentos ocorreram por dois motivos principais: o fato de a obrigatoriedade do consentimento expresso como base única para o tratamento de dados pessoais, positivada pelo Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), não ter sido fiscalizada com afinco; e os impactos gerados nos negócios pelas mudanças demandadas pela adequação à nova lei.

A LGPD representou um marco importante para a proteção de dados no Brasil, mas sua efetividade gerou debates pelos desafios na fiscalização e adequação empresarial. A exigência do consentimento expresso, destacada pelo Marco Civil da Internet, deveria ter sido um dos pilares para garantir transparência e controle dos titulares sobre seus dados, mas a falta de uma fiscalização gerou dúvidas sobre sua real aplicação.

A adequação das empresas à LGPD exigiu profundas mudanças operacionais e estratégicas, impactando desde a coleta e armazenamento de dados até as práticas de segurança e conformidade. Esse movimento não ocorreu isoladamente no Brasil, mas reflete um cenário global em que diversas nações estão buscando regulamentos robustos para garantir que os dados pessoais sejam tratados de maneira ética e segura.

2.1 Aspectos históricos e conceituais sobre a Lei Geral de Proteção de Dados

Com a evolução da era digital e o constante fluxo de informações pessoais que são compartilhados na internet, houve a necessidade de criação da Lei Geral de Proteção de Dados (LGPD), para regular o uso de dados pessoais e garantir o direito à privacidade. Assim se faz necessário entender o contexto histórico em que a LGPD surgiu. “O Ministério da Justiça,

iniciou em dezembro de 2010, uma consulta pública sobre o anteprojeto de lei que pretende garantir a proteção de dados pessoais, inclusive na internet[...]" (Santos, 2021, p.1).

Devido à grande pressão que ocorreu, com relação aos casos de vazamentos de dados do Wikileaks; a exposição de informações sigilosas feitas por Edward Snowden*;* e o escândalo envolvendo a Cambridge Analytica, era necessário que houvesse a criação de uma lei o quanto antes para regular e proteger essas informações. Dessa maneira, foi encaminhado o anteprojeto à Câmara dos Deputados, que mais adiante, se transformaria na PL 5276/2016, para então ser discutida no Senado Federal.

Todavia, somente em 2018, com a condição de que o Brasil precisava se tornar um país-membro da Organização para Cooperação e Desenvolvimento Socioeconômicos (OCDE) e que essa lentidão estava originando prejuízos econômicos ao país (BIONI, 2018), além de que, no mesmo ano, ocorreu o escândalo da Cambridge Analytica*,* em que a empresa teria obtido dados pessoais dos usuários do Facebook e utilizado para influenciar as eleições dos Estados Unidos (Globo, 2018).

Dessa forma, em 14 de agosto de 2018, o presidente Michel Temer sancionou a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, cujo fundamento é garantir segundo a legislação:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I. o respeito à privacidade;
> II. a autodeterminação informativa;
> III. a liberdade de expressão, de informação, de comunicação e de opinião;
> IV. a inviolabilidade da intimidade, da honra e da imagem;
> V. o desenvolvimento econômico e tecnológico e a inovação;
> VI. a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (art. 2ºda Lei n. 13.709, de 14 de agosto de 2018) (Brasil, 2018).

Nesse contexto, nota-se a importância de preservação desses fundamentos, pois é através deles, que os direitos fundamentais são preservados. Outrossim, é que, com a regulação do tratamento de dados, as empresas públicas e privadas devem exercer a boa-fé e seguir os princípios da finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (art. 6ºda Lei n. 13.709, de 14 de agosto de 2018) (Brasil, 2018).

Por isso, para que houvesse maior fiscalização da lei, foi necessário a criação da Autoridade Nacional de Proteção de Dados (ANPD), que segundo a Lei é: "responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional" (Art. 5º, inciso XIX, da Lei n. 13.709, de 14 de agosto de 2018). Nesse sentido, para que a ANPD cumpra

sua função, é essencial compreender suas competências, que determinam suas atribuições e atuação na proteção de dados pessoais:

> Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:
> I. propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
> II.elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade
> III.sugerir ações a serem realizadas pela ANPD
> IV.elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade;
> V.disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (art. 58, alínea B, da Lei n. 13.709, de 14 de agosto de 2018) (Brasil, 2018).

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade exerce um papel importante na formulação e acompanhamento das políticas de proteção de dados no Brasil. Entre suas principais competências, destaca-se a proposição de diretrizes estratégicas e o fornecimento de subsídios para a construção da Política Nacional de Proteção de Dados Pessoais e da Privacidade, além de contribuir para a atuação da ANPD. O conselho também tem a responsabilidade de elaborar relatórios anuais que avaliem a execução dessas políticas, sugerir ações para aprimorar a atuação da ANPD e promover debates e estudos que aprofundem o conhecimento sobre o tema. Ademais, desempenha um papel fundamental na disseminação de informações à população, buscando ampliar a conscientização e fortalecer a proteção dos direitos relacionados à privacidade e ao tratamento de dados pessoais.

A Lei Geral de Proteção de dados n. 13.709 de 2018, (art. 7º, inciso I) dispõem que o tratamento de dados pessoais deve ser realizado com o "consentimento do titular", ou seja, tudo o que for feito com as informações do usuário, deve ter o consentimento expresso. Por conseguinte, o compartilhamento desses dados, deve ser feito com transparência sobre a finalidade e o uso de tais informações, buscando maior controle e segurança aos usuários.

Ademais, para entender a lei, é necessário conhecer o que seriam os dados pessoais e segundo a LGPD, é "informação relacionada a pessoa natural identificada ou identificável". (art. 5º, I da Lei n. 13.709, de 14 de agosto de 2018) (BRASIL, 2018), ou seja, segundo a definição de: (FINKELSTEIN M. e FINKELSTEIN C., 2019, p. 296) "[...] podem englobar materiais como nome, endereço, endereço eletrônico, idade, estado civil de indivíduos e diversas outras possibilidades de informações". A Lei Geral de Proteção de dados descreve ainda que dado pessoal sensível é:

> [...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a

> uma pessoa natural (art. 5º, II da Lei n. 13.709, de 14 de agosto de 2018) (Brasil, 2018).

Acerca da titularidade dos dados pessoais a LGPD, definiu que "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei." (art. 17, da Lei n. 13.709, de 14 de agosto de 2018). Nesse sentido, entende-se que esses dados devem ser preservados, protegidos e por isso há uma grande necessidade que as instituições financeiras atendam às exigências estabelecidas pela LGPD para preservar tais informações, pois, quando há uma falha e ocorre o vazamento desses dados, o controlador ou operador que tem o domínio dessas informações, responde solidariamente pelos danos que foram causados, e é obrigado a reparálos, tanto o dano patrimonial, moral, individual ou coletivo. (art. 42, caput, inc. II da Lei n. 13.709, de 14 de agosto de 2018) (Brasil, 2018).

Sendo assim, é que essas informações ou dados pessoais possuem um grande valor econômico, para as instituições bancárias, pois, ajuda a reduzir custos, em relação a capacidade de processamento das informações e traz mais rapidez. E com o consentimento do usuário, o acesso a esses dados, fará com que os bancos, tenham produtos e serviços mais personalizados para cada cliente, gerando maior concorrência e ofertas melhores aos seus clientes.

2.2 Princípios da LGPD

Com o avanço da era digital, houve a necessidade de que as informações recolhidas dos usuários pelas empresas públicas e privadas fossem mantidas em segurança, ou seja inúmeros países foram obrigados a criarem leis para proteger e regularizar o tratamento de dados pessoais. No Brasil, não foi diferente, mas, para que isso ocorresse, houve um impulso também através do regulamento General Data Protection (GDPR), onde a União Europeia foi a precursora no contexto mundial de governança de dados, promovendo uma cultura de respeito à privacidade e segurança da informação.

Dessa forma, em 14 de agosto de 2018 a Lei Geral de Proteção de Dados surgiu e com ela a necessidade de princípios que norteassem a regulamentação das informações pessoais, buscando a proteção de direitos fundamentais do sigilo, ética e transparência conforme:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
> (art. 6ºda Lei n. 13.709, de 14 de agosto de 2018) (Brasil,2018).

Percebe-se então que, um dos princípios que norteiam a LGPD no seu artigo 6º é a proteção dos direitos fundamentais de boa-fé, liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, ou seja, tanto as empresas públicas ou privadas independentemente do país, da sua sede, devem respeitar esses princípios. Por essa razão, essa lei trouxe mudanças em todos os setores, pois esses princípios são fundamentais para a transparência, segurança e prevenção.

