UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE ADMINISTRAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO – PPA

DIÉLEN CARON

CAPITALISMO DE VIGILÂNCIA DIGITAL NO SISTEMA FINANCEIRO NACIONAL: UMA ANÁLISE DA ADEQUAÇÃO E IMPACTO DAS MEDIDAS DE PROTEÇÃO DE DADOS DO BANCO CENTRAL DO BRASIL PARA A SEGURANÇA DIGITAL NO SETOR DO VAREJO FINANCEIRO BRASILEIRO

Dissertação

Apoio: CAPES

Maringá
2025

DIÉLEN CARON

CAPITALISMO DE VIGILÂNCIA DIGITAL NO SISTEMA FINANCEIRO NACIONAL: UMA ANÁLISE DA ADEQUAÇÃO E IMPACTO DAS MEDIDAS DE PROTEÇÃO DE DADOS DO BANCO CENTRAL DO BRASIL PARA A SEGURANÇA DIGITAL NO SETOR DO VAREJO FINANCEIRO BRASILEIRO

Dissertação apresentada ao Programa de Pós graduação em Administração da Universidade Estadual de Maringá (PPA-UEM) como requisito parcial para obtenção do título de mestre em Administração.

Orientadora: Dra. Josiane Silva de Oliveira

Apoio: CAPES

ODSs contemplados: 10, 12, 16

Maringá

2025

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Central - UEM, Maringá - PR, Brasil)

C293c

Caron, Diélen

Capitalismo de vigilância digital no sistema financeiro nacional : uma análise da adequação e impacto das medidas de proteção de dados do Banco Central do Brasil para a segurança digital no setor do varejo financeiro brasileiro / Diélen Caron. -- Maringá, PR, 2025.

204 f. : il. color., tabs.

Orientadora: Profa. Dra. Josiane Silva de Oliveira.

Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Sociais Aplicadas, Departamento de Administração, Programa de Pós-Graduação em Administração, 2025.

1. Sistema de varejo financeiro - Brasil. 2. Proteção de dados . 3. Banco Central do Brasil. 4. Segurança digital. I. Oliveira, Josiane Silva de, orient. II. Universidade Estadual de Maringá. Centro de Ciências Sociais Aplicadas. Departamento de Administração. Programa de Pós-Graduação em Administração. III. Título.

CDD 23.ed. 658.15

Síntique Raquel de C. Eleutério - CRB 9/1641

UNIVERSIDADE ESTADUAL DE MARINGÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
Av. Colombo, 5790 - Zona 07 - 87020-900 - Maringá - PR
Homepage: www.ppa.uem.br
Facebook: https://www.facebook.com/posgraduacaoadministracaouem/?modal=admin_todo_tour
LinkedIn: https://www.linkedin.com/in/ppa-uem-b1291731/
Contatos: (44) 3011-5949 - E-mail: sec-ppa@uem.br

ATA DE DEFESA PÚBLICA

Aos **dezesseis** dias do mês de **dezembro** do ano de **dois mil e vinte e cinco**, às **nove horas**, realizou-se, presencialmente e por videoconferência com o convidado externo, em conformidade com o Ato Executivo 004/2020-GRE e a Res. 003/2020-CEP, apresentação do Trabalho de Conclusão, sob o título: **"Capitalismo de vigilância digital no sistema financeiro nacional: uma análise da adequação e impacto das medidas de proteção de dados do Banco Central Brasil para a segurança digital no setor do varejo financeiro brasileiro"**, de autoria de **DIÉLEN CARON**, aluna(o) do Programa de Pós-Graduação em Administração (Mestrado) – Área de Concentração: Organizações e Mercado. A Banca Examinadora esteve constituída pelos docentes: Drª Josiane Silva de Oliveira (presidente); Drª Ianaira Barreto Souza Neves (membra examinadora externa – EAESP/FGV); e Drª Priscilla Borgonhoni Chagas (membra examinadora do PPA).

Concluídos os trabalhos de apresentação e arguição, a banca examinadora faz constar a(o) candidata(o) a condição de: ☒ **Aprovada(o);** ☐ **Aprovada(o) com correções;** ☐ **Reprovada(o)** pela Banca Examinadora. E, para constar, foi lavrada a presente Ata, que vai assinada pelo coordenador e pelos membros da Banca Examinadora.

OBS: Esta ata não vale como certificado de conclusão do curso de pós-graduação em Administração. A obtenção da titulação de mestre em Administração está condicionada ao depósito da versão definitiva em PDF e não editável, com todas as correções feitas e atestadas pelo orientador, com a ficha catalográfica da BCE/UEM, no prazo máximo estabelecido no regimento do Programa, de acordo com a condição de aprovação.

EM TEMPO: Houve alteração no título da dissertação? Se sim, descrever aqui: CAPITALISMO DE VIGILÂNCIA DIGITAL NO SISTEMA FINANCEIRO NACIONAL: UMA ANÁLISE DA ADEQUAÇÃO E IMPACTO DAS MEDIDAS DE PROTEÇÃO DE DADOS DO BANCO CENTRAL DO BRASIL PARA A SEGURANÇA DIGITAL NO SETOR DO VAREJO FINANCEIRO BRASILEIRO

OBS: Em caso de "REFORMULAÇÃO DO TRABALHO", haverá necessidade de nova defesa pública?
☐ SIM; ☐ NÃO

Maringá, **16** de **dezembro** de **2025.**

Drª Josiane Silva de Oliveira
(Presidente)

gov.br Documento assinado digitalmente
IANAIRA BARRETTO SOUZA NEVES
Data: 16/12/2025 13:13:23-0300
Verifique em https://validar.iti.gov.br

Drª Ianaira Barreto Souza Neves
(membra examinadora externa – EAESP/FGV)

Drª Priscilla Borgonhoni Chagas
(membra examinadora do PPA)

Dr. José Paulo de Souza
(coordenador do PPA)

AGRADECIMENTOS

Expresso aqui meus agradecimentos a todos que estiveram presentes e me apoiaram de alguma forma ao longo desse período de pós graduação e que contribuíram e torceram para que este estudo chegasse a termo.

À Universidade Estadual de Maringá (UEM), pelo ensino público, gratuito e de qualidade, e pela oportunidade de aprimoramento acadêmico. À CAPES, pelo apoio por meio das bolsas de pesquisa, que possibilitaram a dedicação integral a esta jornada.

Aos professores e professoras do Programa de Pós-Graduação em Administração (PPA), pelos ensinamentos compartilhados, pelas experiências proporcionadas e por serem fonte de inspiração. Em especial, agradeço à minha orientadora, pela paciência e compreensão, pelo apoio e incentivo constante, pela amizade e pelo exemplo inspirador de profissional e de pessoa cuja postura admiro profundamente. Às professoras da banca de qualificação e de defesa, agradeço por aceitarem contribuir com este trabalho e pelas valiosas sugestões.

Também aos colegas e amigos que conheci no PPA, da qual carrego comigo as melhores lembranças. Obrigada pela parceria.

A todos os amigos, próximos e distantes, pelo suporte ao longo desse período.

À minha família, por tudo, amo vocês.

A todos, agradeço imensamente.

"A liberdade começa quando conseguimos decidir o que é nosso e o que entregamos ao mundo."
(Shoshana Zuboff)