Ressai que o princípio da finalidade nada mais é que os dados ou informações coletadas dos usuários devem ter um propósito legítimo, específico e explícito informados ao titular, ou seja, essas empresas devem informar com precisão os seus clientes para qual finalidade as suas informações irão ser utilizadas. O princípio da adequação nada mais é do que a compatibilidade do tratamento de dados com finalidade informada ao titular, ou seja, essa compatibilidade deve seguir o que foi informado ao titular.

O princípio do livre acesso, nada mais é do que garantir ao titular, o direito de ter o acesso facilitado e gratuito aos seus dados e a duração do tratamento. Ademais, o direito a qualidade de dados é um dos princípios dessa lei, onde é explicitado os direitos com clareza e relevância e para o cumprimento da finalidade de seu tratamento. A transparência nada mais é do que a garantia de confiabilidade sobre a clareza das informações e acesso facilitado sobre essas informações.

A segurança é a utilização de técnicas de proteção que visa proteger os dados pessoais de vazamentos, acessos não autorizados e acidentes de destruição, perda ou alteração desses dados. A prevenção é a adoção de meios para que se evite danos em relação ao tratamento de dados. A não discriminação nada mais é que a impossibilidade de uso dessas informações para tratamentos discriminatórios, ilícito ou abusivos e pôr fim a responsabilização e prestação onde dever ser demonstrado a adoção de medidas eficazes para o cumprimento e a observância das normas de proteção de dados e sua eficácia. (art. 6ºda Lei n. 13.709, de 14 de agosto de 2018) (Brasil,2018)

2.2.1 Direitos dos Titulares de Dados

A regulação do tratamento de dados no Brasil teve um avanço significativo com a aprovação da LGPD, que se apoia em normas e regulações internacionais para garantir a proteção dos direitos fundamentais dos titulares de dados. Conforme o artigo 5º, V, da LGPD, considera-se titular qualquer pessoa natural cujos dados pessoais sejam objeto de tratamento.

Dessa forma, o titular fornece seus dados aos operadores e controladores, mas a legislação estabelece limites claros para esse uso. Segundo o artigo 5º, XII, da LGPD, o tratamento de dados deve ocorrer mediante consentimento explícito do titular, caracterizado por uma manifestação livre, informada e inequívoca para uma finalidade específica. Assim, a coleta e uso dessas informações só podem ser realizados com a devida autorização, reforçando o princípio da transparência e da autodeterminação informativa. Nessa perspectiva, conforme Teixeira e Armelin:

> O consentimento do titular de dados é a forma mais conhecida do tratamento legal de dados e deve ser livre e o mais consciente possível, ou seja, o titular deve ter pleno conhecimento de quais dados estão sendo captados e exatamente para qual fim ele será utilizado, o qual perfaz a inequivocabilidade do consentimento (Teixeira; Armelin, 2019, p.43).

Apesar de todo o consentimento, ainda existe uma dualidade na proteção de dados que, em parte, mostra a importância da autonomia privada em que o cidadão oferece o seu consentimento, porém, em outro, os usuários estão extremamente vulneráveis nas suas relações com as empresas. Importante destacar ainda que, os direitos dos titulares de dados estão elencados no artigo 18 da LGPD, que diz:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;

> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> (art. 18 da Lei n. 13.709, de 14 de agosto de 2018) (BRASIL,2018).

Conforme esse artigo, todos os titulares têm direito de requerer dos controladores as suas informações, a qualquer momento e mediante requisição. Por conseguinte, o titular tem o direito de verificar se realmente à existência de tratamento, o acesso aos dados e informações, correção de dados incompletos inexatos ou desatualizados, a anonimização, bloqueio ou eliminação de dados que não sigam a LGPD. A transferência de dados a outro fornecedor de serviço ou produto mediante requisição, a eliminação dos dados pessoais mesmo tratados com o consentimento do titular, acesso as informações das entidades públicas e privadas com os quais o controlador realizou o compartilhamento de dados, informações sobre a possibilidade de não fornecer o consentimento e a revogação do consentimento.

2.2.2 Responsabilidades dos Controladores e Operadores

Em síntese, o controlador toma as decisões e os operadores seguem as orientações do controlador está previsto no artigo 39 da LGPD e, por isso, o controlador deve adotar processos e políticas internas que cumpram as normas de proteção de dados. O principal objetivo desses agentes é estabelecer confiança com os titulares. Versando sobre os controladores e operadores segundo a lei:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (art. 50 da Lei n. 13.709, de 14 de agosto de 2018) (Brasil, 2018).

Nessa perspectiva, os controladores e operadores poderão formular suas regras e boas práticas desde que sigam os princípios estabelecidos pela LGPD, por conseguinte, eles deverão demonstrar a efetividade de seu programa de governança e promover o cumprimento de boas práticas ou condutas seguindo os princípios da Lei Geral de Proteção de Dados (Brasil, Lei 13.709/2018). Sendo assim, Goettenauer explica:

> Como consequência, diluem-se às fronteiras entre público e privado, na medida em que tanto o regulador estatal quanto os agentes privados, especialmente os identificados como controladores, têm responsabilidade de estabelecer parâmetros e mecanismos de monitoramento para atuação dos operadores. Visualiza-se, assim, um cenário de regulação multipolar, sem um núcleo único de convergência. (GOETTENAUER, 2020, p. 180).

Destaca-se a fusão entre as esferas pública e privada na regulação da proteção de dados. Tanto o Estado quanto os agentes privados, especialmente os controladores, devem criar diretrizes e mecanismos para monitorar os operadores. Isso resulta em um modelo de regulação descentralizado e multipolar, sem um único centro de decisão, exigindo cooperação entre diferentes setores para garantir o cumprimento da LGPD.

Ademais, como dispõe o art. 18, o controlador ou o operador dos dados pessoais, que gerarem dano, deverão repará-lo em todas as suas esferas, ou seja, tanto no âmbito patrimonial quanto o moral. Dessa maneira, o controlador ou operador que causarem dano, devem repará-los, além disto, segundo a LGPD tanto o controlador quanto operador respondem solidariamente pelos danos causados pelo tratamento de dados se descumprirem os princípios e obrigações impostas pela LGPD, portanto eles têm a obrigação de proteger e evitar possíveis problemas.

2.2.3 Sanções e Penalidades da LGPD

As sanções e penalidades previstas, se devem ao não cumprimento dos princípios e regras da Lei Geral de Proteção de Dados e conforme disciplina o art. 52 da Lei Geral de Proteção de Dados:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;

> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Sendo assim os agentes devem seguir as normas para que não haja advertências, multas, bloqueios entre outras penalidades. Depreende-se que com a criação da LGPD era necessário também criar uma autoridade que controlasse, fiscalizasse e zelasse pela aplicação da lei, dessa maneira, surgiu a Autoridade Nacional da Proteção de Dados (ANPD), que conforme a lei:

> Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)
> I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)
> II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)
> V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)
> VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)
> VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)
> VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)
> IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019). (BRASIL, 2018).

Portanto, a ANPD é a responsável por zelar, elaborar diretrizes, fiscalizar, promover na população o conhecimento da norma e políticas públicas sobre a proteção de dados e promover ações de cooperação com outros países. O Conselho Nacional de Proteção de Dados

Pessoais e da Privacidade desempenha um papel fundamental na regulamentação da proteção de dados no Brasil. Responsável por propor diretrizes e estratégias para a elaboração de leis, esse órgão também orienta a atuação da ANPD, elabora relatórios anuais e promove ações voltadas à conscientização sobre privacidade e segurança de dados (Lei n. 13.709, de 14 de agosto de 2018).

A atuação desse conselho e da ANPD é essencial para garantir que os titulares de dados pessoais tenham seus direitos protegidos. A expectativa é que os agentes de tratamento ajam com responsabilidade ao lidar com informações sensíveis, evitando prejuízos aos direitos fundamentais das pessoas. Entre esses direitos, destaca-se a privacidade, que visa proteger dados contra vazamentos e ataques, assegurando um ambiente digital seguro e confiável.

2.2.4 Impacto da LGPD nos negócios

A lei Geral de Proteção de Dados trouxe consigo a mudança na cultura de compartilhamentos, tanto pelas empresas públicas quanto privadas, possibilitando assim uma maior confiança nos agentes de tratamentos de dados. Ademais, no âmbito do meio digital, algumas empresas utilizam os dados pessoais para determinar padrões de consumo no futuro e publicidades são direcionadas para esse público, porém, o uso dessas informações pode ser danoso, pois se essas informações fossem utilizadas por exemplo no preço de medicamentos ocorreriam sérios riscos (Martins; Longhi; Júnior, 2022).

Nesse sentido, o objetivo de determinadas empresas no meio digital conforme Peirano (2019, p. 16) explica "é converter cada pessoa viva em uma célula de sua base de dados, para poder enchê-la de informação", ou seja, sua síntese é que essas informações são tratadas como mercadorias, sendo ofertadas a quem paga mais para obtê-las. O artigo 2º, VI, da Lei 13.709/2018, traz consigo a defesa do direito do consumidor como base da proteção de dados pessoais, pois deve haver um equilíbrio tanto por parte do consumidor quanto pelo do fornecedor, dessa forma, a responsabilidade civil nas relações de consumo conforme o Código de Defesa do Consumidor:

> O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. (art. 12 da Lei n. 8.078, de 11 de setembro de 1990) (BRASIL, 1990).

Percebe-se que, quem causou o dano, independentemente de culpa, responde civilmente por isso. Outrossim, é que quando os dados são usados para a criação de perfis comportamentais da pessoa, podem ocorrer diversos abuso e prejuízos, nesse sentido é de suma importância estabelecer limites pela lei a essas situações. Segundo Doneda (2019, p. 44) “o direito precisa ser aplicado à realidade da arquitetura social para atingir sua plena realização e a realidade é hoje em boa parte condicionada pelo desenvolvimento tecnológico”. Ou seja, a realidade que vivemos é basicamente condicionada a dependência tecnológica, por isso a importância de estabelecer limites ao uso da tecnologia, pois o mau uso dela pode trazer sérios riscos para os usuários.

3 O TRATAMENTO DE DADOS PELAS INSTITUIÇÕES FINANCEIRAS E A LEI GERAL DE PROTEÇÃO DE DADOS

As instituições financeiras lidam diariamente com um grande volume de dados e informações pessoais de seus clientes, o que exige um elevado grau de responsabilidade quanto à segurança e à confidencialidade dessas informações. Para garantir a proteção desses dados, é fundamental que essas instituições cumpram rigorosamente as diretrizes estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD), que regulamenta o tratamento de dados no Brasil. A não observância da legislação pode acarretar consequências significativas, como advertências, multas simples de até 2% do faturamento da empresa, aplicação de multa diária, publicização da infração, bloqueio ou eliminação dos dados pessoais, suspensão parcial do banco de dados, suspensão do exercício da atividade de tratamento de dados, e até mesmo a proibição parcial ou total da atividade (Brasil, 2018).

Diante dessas possíveis sanções, previstas no art. 52, inciso II, da Lei n. 13.709, de 14 de agosto de 2018, é imprescindível que o setor bancário adote medidas técnicas e administrativas eficazes para proteger os dados que coleta e armazena. A LGPD não apenas impõe obrigações legais, mas também reforça a importância da ética e da transparência no relacionamento com os consumidores. Assim, é necessário que as instituições desenvolvam uma cultura de proteção de dados, investindo continuamente em segurança da informação, capacitação de seus colaboradores e revisão de seus processos internos, a fim de garantir o cumprimento da legislação e preservar a confiança dos clientes.

3.1 Conformidade e Boas Práticas

Para que haja conformidade e boas práticas, portanto, é necessário conhecer o que seria o tratamento de dados irregulares e está previsto na Lei nº 13.709, de 14 de agosto de 2018, art.44, que diz que o tratamento de dados irregulares nada mais é que deixar de seguir ou observar a legislação e quando não puder fornecer a segurança que o titular espera. (art.44,

caput da Lei n. 13.709, de 14 de agosto de 2018) (Brasil, 2018). Por isso, toda empresa pública ou privada que lida com o tratamento de dados deve observar a LGPD para evitar possíveis irregularidades. Outrossim é que os controladores e operadores poderão formular regras e boas práticas segundo a LGPD:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular (BRASIL, 2018).

O Banco Central do Brasil atua como órgão regulador, fiscalizando o sistema financeiro e assegurando o cumprimento das normas pelas instituições. Da mesma maneira, a Autoridade Nacional de Proteção de Dados (ANPD) trabalha para garantir a observância dos princípios e diretrizes da LGPD, reforçando a necessidade de uma governança eficiente sobre o uso de informações pessoais. Essa preocupação é evidenciada na reflexão de Harari, citada por Jarude e Silveira, que alerta para a urgência de se estabelecer parâmetros claros para a propriedade dos dados:

> Assim, faríamos melhor em invocar juristas, políticos, filósofos e mesmo poetas para que voltem sua atenção para essa charada: como regular a propriedade de dados? Essa talvez seja a questão política mais importante da nossa era. Se não formos capazes de responder a essa pergunta logo, nosso sistema sociopolítico poderá entrar em colapso (SILVEIRA, 2021, p.85).

Assim, percebe-se que a regulação da propriedade de dados se tornou uma questão fundamental na atualidade, exigindo esforços conjuntos entre juristas, políticos e especialistas para evitar possíveis impactos negativos no sistema sociopolítico e fortalecer a proteção das informações pessoais (Susskind, 2024). As instituições financeiras devem sempre verificar as informações coletadas e armazenadas para que não haja irregularidades e há também uma certificação internacional da segurança da informação que é o ISO 27001, onde é possível saber que a empresa mantém um comprometimento com a segurança das informações.

3.1.1 Transparência e Consentimento

A transparência é um dos princípios fundamentais da Lei Geral de Proteção de Dados Pessoais (LGPD) e está relacionada à clareza, objetividade e acessibilidade das informações sobre o tratamento de dados pessoais. No âmbito das instituições financeiras, isso implica o dever de informar, de forma clara e compreensível, como os dados dos clientes são coletados, armazenados, compartilhados e protegidos. Essa obrigação busca coibir práticas abusivas, dissimuladas ou arbitrárias, promovendo um relacionamento mais ético e seguro entre as instituições e os titulares dos dados.

Outro pilar essencial da LGPD é o consentimento, previsto no art. 7º da referida lei, que consiste na autorização expressa do titular para o tratamento de seus dados pessoais. Para ser válido, esse consentimento deve ser livre, informado e inequívoco, ou seja, o titular precisa compreender exatamente quais dados serão utilizados, com qual finalidade e por quais meios. A lei assegura o direito de revogação a qualquer momento, reforçando a autonomia do indivíduo sobre suas informações. Diante disso, é fundamental que as instituições financeiras priorizem tanto a transparência quanto o consentimento em suas políticas internas, garantindo conformidade legal e respeito à privacidade de seus clientes.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018).

Embora o consentimento do titular seja uma das bases legais mais conhecidas para o tratamento de dados pessoais, a LGPD prevê exceções em que esse consentimento não é

necessário. Entre essas hipóteses estão o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas pela administração pública, a realização de estudos por órgãos de pesquisa, desde que, sempre que possível, os dados sejam anonimizados, além de situações que envolvem a execução de contratos ou procedimentos preliminares relacionados ao titular. Também se dispensa o consentimento nos casos de exercício regular de direitos em processos judiciais, proteção da vida ou da incolumidade física, tutela da saúde por profissionais ou autoridades sanitárias, interesse legítimo do controlador e proteção do crédito.

Essas exceções demonstram que o tratamento de dados pode ser legítimo mesmo sem o consentimento do titular, desde que respeitados os princípios da finalidade, necessidade e proporcionalidade. Conforme observa o Ministro Gilmar Mendes, é preciso buscar um equilíbrio entre o interesse público e a proteção da privacidade, de modo que os direitos fundamentais não sejam violados sob o pretexto de atender a interesses coletivos. Assim, a LGPD estabelece um marco importante na garantia de que o uso dos dados pessoais, mesmo quando permitido sem consentimento, seja feito com responsabilidade, transparência e respeito à dignidade do cidadão.

> DIREITO CONSTITUCIONAL. DIREITOS FUNDAMENTAIS À PRIVACIDADE E AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE. TRATAMENTO DE DADOS PESSOAIS PELO ESTADO BRASILEIRO. COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. ADI E ADPF CONHECIDAS E, NO MÉRITO, JULGADAS PARCIALMENTE PROCEDENTES. INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO. DECLARAÇÃO DE INCONSTITUCIONALIDADE COM EFEITOS FUTUROS. [...] 3. O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. Interpretação conforme à Constituição para subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público [...]. (TP-DF -ADI 6649, Relator: GILMAR MENDES, Data de Julgamento: 15/09/2022, Tribunal Pleno, Data de Publicação: 19/06/2023). (BRASIL,2022).

O tratamento de dados pessoais pelo Estado deve respeitar princípios fundamentais, especialmente a transparência e o consentimento dos titulares. Ainda que o compartilhamento de informações entre órgãos públicos seja necessário para a prestação de serviços eficientes, ele não pode ocorrer de forma indiscriminada. A LGPD estabelece requisitos rigorosos para

garantir que qualquer uso de dados pessoais respeite a finalidade informada e não viole os direitos dos cidadãos.