RESUMO

Este estudo teve como objetivo compreender como as medidas de proteção de dados do Banco Central do Brasil (BC) buscam mitigar os riscos de segurança digital no setor de varejo financeiro brasileiro. O estudo foi desenvolvido a partir de uma perspectiva crítica amparada pela teoria do capitalismo de vigilância e as diretrizes de regulamentação sobre proteção de dados instituídas pelas legislações brasileiras desde a Constituição Federal de 1988. Justifica-se tal opção pelas relações entre o chamado capitalismo de vigilância (Zuboff, 2020) e a necessidade de criação de políticas de proteção de dados e segurança digital nas nações, nesse caso especificamente no que se refere ao Sistema Financeiro Nacional (SFN), precisamente no sistema de varejo financeiro, na qual protege os consumidores residentes no Brasil. A pesquisa qualitativa foi realizada por meio do método de pesquisa documental na qual foram analisados os conteúdos das legislações sobre proteção de dados no Brasil em articulação com as políticas de proteção de dados e segurança digital instituídas pelo Banco Central do Brasil, como órgão que regulamenta o sistema de varejo financeiro nacional. Os achados indicam que, embora o arcabouço regulatório brasileiro e as medidas do Banco Central do Brasil promovam proteção formal e operacional, garantindo princípios de confidencialidade, integridade e disponibilidade, ainda existem desafios quanto à efetividade prática, à supervisão de serviços terceirizados e à visibilidade do fluxo de dados para os titulares. A análise evidenciou cinco categorias centrais de atuação: gestão de dados pessoais, segurança digital e resiliência de sistemas, planos de continuidade de negócios, supervisão interna e reporte de incidentes de segurança, e gestão de riscos de terceiros. A pesquisa conclui que as medidas do Banco Central do Brasil contribuem significativamente para a segurança digital no varejo financeiro, mas que avanços são necessários para consolidar a soberania digital e reduzir os riscos associados às práticas do capitalismo de vigilância. Este estudo reforça que a soberania digital não se esgota na letra da lei, mas se realiza na capacidade de proteger dados, pessoas e instituições em um ambiente cada vez mais mediado por algoritmos e vulnerável a formas sofisticadas de exploração informacional. Numa era marcada por riscos cibernéticos globais e pela lógica do capitalismo de vigilância, garantir a integridade dos sistemas financeiros e a privacidade dos cidadãos não é apenas uma demanda técnica, mas um imperativo democrático, que exige ação efetiva além das normas formais. Por fim, o estudo ainda evidenciou que os efeitos da exploração de dados pessoais no Brasil refletem uma realidade tipicamente nacional, distinta das experiências regulatórias observadas no cenário internacional.

Palavras Chave: Capitalismo de Vigilância. Proteção de Dados. Segurança Digital. Sistema Financeiro Brasileiro. Análise documental.

ABSTRACT

This study aimed to understand how the data protection measures of the Central Bank of Brazil (BC) seek to mitigate digital security risks in the Brazilian financial retail sector. The study was developed from a critical perspective grounded in surveillance capitalism theory and the data protection regulatory guidelines established by Brazilian legislation since the 1988 Federal Constitution. This approach is justified by the relationship between the so-called surveillance capitalism (Zuboff, 2020) and the need to create data protection and digital security policies in nations, specifically regarding the National Financial System (SFN), particularly in the financial retail system, which protects consumers residing in Brazil. The qualitative research was conducted using a documentary research method, in which the contents of Brazilian data protection legislation were analyzed in conjunction with the data protection and digital security policies established by the Central Bank of Brazil, as the regulatory authority of the national financial retail system. The findings indicate that, although the Brazilian regulatory framework and the Central Bank's measures promote formal and operational protection, ensuring principles of confidentiality, integrity, and availability, there are still challenges regarding practical effectiveness, oversight of outsourced services, and visibility of data flows to data subjects. The analysis identified five central areas of action: personal data management, digital security and system resilience, business continuity planning, internal supervision and security incident reporting, and third-party risk management. The research concludes that the Central Bank of Brazil's measures contribute significantly to digital security in financial retail, but further advances are necessary to consolidate digital sovereignty and reduce the risks associated with surveillance capitalism practices. This study reinforces that digital sovereignty is not exhausted by the letter of the law but is realized in the capacity to protect data, people, and institutions in an environment increasingly mediated by algorithms and vulnerable to sophisticated forms of informational exploitation. In an era marked by global cyber risks and the logic of surveillance capitalism, ensuring the integrity of financial systems and the privacy of citizens is not merely a technical demand but a democratic imperative, requiring effective action beyond formal regulations. Finally, the study also evidenced that the effects of personal data exploitation in Brazil reflect a typically national reality, distinct from the regulatory experiences observed internationally.