Assim, o consentimento do titular surge como um mecanismo essencial, permitindo que ele tenha controle sobre o uso de suas informações e assegurando a conformidade com a legislação vigente. Dessa maneira, a transparência no tratamento de dados fortalece a confiança na administração pública e previne abusos ou irregularidades no compartilhamento de informações pessoais.

3.1.2 Segurança de Dados

A segurança de dados na era digital tem sido debatida e modificada todos os dias, pois com a constante mudança na tecnologia é necessário que a lei acompanhe toda essa evolução e é por isso que o Banco Central do Brasil atua como órgão regulador conjuntamente com a ANPD, para garantir a proteção dos princípios da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), sendo assim, a Resolução nº 4.658, de 26 de abril de 2018, desponta que:

> Art. 1º Esta Resolução dispõe sobre 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 financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. (BACEN, p. 1) (BRASIL, 2018).

De acordo com a resolução do Banco Central, as instituições autorizadas a operar devem seguir as políticas de segurança e incluir medidas adicionais de proteção além de que devem contemplar:

> Art. 3º A política de segurança cibernética deve contemplar, no mínimo:
> I - os objetivos de segurança cibernética da instituição; II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;
> III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
> IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;
> V - as diretrizes para:
> a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;
> b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;
> c) a classificação dos dados e das informações quanto à relevância; e
> d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;
> VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

> a) a implementação de programas de capacitação e de avaliação periódica de pessoal; b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros[...]. (BACEN, p. 2) (BRASIL, 2018).

Dessa forma, é imprescindível que todas as instituições financeiras adotem políticas robustas de segurança da informação, com controles específicos capazes de minimizar vulnerabilidades em seus sistemas, prevenindo vazamentos de dados e ataques cibernéticos. Entre essas medidas, destacam-se os mecanismos voltados à rastreabilidade das informações, à proteção de dados sensíveis e à análise de riscos e impactos em caso de incidentes.

A criação de estratégias para disseminar a cultura da segurança cibernética é essencial, o que inclui a capacitação contínua dos colaboradores para lidar adequadamente com informações sigilosas, uma vez que as falhas internas também representam riscos relevantes. A Resolução n.º 4.658/2018, do Banco Central do Brasil, estabelece diretrizes para a governança cibernética no setor financeiro, reforçando a importância da proteção de dados e da privacidade dos usuários. Conforme aponta Santos, tais diretrizes contribuem para estruturar um ambiente financeiro mais seguro e resiliente diante das ameaças digitais.

> A resolução 4.658/18 tem o objetivo de efetivar a governança cibernética no que tange a proteção de dados e privacidade de seus usuários. Para isso, é possível diante das ações previstas, efetivar a gestão de riscos, o compliance, e os controles internos. Visando a melhoria, o grau de sensibilidade dos dados e informações que percorrem nas instituições financeiras, o Bacen exigiu que as instituições financeiras se adequem a: definir, implementar, divulgar e manter política de segurança cibernética formulada a partir de princípios e diretrizes que busquem assegurar a confidencialidade, integridade e disponibilidade dos dados dos sistemas de informação utilizados. Reiterando que, as empresas devem garantir a efetivação de um plano de ação e de respostas a incidentes cibernéticos. Aponta, ainda, que a resolução do Bacen visa garantir políticas para gerenciamento de riscos referentes à continuidade de negócios, proteção e privacidade de dados, definindo: o tratamento dos incidentes cibernéticos, procedimentos que devem ser seguidos no caso de interrupção de serviços de computação nuvem contratados, armazenamento e processamento de dados (SANTOS, 2021, p. 4).

Nessa ótica, portanto a resolução 4.658/18 veio com objetivo de proteger os dados e a privacidade do usuários, mas para isso é necessário que as instituições financeiras se adequem e façam uma efetiva gestão de riscos e controles internos para evitar o vazamentos de informações sigilosas ou seja, tomar medidas para evitar acessos não autorizados, situações em que haja a perda, alteração dessas informações e detectação de falhas, pois, uma simples falha pode acarretar um enorme vazamento de informações sigilosas (Daniel, 2022).

Para mais, a segurança de dados pessoais é um dos pilares da Lei Geral de Proteção de Dados e como as instituições financeiras são alvos de ataques cibernéticos diariamente quando há um vazamento de informações a credibilidade daquela instituição cai, por isso a LGPD ela

veio para fazer a gestão de riscos e uma das medidas de segurança utilizadas é a criptografia dos dados, pois segundo Susskind (2024, p.2) “mesmo em caso de acesso não autorizado, os dados estejam protegidos contra leitura indevida”.

Ademais, a Lei Geral de Proteção de Dados exige que todas as instituições financeiras nomeiem um Encarregado de Proteção de Dados (DPO) que nada mais é que o responsável por intermediar a comunicação com Autoridade Nacional de Proteção de Dados (ANPD) e com os titulares de dados (SUSSKIND, 2024) e segundo a Lei nº 13.709, de 14 de agosto de 2018, Art. 55-J, inc. XIII, diz “ [...] bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei” (BRASIL,2018).

O Encarregado de Proteção de Dados ele é responsável por garantir e orientar as instituições na proteção dos dados e que elas sigam a lei. Ressai que com relação a cibersegurança Nakamura destaca:

> No universo digital, todos estão suscetíveis aos ataques cibernéticos. Um indivíduo, um cidadão aleatório de um país ou um colaborador de uma organização que possuem a sua identidade digital são alvos importantes, que devem ser considerados. A relevância das pessoas na cibersegurança é grande porque elas são, muitas vezes, utilizadas como entrada ou parte do fluxo de ataques cibernéticos em empresas, instituições ou organizações de diferentes tamanhos e setores. Além das pessoas, há o parque tecnológico, que inclui sistemas, equipamentos ou plataformas que são alvos constantes de ataques cibernéticos. Adicionalmente, há os ativos físicos, que também representam riscos cibernéticos. O escopo da cibersegurança em uma empresa normalmente consiste em sua rede interna ou corporativa. Mas o provisionamento de serviços para clientes ou mesmo para os usuários internos já expande o escopo e, principalmente, a superfície de ataques (NAKAMURA, 2024, p. 307).

Nakamura destaca que todos estão suscetíveis a ataques cibernéticos, sendo essencial a existência de um preparo ou uma gestão de riscos para minimizar ou controlar seus efeitos. Por esse motivo, é fundamental que as instituições financeiras se adequem à legislação vigente, a fim de evitar acessos indevidos às informações e garantir a proteção dos dados.

3.1.3 Impacto das Sanções

Se os agentes de tratamento de dados cometerem alguma infração agindo de forma irregular com a Lei Geral de Proteção de Dados eles sofrerão sanções que estão previstas no art. 52 da Lei nº 13.709, de 14 de agosto de 2018, como multas, bloqueios, suspensão do exercício das atividades entre outros. Os controladores e operadores respondem solidariamente pelos danos causados quando descumprirem a LGPD além de que caso alguma instituição

financeira viole a lei ela perderá também, a confiança do seu cliente o que acarretará sérios riscos financeiros além das penalidades impostas pela lei.

Nesse sentido, as empresas públicas e sociedades de economia mista devem garantir a segurança das informações, informando de maneira clara e acessível, por meio de relatórios e plataformas digitais, o tratamento dado aos dados pessoais e sua finalidade. A LGPD determina a manutenção de registros detalhados sobre o uso das informações, assegurando que, em casos de irregularidades, os dados estejam disponíveis para análise das autoridades competentes, contribuindo para a conformidade e fiscalização da lei e conforme Almeida e Soares:

> As empresas públicas e as sociedades de economia mista, devem adotar medidas que visem a segurança das informações, além de informar de forma específica e clara por meio de relatórios e sites, o tratamento e os impactos à proteção de dados pessoais de suas atividades ao seu titular ou responsável legal, seu uso e finalidade. A Lei nº 13.709/18 - LGPD em toda a sua extensão, prevê obrigações para que as empresas e as instituições possam manter o registro e tratamento dos dados visando em ações futura, sua utilização, e/ou em casos de irregularidades, estejam disponíveis a autoridades nacionais para futuras decisões (ALMEIDA; SOARES, 2022, p.14).

Portanto, o descumprimento da LGPD pode resultar em severas sanções, que vão desde advertências até multas significativas, podendo atingir 2% do faturamento da empresa, limitada a R$ 50 milhões por infração (art.52, inc. II, da Lei n. 13.709, de 14 de agosto de 2018) (BRASIL, 2018). Além das penalidades financeiras, o não cumprimento às normas pode levar à suspensão das atividades de processamento de dados, impactando diretamente a operação da instituição.