Keywords: Surveillance Capitalism. Data Protection. Digital Security. Brazilian Financial System. Documentary Analysis.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
APIs	Interface de Programação de Aplicações
AWS	Amazon Web Services
BC	Banco Central do Brasil
BIS	Banco de Compensações Internacionais
CCPA	Lei de Privacidade do Consumidor da Califórnia
CGU	Controladoria-Geral da União
CMN	Conselho Monetário Nacional
CNDL	Confederação Nacional de Dirigentes Lojistas
CNPC	Conselho Nacional de Previdência Complementar
CNSP	Conselho Nacional de Seguros Privados
CVM	Comissão de Valores Mobiliários
Comef	Comitê de Estabilidade Financeira
Copom	Comitê de Política Monetária
CRSFN	Conselho de Recursos do Sistema Financeiro Nacional
Deati	Departamento de Atendimento ao Cidadão
Decem	Departamento de Competição e de Estrutura do Mercado Financeiro
Degef	Departamento de Gestão Estratégica e Supervisão Especializada
Deinf	Departamento de Tecnologia da Informação
Denor	Departamento de Regulação do Sistema Financeiro
Deorf	Departamento de Organização do Sistema Financeiro
Deris	Departamento de Riscos Corporativos e Referências Operacionais
Dinor	Diretor de Regulação
Dirad	Diretor de Administração
Direx	Diretor de Assuntos Internacionais e de Gestão de Riscos Corporativos
DoS	Ataque de Negação de Serviço
DDoS	Distributed Denial of Service
DNS	Sistema de Nomes de Domínio
E-CIBER	Estratégia Nacional de Cibersegurança do Brasil
ENSC	Estratégia Nacional de Segurança Cibernética
FEBRABAN	Federação Brasileira de Bancos

FMI	Fundo Monetário Internacional
FSB	Conselho de Estabilidade Financeira
GAFI	Grupo de Ação Financeira
GDPR	Regulamento Geral de Proteção de Dados
GRC	Comitê de Governança, Riscos e Controles
IDS	Sistema de Detecção de Intrusão
IPS	Sistema de Prevenção de Intrusão
IoT	Internet das Coisas
LGPD	Lei Geral de Proteção de Dados Pessoais
MPF	Ministério Público Federal
NSA	Agência de Segurança Nacional
PIPEDA	Lei de Proteção de Informações Pessoais e Documentos Eletrônicos
Presi	Presidente
PREVIC	Superintendência Nacional de Previdência Complementar
Secre	Secretaria-Executiva
SFN	Sistema Financeiro Nacional
SISBACEN	Sistema de Informações Banco Central
SUMOC	Superintendência da Moeda e do Crédito
SUSEP	Superintendência de Seguros Privados
TCU	Tribunal de Contas da União

SUMÁRIO

1. INTRODUÇÃO

A globalização tecnológica ampliou significativamente sua presença na vida cotidiana, estabelecendo-se como o principal sistema de comunicação global, tanto em termos quantitativos quanto qualitativos (Santos, 2003). Esse desenvolvimento permite comunicação instantânea e acesso a informações em todo o mundo. No entanto, esse progresso também criou um novo cenário para a prática de delitos, dando origem a uma nova categoria de crimes cibernéticos que evidencia o paradoxo de um espaço simultaneamente livre e instável (Castells, 2013; 2014).

Os mecanismos de acesso à internet, que podem superar barreiras geográficas e políticas, impõe desafios ao controle regulatório, transformando-a em um território vasto e frequentemente fora da alçada da legislação, caracterizado pelo anonimato e pela ilegalidade, ao mesmo tempo em que serve como um meio democrático de interação social acessível (Mendes, Alves, Doneda, 2020). É fundamental, entretanto, reconhecer que essa democratização não deve comprometer a segurança jurídica ou a proteção dos direitos fundamentais. Assim, a busca por soluções jurídicas deve dialogar com a complexidade da era digital, respeitando suas particularidades sem abrir mão dos princípios que fundamentam a convivência em sociedade (Beli, Ramos, 2021).

A proteção de dados pessoais tem se tornado um tema central nos processos empresariais e nas normativas governamentais, em virtude da necessidade de resguardar informações sensíveis de indivíduos, organizações e empresas, que continuam expostas a riscos como vazamentos, furtos e usos indevidos, especialmente no âmbito do setor financeiro (Ferreira, Campos, 2020) Nesse contexto, destaca-se a necessidade de um esforço crescente por parte de instituições bancárias, financeiras e fintechs para adequar-se às exigências regulatórias e garantir a segurança dos dados pessoais. Tais transformações são amplificadas pela digitalização, pela convergência setorial e pela difusão dos ecossistemas digitais, os quais promovem a rápida circulação de informações.

O compartilhamento de informações pessoais durante uma transação comercial tornou-se comum para a maioria das instituições financeiras. Essa atividade pode ser a causa da disseminação de mais do que dados bancários, como números de contas ou números de cartões de crédito, e da troca de informações pessoais, como nomes, documentos, e-mails, entre outros. Nesse sentido, as organizações tiveram que adotar novas medidas de proteção de dados, com a implementação de medidas e práticas destinadas a proteger as informações pessoais e financeiras de seus clientes. Isso inclui informações como nomes, endereços,

números de documentos, histórico de crédito e outros dados confidenciais que podem ser usados para identificar um indivíduo ou sua situação financeira (Gonçalves, 2023).

Essas transformações operam em um contexto caracterizado pela pensadora estadunidense Shoshana Zuboff como “Capitalismo de vigilância". Em seu livro "A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Nova Fronteira do Poder", Zuboff (2020) argumenta que o capitalismo de vigilância se refere a um novo paradigma econômico onde as empresas de tecnologia coletam e analisam grandes quantidades de dados pessoais para prever e influenciar comportamentos, maximizando seus lucros através da manipulação de informações. Isso implica um controle cada vez maior sobre a vida privada dos indivíduos, uma vez que essas empresas acumulam e utilizam dados de maneira extensiva e muitas vezes opaca (Zuboff, 2020).

O compartilhamento de informações pessoais durante transações comerciais, comum entre instituições financeiras, se insere no contexto mais amplo do capitalismo de vigilância, onde a coleta e análise de dados pessoais não se restringem apenas a proteger a privacidade dos indivíduos, mas também a otimizar estratégias de mercado (Zuboff, 2015; 2020). Nesse cenário, a troca de dados como nomes, endereços e históricos financeiros não é apenas uma questão de segurança, mas uma prática que potencializa a criação de perfis detalhados dos consumidores. Essa abordagem permite que as organizações monitorem comportamentos, prevejam necessidades e personalizem ofertas, gerando lucros a partir da exploração das informações (Zuboff, 2015; 2020).

Assim, as medidas de proteção de dados tornam-se não só uma responsabilidade ética, mas também uma exigência para manter a confiança do consumidor em um ambiente onde a vigilância constante se torna a norma. Ainda conforme contextualizado pela autora, o desafio é equilibrar a necessidade de inovação e eficiência comercial com a proteção da privacidade individual, em um sistema onde os dados se tornaram a moeda mais valiosa (Zuboff, 2015; 2020).

No contexto brasileiro, a regulamentação do ambiente digital foi incorporada de forma gradual e, inicialmente, de maneira indireta no ordenamento jurídico (Fereira, Campos, 2020). Esse processo culminou, com o passar dos anos, na formulação de normas específicas que tratam diretamente das particularidades do meio digital, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD), além da posterior criação da Autoridade Nacional de Proteção de Dados (ANPD). Tal evolução normativa reflete não apenas o reconhecimento da relevância social, econômica e jurídica da internet e do tratamento de

dados pessoais, mas também a necessidade de adequação do país aos desafios impostos pela digitalização.

Grande parte dessas medidas regulatórias foi inspirada e fundamentada em legislações e tratados internacionais que estabeleceram parâmetros para a proteção de direitos e a segurança no ambiente digital. Nesse sentido, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia exerceu papel decisivo como referência para a elaboração da LGPD, influenciando significativamente os princípios e obrigações previstos na legislação brasileira. Paralelamente, a adesão do Brasil à Convenção de Budapeste sobre o cibercrime marca um compromisso com padrões internacionais de cooperação e segurança digital, estabelecendo diretrizes para o enfrentamento dos crimes cibernéticos e a proteção do espaço digital no país.

O surgimento desses marcos regulatórios no Brasil pode ser compreendido como uma reação ao avanço de estruturas sistêmicas de exploração informacional que caracterizam o atual estágio do capitalismo, descrito por Zuboff (2020). Esses dispositivos normativos emergem num contexto em que a coleta massiva de dados e sua utilização comercial — sobretudo por grandes plataformas digitais — tornam-se práticas centralizadas na lógica de controle e previsibilidade comportamental.