Empresas que não se adequam à legislação correm o risco de perder a confiança de seus clientes, o que pode comprometer sua reputação e sustentabilidade no mercado. Todas as empresas devem adotar medidas preventivas para evitar vazamentos e irregularidades, garantindo não apenas a conformidade com a legislação, mas também a proteção da credibilidade e continuidade dos negócios.

4 OPEN FINANCE E A LEI GERAL DE PROTEÇÃO DE DADOS

O *Open Finance* representa uma evolução do *Open Banking*, surgindo como resposta às transformações tecnológicas que modificaram a forma como os serviços financeiros são ofertados. Antes prestados de forma presencial, os serviços bancários passaram a ser acessados digitalmente, especialmente por meio de dispositivos móveis. Nesse contexto, o *Open Banking* foi desenvolvido com o objetivo de agilizar o compartilhamento de dados, ampliar a oferta de produtos e serviços, além de proporcionar maior integração e personalização das soluções financeiras disponíveis.

A partir desse avanço, o *Open Finance* ampliou o escopo de atuação do Open Banking, permitindo que diferentes instituições financeiras compartilhem dados de forma padronizada, com o consentimento do cliente, reunindo diversos serviços em um único ambiente digital. Essa integração visa atender às necessidades dos consumidores de forma mais eficiente e personalizada, promovendo uma experiência financeira mais acessível e centrada no usuário.

De acordo com o art. 3º da Resolução Conjunta nº 4/2022, os principais objetivos do *Open Finance* são: incentivar a inovação, fomentar a concorrência entre instituições, aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro e promover a cidadania financeira. Assim, o modelo contribui para um mercado mais dinâmico, oferecendo melhores condições e soluções aos clientes por meio de maior competitividade e transparência.

4.1 Introdução ao Open Finance

O *Open Finance*, ou sistema financeiro aberto, permite que clientes compartilhem seus dados pessoais e transacionais entre instituições financeiras autorizadas pelo Banco Central. Esse compartilhamento só pode ocorrer com a autorização do titular, devendo conter a finalidade específica e o prazo de utilização das informações. A iniciativa busca oferecer mais

autonomia aos consumidores, promovendo transparência e inovação no setor financeiro. (BANCO CENTRAL DO BRASIL, 2023).

Além disso, o *open finance* é uma evolução do open banking*,* pois, o open banking é mais voltado para dados e serviços bancários "O Open Banking é a padronização do processo de compartilhamento de dados e serviços financeiros pelas instituições, por meio de abertura e integração de plataformas e infraestruturas de tecnologia" (Banco Central do Brasil, 2021, p. 3). Já o *open finance* é considerado uma ideia mais ampla, porque abrange credenciamento, câmbio, investimentos, seguros e previdência.

Diante do avanço das tecnologias e da transformação digital no setor financeiro, tornou-se indispensável a integração da LGPD. Essa legislação tem como finalidade orientar e regulamentar o uso de dados pessoais, assegurando maior segurança no compartilhamento de informações entre usuários e instituições financeiras, sejam elas públicas ou privadas. A aplicação da LGPD proporciona uma base legal sólida para garantir a privacidade dos dados e fortalecer a confiança dos consumidores nos serviços digitais.

Nesse contexto, muitas instituições financeiras, visando adotar boas práticas de governança e preservar sua reputação no mercado, recorrem ao compliance como uma estratégia essencial. Conforme a Federação Brasileira de Bancos (FEBRABAN, 2018), o compliance significa "estar em conformidade" com leis, normas e regulamentos, sendo um dos pilares na gestão de riscos. Ele orienta a conduta institucional, promovendo integridade, ética e responsabilidade, e está estruturado em componentes que visam prevenir, detectar e responder a eventuais irregularidades.

> O Programa de Compliance é composto de políticas, procedimentos e planejamento de atividades que visam fortalecer as Instituições direcionando as ações para a condução dos negócios de forma adequada, em relação ao cumprimento das leis e regulamentações, questões de ética e conduta, aspectos concorrenciais e socioambientais, contratos com terceiros, normas contábeis, entre outros. Para construção de um programa efetivo, devem-se considerar as boas práticas disponíveis globalmente e adequá-las ao porte, à complexidade, à estrutura, ao perfil de risco, ao modelo de negócio e à base legal e regulatória a que a Instituição está submetida. A estrutura da área de Compliance bem como suas responsabilidades devem estar aderentes às exigências legais e regulamentares aplicáveis nas jurisdições em que a Instituição opera (FEBRABAN, 2018, p. 8)

Assim, para fortalecer sua imagem e manter a conformidade legal, as instituições devem adotar boas práticas reconhecidas globalmente, ajustando-as ao seu porte, estrutura, modelo de negócio e perfil de risco. Esse alinhamento é fundamental para construir uma reputação sólida e confiável no mercado.

4.1.2 Impacto da LGPD no Open Finance

O *open finance* é regulamentado pelo Banco Central do Brasil e deve observar rigorosamente as disposições da LGPD e da Lei de Sigilo Bancário (BARROSO, 2020). Assim, todas as informações compartilhadas no âmbito desse sistema precisam cumprir os requisitos legais que garantem a privacidade e segurança dos dados pessoais dos usuários.

A coleta desses dados inclui informações como nome, endereço, e-mail, entre outros. O uso dessas informações por entes públicos e privados depende, em regra, da autorização expressa do titular. Contudo, existem exceções previstas em lei, como o uso pelo poder público para estudos e políticas públicas, especialmente na área da saúde (CARVALHO, 2024).

A LGPD tem como objetivo proteger os direitos fundamentais, sendo assim, ela visa proteger os direitos de liberdade, privacidade e o livre desenvolvimento da pessoa natural. (BRASIL,2018). Dessa forma, fica evidente que o titular dos dados está em posição vulnerável diante das instituições que os utilizam, o que justifica a necessidade da criação da LGPD para garantir a proteção desses dados.

Nesse sentido, ao abordar o compartilhamento de dados pelo Estado e outros entes, Carvalho (2024) reforça a importância de que essas operações respeitem os limites legais, assegurando sempre a proteção dos direitos dos titulares e promovendo a transparência no uso das informações.

> Os dados coletados pelo Estado podem ser compartilhados entre entes para fins de pesquisa e ou políticas desenvolvimento não podendo ser compartilhado com entes privados. Salvo se houver o consentimento do titular sobre a possibilidade deste. Neste quesito empresas públicas terão os mesmos deveres dos entes privados, estas como (Petrobras, Correios, Banco do Brasil). Só terão o benefício de gozar dos direitos como ente público quando estas estiverem se fazendo do uso dos dados quanto para promover políticas públicas se forem utilizar para concorrência no mercado, serão tratadas de igual maneira como uma empresa privada normal. (CARVALHO, 2024, p. 115).

Dessa forma, a Lei Geral de Proteção de Dados (LGPD) foi criada com o propósito de proteger e amparar os titulares de dados, sejam eles tratados por empresas públicas ou privadas. A legislação busca evitar prejuízos aos indivíduos, que ocupam uma posição mais frágil nesse processo, garantindo-lhes maior controle sobre suas informações pessoais.

No contexto do sistema financeiro aberto, o *open finance* é regulamentado tanto pelo Banco Central do Brasil quanto pela LGPD, o que confere segurança ao seu funcionamento. Como destaca carvalho (2024, p. 119), “o *open finance* tange em um processo seguro, devido ser regulamentado pelo Banco Central, onde as instituições financeiras que apresentam o supracitado sistema têm por obrigação de fazer com que o processo nesse sistema seja de forma

protegida". Além disso, conforme a Resolução Conjunta nº 1, de 4 de maio de 2020, o *open finance* fundamenta-se em princípios como a transparência, a segurança, a portabilidade de dados e a promoção da cidadania financeira.

> Art. 4º As instituições de que trata o art. 1º, para fins do cumprimento dos objetivos de que trata o art. 3º, devem conduzir suas atividades com ética e responsabilidade, com observância da legislação e regulamentação em vigor, bem como dos seguintes princípios:
> I - transparência;
> II - segurança e privacidade de dados e de informações sobre serviços compartilhados no âmbito desta Resolução Conjunta;
> III - qualidade dos dados;
> IV - tratamento não discriminatório;
> V - reciprocidade; (Redação dada, a partir de 2/5/2022, pela Resolução Conjunta nº 4, de 24/3/2022.)
> VI - Interoperabilidade: (Redação dada, a partir de 2/5/2022, pela Resolução Conjunta nº 4, de 24/3/2022.) (BANCO CENTRAL DO BRASIL, 2020).

Conforme a Resolução do Banco Central do Brasil, o *open finance* é orientado por princípios como segurança, privacidade, transparência e qualidade dos dados, os quais estão diretamente alinhados com as diretrizes da LGPD. Caso esses princípios não fossem observados, haveria sérias violações legais e impactos significativos tanto para as instituições quanto para os titulares dos dados.

4.1.3 Direitos dos Titulares de Dados no Open Finance

A relação entre a LGPD e o *open finance* é direta, uma vez que este modelo depende do consentimento do titular de dados para funcionar plenamente. O artigo 7º, inciso I, da LGPD, determina que o tratamento de dados pessoais deve ocorrer somente mediante autorização do titular. Isso significa que nenhuma informação pode ser acessada ou compartilhada sem que o usuário permita de forma clara e consciente. Ou seja, o consentimento é um dos pilares que sustentam o *open finance*. Como aponta Malta:

> Nesse espectro, oportuno rememorar que a interação social nos dias atuais depende do fluxo informacional, de modo que o indivíduo, como parte mais vulnerável, consente ao tratamento de seus dados para assim alcançar sua conformação social, sob pena de sua exclusão, o que passa ao largo do almejado empoderamento do titular dos dados pessoais preconizado pelo princípio da autodeterminação informativa (MALTA, 2023, p.60).

Ou seja, as informações pessoais se tornaram moeda de troca e com isso o indivíduo que não a utiliza torna-se obsoleto e as vezes até excluído socialmente, além disto em um meio em que tudo gira em torno da celeridade e com apenas um clique o titular das informações consente e faz anuência sem mesmo ter refletido sobre os seus direitos e sobre o que versava

aquela autorização, corre riscos de aceitar algo que não lhe convém. Por isso a necessidade de buscar informações e procurar saber sobre os seus direitos e de também as empresas que colhem esses dados serem transparentes na hora de requerer esse consentimento. E ainda falando sobre transparência:

> O princípio da transparência é um dos pilares fundamentais do Open Finance, que busca garantir a confiança dos usuários no compartilhamento de seus dados financeiros. Em linhas gerais, a transparência no Open Finance refere-se à clareza e à objetividade com que as informações são apresentadas aos usuários, de modo que eles possam compreender como seus dados estão sendo utilizados e por quem. Isso inclui informações sobre quais dados estão sendo compartilhados, com quem e para quais finalidades. Em resumo, a transparência é um elemento crucial do Open Finance para garantir que os usuários tenham controle sobre seus dados financeiros e possam tomar decisões informadas sobre como compartilhá-los (TARGHER, 2023, p.23)

A transparência no open finance é fundamental para consolidar a confiança dos usuários no processo de compartilhamento de dados financeiros. Esse princípio está diretamente relacionado à clareza na apresentação das informações, permitindo que os indivíduos compreendam quem está acessando seus dados, com qual finalidade e de que forma serão utilizados. Ao garantir esse entendimento, o sistema reforça o poder de decisão dos usuários, assegurando que o consentimento seja concedido de maneira consciente e informada.

Nesse contexto, é imprescindível destacar que as instituições financeiras precisam obter autorização expressa dos clientes, processo realizado por meio de seus próprios canais eletrônicos. Essa autorização deve ser apresentada de forma clara, objetiva e adequada, especificando a finalidade do uso dos dados e o prazo de validade, que não pode exceder 12 meses. Após esse período, torna-se obrigatória uma nova autorização, conforme estabelecido pelo Banco Central do Brasil (2023), o que contribui para maior segurança e controle por parte dos titulares.

Além disso, os princípios voltados à experiência do cliente estão definidos na Instrução Normativa BCB nº 559, de 4 de dezembro de 2024 (BANCO CENTRAL DO BRASIL, 2024). A norma exige que o cliente receba informações precisas e no momento oportuno ao optar pelo compartilhamento de dados ou serviços.

Cabe à instituição receptora detalhar quais dados serão acessados, sua finalidade e possíveis usos futuros, conforme as diretrizes regulatórias. Em relação aos serviços, deve-se informar de forma transparente qual instituição será responsável pela execução, bem como as condições envolvidas. Esse cuidado evita informações desnecessárias ou confusas, assegurando maior tranquilidade ao usuário e respeito aos seus direitos.

4.1.4 Desafios e Oportunidades

A implementação do *open finance* no Brasil representa um avanço significativo na modernização do sistema financeiro, mas ainda enfrenta obstáculos que precisam ser superados para garantir sua consolidação. Entre os principais desafios estão a conscientização dos usuários, a adaptação das instituições financeiras às novas exigências regulatórias, a padronização tecnológica e a segurança no tratamento dos dados pessoais. A confiança do consumidor também é um fator crucial, já que o modelo depende diretamente do consentimento informado e da percepção de segurança por parte dos titulares de dados.

> 1. Estimular a adesão ao maior número possível de instituições financeiras e fintechs. Assim como exposto por Dratva (2020), se não houver uma adesão massiva das maiores instituições financeiras, o número de pessoas que serão impactadas pelo open finance pode não ser satisfatório para alcançar os seus objetivos.2. Garantir o sigilo e a privacidade dos dados dos usuários. A ameaça de que os dados privativos podem ser acessados indevidamente por terceiros tem sido apontado como um dos principais entraves à maior difusão do open banking no Reino Unido (RAMDANI et al., 2020) 3. Garantir a confiabilidade das APIs do sistema, de forma a permitir o adequado compartilhamento de dados com as demais instituições participantes do open 26 finance. Omarini (2020) propõe que as APIs são os principais componentes do open finance, e devem permitir a intercomunicação entre diversas instituições financeiras de forma livre de falhas, indisponibilidades ou incompatibilidades técnicas (MELO, 2023, p. 41)

Diante dos desafios apresentados, cabe ao Banco Central do Brasil desenvolver políticas que incentivem tanto instituições financeiras quanto os próprios consumidores a aderirem ao *open finance*, ampliando assim seu alcance e eficácia. Para isso, é essencial garantir o sigilo e a privacidade dos dados dos usuários, adotando medidas robustas de segurança da informação.

Entre essas medidas, destaca-se a capacitação dos profissionais envolvidos, assegurando que estejam aptos a lidar com dados sensíveis e operar corretamente os sistemas integrados. Além disso, é fundamental assegurar a confiabilidade das APIs, interfaces que permitem a comunicação entre diferentes sistemas financeiros, garantindo que sejam seguras, estáveis e livres de falhas técnicas que comprometam a experiência do usuário e a integridade do sistema.

Apesar do avanço tecnológico que o open finance representa, sua implementação ainda encontra barreiras significativas. Muitas empresas, especialmente de pequeno e médio porte, enfrentam dificuldades para adotar essa nova infraestrutura, sobretudo devido aos altos custos com equipamentos, atualizações de sistemas e adequações regulatórias. Isso demonstra que, além de políticas de incentivo, é necessário um suporte técnico e financeiro que permita a

inclusão de um número maior de participantes no ecossistema, contribuindo para a democratização do acesso aos benefícios proporcionados por essa inovação.

> Com isso, podemos notar que o open finance ainda possui pontos de melhoria, contudo no âmbito das empresas, alguns desafios, como garantir a segurança dos dados e lidar com o tratamento de dados fornecidos pode ser mitigado através de boas práticas e uma governança de dados que irá gerenciar a melhor maneira para lidar com os esses tópicos (CAMARGO, 2023, p.27).

Apesar dos desafios enfrentados, o open finance traz diversas oportunidades que podem transformar o mercado financeiro. Entre elas, destaca-se a redução dos custos de transação envolvidos no planejamento, distribuição, negociação e liquidação de acordos financeiros, conforme aponta o Banco Central do Brasil (2022). Essa economia impacta diretamente na eficiência dos processos, tornando as operações mais ágeis e acessíveis para diferentes perfis de usuários e instituições.

O *open finance* promove maior transparência e rastreabilidade na prestação de contas, o que fortalece a confiança dos consumidores e regula o ambiente financeiro. A inclusão financeira também é ampliada, uma vez que ferramentas automáticas possibilitam o acesso a serviços para um público mais amplo, democratizando o uso de produtos financeiros. Esse cenário estimula a competição entre as instituições, que, ao buscarem diferenciação, tendem a inovar constantemente e aprimorar a qualidade dos serviços oferecidos (BANCO CENTRAL DO BRASIL, 2023).

Outro benefício importante está na oferta de aplicativos voltados para aconselhamento e planejamento financeiro, que auxiliam os usuários a esclarecer dúvidas, controlar melhor seus recursos e realizar operações com maior segurança. Além disso, o sistema contribui para uma gestão dos riscos, beneficiando tanto os consumidores quanto as instituições financeiras, que passam a contar com informações mais precisas e atualizadas para tomada de decisões.