A adoção dessas legislações não foi motivada apenas por preocupações internas com privacidade e segurança, mas também pela pressão internacional por alinhamento normativo, especialmente com o GDPR europeu, e pela crescente visibilidade dos impactos sociais, políticos e econômicos gerados por modelos econômicos fundados na vigilância. Tais normativas se constituem dentro de um campo de tensões: ao mesmo tempo em que visam proteger direitos fundamentais, também operam dentro das margens permitidas por uma economia orientada à exploração contínua de dados como ativo estratégico. Nesse sentido, o aparato jurídico nacional voltado à regulação do digital insere-se como tentativa de mitigação dos efeitos mais danosos desse modelo, buscando estabelecer limites mínimos às práticas de coleta, armazenamento e tratamento de dados pessoais.

Nesse contexto de crescente institucionalização de legislações voltadas à proteção de dados pessoais no Brasil — impulsionadas pelas dinâmicas do capitalismo de vigilância —, torna-se particularmente evidente a vulnerabilidade de setores estratégicos como o financeiro. A centralidade que os dados adquiriram nas operações bancárias, tanto para fins de personalização de serviços quanto para análise de risco e gestão automatizada de decisões, coloca as instituições financeiras brasileiras em uma posição delicada: ao mesmo tempo em

que se beneficiam economicamente do tratamento intensivo de informações, tornam-se alvos prioritários de crimes cibernéticos, fraudes e vazamentos em larga escala.

O aumento expressivo dos golpes e fraudes financeiras no Brasil nas últimas décadas revela uma faceta crítica da digitalização dos serviços bancários e da fragilidade dos mecanismos de proteção informacional. De acordo com dados da Serasa Experian (2025), somente em fevereiro deste ano foram registradas mais de 1,1 milhão de tentativas de fraude, o que equivale a uma ocorrência a cada 2,2 segundos. O setor de "Bancos e Cartões" concentrou mais da metade dessas tentativas (54,2%), seguido pelos segmentos de "Serviços" (30,9%) e "Financeiras" (7,2%), indicando que as instituições financeiras permanecem entre os principais alvos de atividades fraudulentas.

Essa tendência é confirmada por levantamento conduzido pelo Fórum Brasileiro de Segurança Pública, em parceria com o Instituto Datafolha, o qual aponta que aproximadamente 56 milhões de brasileiros — cerca de um terço da população adulta — foram vítimas de golpes financeiros virtuais com prejuízo direto no período de 12 meses anteriores a julho de 2024. O montante estimado de perdas ultrapassa R$111,9 bilhões, evidenciando não apenas a extensão do problema, mas também o impacto econômico significativo dessas práticas ilícitas para indivíduos e para o sistema financeiro como um todo.

No primeiro semestre de 2025, o país registrou mais de 6,4 milhões de tentativas de fraude, com perdas potenciais estimadas em R$39,8 bilhões, caso essas ações tivessem sido bem-sucedidas (SERASA EXPERIAN, 2025). Projeções ainda mais alarmantes são apresentadas pelo relatório Scamscope (2024), que estima que, apenas no âmbito das fraudes realizadas via pagamentos instantâneos — como o sistema Pix —, as perdas podem atingir a marca de R$ 11 bilhões até 2028, caso não sejam adotadas medidas de contenção eficazes. Esses dados apontam para uma crescente sofisticação dos mecanismos de fraude e para a necessidade de fortalecimento das políticas de segurança digital no setor financeiro brasileiro.

A adoção de práticas de segurança digital, portanto, surge não apenas como uma medida técnica, mas como uma resposta estrutural à crescente exposição de dados no mercado financeiro, fortemente impactado pela digitalização dos serviços e pela intensificação das operações online.

No Brasil, a instituição responsável pela supervisão das atividades nas instituições financeiras é o Banco Central do Brasil (BC), cuja atuação tem se tornado progressivamente mais complexa diante das novas exigências regulatórias e dos riscos associados à inovação tecnológica. O BC desempenha papel central na normatização das transações financeiras,

buscando garantir a estabilidade, a eficiência e a segurança do Sistema Financeiro Nacional (SFN).

Dentro da estrutura do SFN destaca-se o Sistema de Varejo Financeiro, responsável por intermediar as relações entre as instituições financeiras e os clientes de perfil individual, especialmente pessoas físicas e micro e pequenas empresas. Esse subsistema tem como finalidade principal oferecer produtos e serviços de uso cotidiano, como contas correntes, cartões, operações de crédito, investimentos e meios de pagamento, viabilizando o acesso da população ao mercado financeiro. Reguladas e supervisionadas pelo BC, as instituições que compõem o sistema de varejo — como bancos comerciais, cooperativas de crédito e fintechs — desempenham papel fundamental na inclusão financeira e na circulação de recursos na economia, contribuindo diretamente para o desenvolvimento econômico e social do país (BANCO CENTRAL DO BRASIL, 2021; Lima, 2009).