4.1.5 Casos de Sucesso

Uma das primeiras decisões judiciais de sucesso relacionada à infração da Lei Geral de Proteção de Dados (LGPD) envolveu a empresa Cyrela, que foi condenada a pagar uma indenização de R$ 10 mil por danos morais a um cliente. O caso ocorreu após a compra de um imóvel no bairro de Moema, quando o consumidor passou a ser contatado sem autorização por instituições financeiras, consórcios, empresas de arquitetura, construção e fornecimento de mobiliário planejado (OLIVEIRA *et al.,* 2021, p. 31).

Esse episódio evidencia como, antes da LGPD, tanto empresas públicas quanto privadas agiam de forma pouco transparente em relação ao uso dos dados pessoais dos clientes. Com a implementação da lei, práticas consideradas assédio moral passaram a ser rigorosamente penalizadas, forçando as organizações a se adequarem às novas exigências legais. Nesse contexto, o open finance no Brasil representa um avanço importante, mas para que esse modelo não se torne obsoleto, é fundamental que esteja em constante evolução, especialmente no que tange à adequação às normas da LGPD. Sobre o tema, Roger da Silva Nascimento (2024, p. 54) destaca:

> O Open Finance no Brasil tem se consolidado como uma das mais significativas inovações do mercado financeiro nacional, destacando o país como pioneiro na implementação desse modelo. No entanto, seu futuro será moldado por tendências tecnológicas, regulatórias e de mercado, bem como pela capacidade de integrar novas soluções que vão além do setor financeiro, como marketplaces financeiros e superapps. Essa evolução exigirá esforços conjuntos entre reguladores, instituições financeiras e outros agentes econômicos para criar um ecossistema verdadeiramente inclusivo e inovador.

Assim, *o open finance* tem se mostrado um modelo exitoso, mas para manter esse desempenho, as instituições devem se adaptar continuamente às demandas do mercado financeiro. Isso inclui integrar soluções tecnológicas seguras e econômicas, alinhadas à LGPD, além de acompanhar as tendências do setor para garantir inovação, competitividade e proteção aos usuários.

5 CONSIDERAÇÕES FINAIS

A LGPD foi um avanço no campo jurídico brasileiro, ampliando o escopo e a responsabilização em relação à proteção dos dados pessoais. Antes, o Marco Civil da Internet já estabelecia algumas diretrizes, porém sua abrangência e mecanismos de fiscalização eram limitados. Com o aumento dos escândalos internacionais envolvendo vazamento e uso indevido de dados, o Brasil sentiu a necessidade de se adequar a esse novo contexto global, impulsionando a criação de uma legislação mais robusta e eficaz.

A entrada em vigor da LGPD trouxe para as empresas públicas e privadas a obrigação de seguir princípios essenciais como boa-fé, finalidade, adequação, necessidade, transparência, segurança e responsabilização. O descumprimento dessas normas implica em penalidades severas, incluindo multas e bloqueios. Isso é fundamental porque, na era digital, os dados pessoais adquiriram valor econômico, funcionando como mercadoria, e demandam uma regulamentação rigorosa para garantir a proteção dos direitos dos titulares.

Para garantir a aplicação e fiscalização da LGPD, foi criada a ANPD, órgão responsável por supervisionar a conformidade das instituições com a lei, proteger segredos comerciais, elaborar diretrizes e promover o conhecimento público sobre direitos e deveres relacionados à proteção de dados. Essa atua como guardiã da privacidade, incentivando a transparência e a segurança no tratamento das informações pessoais.

A coleta e o uso de dados só podem ocorrer mediante o consentimento explícito do titular, que deve receber informações claras e acessíveis sobre como suas informações serão utilizadas. A transparência e a segurança são pilares que garantem a confiabilidade desse processo, protegendo os dados contra acessos não autorizados, vazamentos e incidentes que possam comprometer a integridade das informações. A prevenção, por sua vez, exige a adoção de medidas proativas para evitar danos decorrentes do tratamento inadequado.

Nesse cenário, as empresas são responsáveis pela coleta, pela segurança e armazenamento das informações, respondendo pelos prejuízos causados por falhas ou

vazamentos. Instituições financeiras, em especial, precisam implementar políticas rigorosas para garantir a rastreabilidade e proteção dos dados, minimizando vulnerabilidades e fortalecendo a cultura de segurança cibernética entre seus colaboradores.

O avanço tecnológico possibilitou a digitalização dos serviços financeiros, permitindo que o acesso a informações e operações seja realizado de forma rápida e simples, muitas vezes pelo smartphone. O *open finance* surge como evolução do *open banking*, amplia o compartilhamento de dados e promove integração entre produtos e serviços financeiros, sempre pautado pela personalização e conveniência para o consumidor.

O *open finance* tem como objetivos incentivar a inovação, aumentar a concorrência, promover a eficiência do sistema financeiro nacional e fomentar a cidadania financeira, ampliando a inclusão por meio do acesso facilitado a variedade de produtos e serviços, como investimentos, seguros e previdência. A transparência e a rastreabilidade no sistema geram confiança e estimulam a melhoria dos serviços oferecidos pelas instituições.

A regulamentação do *open finance* no Brasil é feita de forma conjunta pelo Banco Central e pela LGPD, exigindo que as instituições financeiras cumpram requisitos rigorosos para garantir a segurança e a privacidade dos dados dos clientes. Muitas instituições adotam programas de *compliance* para assegurar a conformidade com a legislação, reduzindo riscos e protegendo sua reputação no mercado.

Apesar dos desafios, como a necessidade de ampliar a adesão dos usuários, garantir a segurança dos dados e manter a confiabilidade dos sistemas, o *open finance* traz oportunidades relevantes, como a redução dos custos das transações e o aprimoramento dos serviços financeiros, com maior personalização e eficiência. Para que o modelo continue a avançar, é fundamental que esteja em constante evolução, acompanhando as mudanças tecnológicas e regulatórias, sobretudo em relação à LGPD.

O sucesso do *open finance* no Brasil está relacionado ao fortalecimento da proteção de dados pessoais e ao compromisso das instituições com a inovação responsável. Tanto o setor financeiro quanto a legislação precisam se adaptar para enfrentar os desafios emergentes, garantindo ambiente seguro, transparente e inclusivo para todos os usuários. Assim, a LGPD e o *open finance* caminham lado a lado na construção de um sistema financeiro moderno e confiável.

REFERÊNCIAS

ALMEIDA, S.C.D, SOARES, T. A, **Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital**, 2022, p. 14. Disponível em: https://doi.org/10.1590/1981-5344/25905. Acesso em: 13 mar.2025

BARROSO, L. C. **Open Banking: origens, experiências internacionais e a proposta brasileira**, 2020, Ano 5, nº 1. Disponível em: https://bnb.gov.br/s482-dspace/bitstream/123456789/880/1/2020_INET_01.pdf. Acesso em: 14 mar. 2025.

BIONI, B. R. De 2010 a 2018: **a discussão brasileira sobre uma lei geral de proteção de dados. Jota**, [S.1: s.n.], 02 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados. Acesso em: 18 mar. 2025.

BRASIL, **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, Acesso em: 09 mar. 2025.

BRASIL, **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 20 mar. 2025.

BRASIL, Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade 6.649/DF**. Direito Constitucional. Direitos Fundamentais à Privacidade e ao Livre Desenvolvimento da Personalidade. tratamento de dados pessoais pelo estado brasileiro. compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública Federal. ADI E ADPF [...]. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Relator: Min. Gilmar Mendes, Brasília, 15 de setembro de 2022. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768683585. Acesso em: 22 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF**:** Presidência da República, 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 mar. 2025.

BRASIL. **Banco Central do Brasil. Banco Central detalha prazos do Open Banking. Banco Central do Brasil**, 2021. Disponível em: https://www.bcb.gov.br/detalhenoticia/561/noticia. Acesso em: 11 mar. 2025.

BRASIL. **Banco Central do Brasil. Banco Central do Brasil. Diferenciais do modelo brasileiro. Banco Central do Brasil**, 2021, p. 6. Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/OD_IBRAC_Openbanking_22.6.pdf. Acesso em: 11 mar. 2025.

BRASIL. **Banco Central do Brasil. BC lança o Open Finance: uma evolução do Open Banking. Banco** Central do Brasil, 2022. Disponível em: https://www.bcb.gov.br/detalhenoticia/17648/nota. Acesso em: 11 mar. 2025.

BRASIL. Banco Central do Brasil. **O Open Finance é seguro? Banco Central do Brasil, 2023.** Disponível em: https://www.bcb.gov.br/meubc/faqs/p/o-open-finance-e-seguro. Acesso em: 11 mar. 2025.