A crescente digitalização dos serviços financeiros e a intensificação dos riscos associados à segurança da informação impõem ao BC responsabilidades que vão além da regulação tradicional das atividades econômicas. Como principal autoridade monetária e reguladora do SFN, o BC deve assumir um papel incisivo na formulação de diretrizes específicas voltadas à proteção de dados, à cibersegurança e à prevenção de fraudes digitais. Isso implica, entre outras medidas, a necessidade de estabelecer normas claras, atualizadas e tecnicamente fundamentadas que obriguem as instituições financeiras a adotarem políticas robustas de governança de dados, gestão de riscos cibernéticos e resposta a incidentes.

A luz deste contexto, emerge o seguinte problema de pesquisa: **Como as medidas de proteção de dados do Banco Central do Brasil (BC) buscam mitigar os riscos de segurança digital no setor do varejo financeiro brasileiro?**

A justificativa para a realização deste estudo na área de Administração, especificamente no campo dos Estudos Organizacionais, fundamenta-se em diversos aspectos cruciais para a gestão contemporânea, especialmente no contexto do setor de varejo financeiro brasileiro. A transformação digital tem promovido mudanças profundas nas operações, estruturas e estratégias organizacionais, fazendo com que a proteção de dados e a segurança da informação assumam papel central na gestão. Nesse cenário, as regulamentações desenvolvidas no Brasil e reguladas pelo Banco Central (BC) oferecem um referencial normativo que orienta as organizações do setor financeiro na elaboração de políticas de segurança digital, supostamente alinhadas às melhores práticas globais.

No entanto, embora tais marcos regulatórios sejam amplamente difundidos, ainda há uma lacuna importante na literatura sobre como essas normas são efetivamente interpretadas,

traduzidas e incorporadas às práticas organizacionais cotidianas, especialmente em organizações de diferentes portes e capacidades estruturais. Assim, este estudo se justifica por buscar compreender, sob uma perspectiva organizacional e crítica, em que medida as regulamentações brasileiras de segurança digital se materializam em práticas concretas ou permanecem restritas a um cumprimento formal e burocrático. Ao fazer isso, a pesquisa contribui para os Estudos Organizacionais ao deslocar o foco de análises predominantemente normativas ou tecnicistas para uma abordagem sociotécnica, que considera as dinâmicas de poder, controle e racionalidade gerencial envolvidas na implementação dessas políticas.

Nos últimos anos, as práticas de vigilância também passaram por transformações significativas, assim como as questões que motivam a pesquisa sobre esses temas. De maneira semelhante ao que ocorreu na transição para o século XXI, quando a crítica à centralidade do modelo panóptico (Foucault, 2014) ganhou destaque, novos arranjos sociotécnicos, econômicos e geopolíticos têm alterado o foco e o interesse dos pesquisadores. Esses movimentos impulsionam a emergência de novas reflexões teóricas, especialmente em torno do uso de algoritmos, da expansão do capitalismo de vigilância, dos efeitos preditivos sobre o comportamento de indivíduos e populações e das formas contemporâneas de resistência e contestação às assimetrias de poder. Nesse contexto, o setor financeiro se apresenta como um campo empírico particularmente relevante, ainda pouco explorado sob a ótica crítica dos Estudos Organizacionais.

A realização deste estudo, portanto, se justifica pela possibilidade de analisar criticamente se as propostas regulatórias e as políticas organizacionais de segurança digital realmente se traduzem em práticas efetivas de proteção de dados ou se operam majoritariamente como mecanismos formais de conformidade. Muitas organizações adotam abordagens baseadas em “checklists”, implementando políticas superficiais apenas para atender às exigências legais, sem internalizar uma cultura organizacional de segurança (Schneier, 2015). Ao investigar essa dinâmica, o estudo contribui para o debate teórico sobre o descompasso entre discurso institucional e prática organizacional, aprofundando a compreensão sobre os limites da regulação como indutora de mudanças organizacionais substantivas.