BRASIL. **Banco Central do Brasil. O que é open banking? Banco Central do Brasil**, 2021, p. 3. Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/OD_IBRAC_Openbanking_22.6.pdf. Acesso em: 11 mar. 2025.

BRASIL. Banco Central do Brasil. **O que é o Sistema Financeiro Aberto (Open Finance)? Banco Central do Brasil**, 2023, p. 1. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/o-que-e-o-sistema-financeiro-aberto-open-finance. Acesso em: 11 mar. 2025.

BRASIL. Banco Central do Brasil. **Quais as funções das instituições participantes do Open Finance?** Banco Central do Brasil, 2023. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/quais-as-funcoes-das-instituicoes-participantes-do-open-finance. Acesso em: 11 mar. 2025.

BRASIL. Banco Central do Brasil. **Quais são os objetivos do Open Finance? Banco Central do Brasil**, 2023, p. 1. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/quais-sao-os-objetivos-do-open-finance. Acesso em: 11 mar. 2025.

BRASIL. Banco Central do Brasil. **O que é o Sistema Financeiro Aberto (Open Finance)? Banco Central do Brasil**, 2023, p. 1. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/o-que-e-o-sistema-financeiro-aberto-open-finance. Acesso em: 23 mar. 2025.

BRASIL. Banco Central do Brasil. **Resolução Conjunta nº 1, de 4 de maio de 2020.** Dispõe sobre a implementação do Sistema Financeiro Aberto (Open Banking). Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/51028/Res_Conj_0001_v4_L.pdf. Acesso em: 25 mar. 2025.

BRASIL. Banco Central do Brasil. **Resolução Conjunta nº 4.658, de 26 de abril de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados. Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em: 29 mar. 2025.

BRASIL. Banco Central do Brasil. **Resolução Conjunta nº 4, de 24 de março de 2022**. Altera a Resolução Conjunta nº 1, de 4 de maio de 2020, para dispor sobre o Open Finance. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=4. Acesso em: 29 abril. 2025.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 559, de 4 de dezembro de 2024**. Divulga a versão 7.0 do Manual de Experiência do Cliente no Open Finance. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=559. Acesso em: 9 abr. 2025.

CARVALHO, Flávia Rodrigues. **Open finance e a responsabilidade solidária em caso de vazamento de dados pessoais: uma breve análise da LGPD**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 09, Ed. 04, Vol. 01, pp. 112 123. Abril de 2024. ISSN: 2448-0959. Disponível em: https://www.nucleodoconhecimento.com.br/lei/open-finance, 10.32749/nucleodoconhecimento.com.br/lei/open-finance. Acesso em: 21 mar. 2025.

CAMARGO, Guilherme Ramon Santos. **Tendências e desafios do open finance: uma análise do impacto nas instituições financeiras**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Ciências Atuariais) - Universidade Federal de São Paulo, Escola Paulista de Política, Economia e Negócios, Osasco, 2023. Disponível em: https://repositorio.unifesp.br/server/api/core/bitstreams/1ba8845d-aa20-41e5-ab3d-8ea5c59a523d/content.Acesso em: 17 mar. 2025.

DANIEL, M. A. **A evolução e aplicação da segurança da informação por meio da Lei Geral de Proteção de Dados Pessoais (LGPD): um estudo de caso em uma instituição financeira.** 2022, 63 p, Trabalho de conclusão de curso, (Bacharel em Tecnologias da Informação e Comunicação) - Universidade Federal de Santa Catarina Campus Araranguá, Araranguá/SC, 11 de mar. de 2025. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/233375/TCC%20MAYCON.pdf?sequence=1&isAllowed=y. Acesso em: 11 mar. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 44.

FEBRABAN. **Guia boas práticas de compliance**. 2018, ed. revista e atualizada. Disponível em:https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/febraban_manual_compliance_2018_2web.pdf. Acesso em: 9 mai. 2025.

FINKELSTEIN, Maria Eugenia. FINKELSTEIN, Claudio. **Privacidade e Lei Geral de Proteção de Dados Pessoais**. In: Revista de Direito Brasileira, Florianópolis, v. 23, n. 9, p. 284-301, mai./ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 20 mai. 2025.

GOETTENAUER, C. **O Sistema Financeiro Brasileiro, Política de Segurança Cibernética e Proteção de Dados Pessoais: uma Abordagem sob a Ótica da Regulação Policêntrica**. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, nº 2, p. 172-186, outubro de 2020. Disponível em: https://core.ac.uk/download/pdf/337598123.pdf. Acesso em: 11 mar. 2025.

JARUDE, J; SILVEIRA, D. **O sistema financeiro aberto (open banking) sob a perspectiva da regulação bancária e da Lei Geral de Proteção de Dados (LGPD).** Revista Jurídica da FA7, [S. l.], v. 18, n. 2, p. 77–90, 2021. DOI: 10.24067/rjfa7;18.2:1245. Disponível em: https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1245. Acesso em: 11 mar. 2025.

MALTA, Daniele de Andrade. **A regulação do open finance e sua interseção com a proteção de dados pessoais** / Daniele de Andrade Malta. – 2023. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/5b167940-0c29-4780-875d-c566be982d8a/content. Acesso em: 15 mar.2025.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros. **Comentários à Lei Geral de Proteção de Dados Pessoais: Lei 13.709/2018**. Editora Foco, 2022. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=P1lcEAAAQBAJ&oi=fnd&pg=PA22&dq=(MARTINS%3B+LONGHI%3B+J%C3%9ANIOR,+2022&ots=-SmHwYTKCB&sig=zGQ_FszmMWhJJ_Bqk-z0LODCS8M#v=onepage&q=(MARTINS%3B%20LONGHI%3B%20J%C3%9ANIOR%2C%202022&f=false. Acesso em: 15 mar. 2025.

MELO, Eduardo Alverne. **Implatação do Open Finance no Brasil: desafios e efeitos potenciais**. / Eduardo Alverne Melo-2023. Disponível em: https://repositorio.ufc.br/bitstream/riufc/71356/2/2023_dis_eamelo.pdf. Acesso em: em: 11 mar. 2025.

NAKAMURA, E; T. **Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil. 1. ed. Rio de Janeiro: Instituto de Pesquisa Econômica Aplicada (Ipea),** 2024. 307 p. Disponível em: https://repositorio.ipea.gov.br/handle/11058/13148. Acesso em: 11 mar. 2025.

NASCIMENTO, Roger da Silva do. **O impacto do open finance no mercado financeiro brasileiro de 2021 a 2023,** (2024), 62 f, p. 54. Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Ciências Econômicas, Porto Alegre, BR-RS, 2024. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/284219/001240989.pdf?sequence=1&isAllowed=y. Acesso em: 12 mai.2025.

OLIVEIRA, Ana Luiza Silva et al. Lei geral de proteção de dados pessoais. **Revista Projetos Extensionistas**, v. 1, n. 2, p. 26-33, 2021.Disponível em: https://periodicos.fapam.edu.br/index.php/RPE/article/view/381. Acesso em: 11 mai. 2025.

PALHARES, Felipe. As falácias do amanhã: A saga da entrada em vigor da LGPD. In: PALHARES, Felipe (Coord.). Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil, 2020, p. 529.

PEIRANO, Marta. **El enemigo conoce el sistema: manipulación de datos, personas y influencias después de la Economia de la atención.** Barcelona: Penguin Random House, 2019. p. 16 (e-book). Disponível em: https://www.amazon.com.br/enemigo-conoce-sistema-Manipulaci%C3%B3n-influencias-ebook/dp/B07QMB2W7G. Acesso em: 11 abr. 2025.

SANTOS FILHO, L. A. R. dos. **A resolução 4.658/18: política de segurança cibernética no Brasil**. Revista Direito, Economia e Globalização, [S. l.], v. 1, n. 2, p. 1–12, 2021. Disponível em: https://revistadedireito.catolicasc.org.br/index.php/revistadedireito/article/view/10. Acesso em: 12 mai. 2025.

SUSSKIND, R. **LGPD no Setor Financeiro: Desafios e Obrigações,** 2024, p. 2. Disponível em: https://dpoexpert.com.br/lgpd-setor-financeiro-desafios-e-conformidade/. Acesso em: 11 de mar.2025.

[s. n.]. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades.** Globo, [S.1: s.n.], 20 mar. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-

dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 16 mar. 2025

TARGHER, Roberto Magri. Open finance no Brasil: levantamento de desafios e lições aprendidas / Roberto Magri Targher. - 2023. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/0b51cf70-3070-4d9b-9fda-8e4884db71d8/content. Acesso em: 09 de mar.2025.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo.** Salvador: Editora JusPodivm, 2019.