Além disso, a pesquisa se justifica ao reconhecer que a implementação dos marcos regulatórios de segurança digital pode gerar impactos assimétricos entre as organizações. Empresas de grande porte tendem a dispor de mais recursos técnicos, financeiros e humanos para atender às exigências regulatórias, enquanto pequenas e médias organizações enfrentam maiores dificuldades para se adequar a normas complexas. A análise dessas assimetrias

contribui empiricamente para os Estudos Organizacionais ao evidenciar como regulamentações aparentemente neutras podem reforçar desigualdades organizacionais, favorecendo determinados atores em detrimento de outros.

Outro aspecto relevante que fundamenta a realização deste estudo diz respeito ao papel da vigilância e do monitoramento intensificados pela adoção de medidas rigorosas de segurança digital. Uma abordagem crítica permite questionar até que ponto essas práticas impactam a privacidade dos consumidores e a autonomia dos trabalhadores dentro das organizações. Ao problematizar o equilíbrio entre segurança e privacidade, o estudo contribui para ampliar o debate sobre os efeitos organizacionais, sociais e éticos da governança digital, reforçando que a proteção de dados não deve ocorrer à custa de direitos fundamentais.

Por fim, ao adotar uma perspectiva crítica, este estudo se justifica por contribuir para um debate mais amplo sobre governança digital, responsabilidade organizacional e ética no uso de tecnologias de vigilância. Do ponto de vista acadêmico, a pesquisa busca avançar no campo da Administração e dos Estudos Organizacionais ao articular segurança digital, regulamentações brasileiras e práticas organizacionais em um setor estratégico da economia. Do ponto de vista prático e institucional, o estudo oferece subsídios para gestores e formuladores de políticas públicas, ao fornecer evidências empíricas sobre os desafios da conformidade regulatória e sobre a eficácia das políticas de segurança digital. Dessa forma, a pesquisa contribui para a construção de práticas organizacionais mais conscientes, sustentáveis e alinhadas a uma governança digital que considere simultaneamente segurança, privacidade e viabilidade organizacional.

2. OBJETIVOS

A partir da problematização e a contextualização da temática abordada na seção introdutória, os objetivos propostos para este estudo são:

2.1 OBJETIVO GERAL

Compreender como as medidas de proteção de dados do Banco Central do Brasil buscam mitigar os riscos de segurança digital no setor do varejo financeiro brasileiro.

2.2 OBJETIVOS ESPECÍFICOS

1. Caracterizar como as políticas de proteção de dados estão normatizadas pelo estado brasileiro pós constituição de 1988.
2. Identificar como o Banco Central do Brasil tem ajustado suas políticas para atender às diretrizes nacionais instituídas para a proteção de dados e prevenção de crimes cibernéticos.
3. Compreender os efeitos dessas políticas estabelecidas pelo Banco Central do Brasil na proteção de dados dos consumidores e prevenção de crimes cibernéticos.

3. REFERENCIAL TEÓRICO

A análise das medidas de proteção de dados adotadas pelo Banco Central do Brasil no contexto do varejo financeiro brasileiro exige uma abordagem teórica que considere, de forma articulada, às transformações estruturais da economia digital, o papel do Estado na normatização da proteção de dados e a atuação das instituições reguladoras do sistema financeiro. Assim, o referencial teórico desta pesquisa foi organizado em três eixos complementares, alinhados ao objetivo geral de compreender como essas medidas buscam mitigar os riscos de segurança digital no setor financeiro.

O primeiro eixo aborda o capitalismo de vigilância e a nova ordem digital, discutindo as dinâmicas de coleta, processamento e uso de dados pelas plataformas digitais, bem como seus impactos sobre o setor financeiro. Esse debate permite situar a centralidade dos dados na economia contemporânea e evidenciar os riscos associados à intensificação da vigilância e da financeirização da informação, estabelecendo o contexto no qual a proteção de dados se torna um elemento estratégico para a segurança dos consumidores.

O segundo eixo trata da segurança e soberania digital, com foco no processo de normatização da proteção de dados no Brasil, especialmente no período pós-Constituição de 1988. Ao examinar o papel do Estado brasileiro na formulação de políticas públicas voltadas à proteção da informação e à prevenção de crimes cibernéticos, este tópico contribui para a compreensão do arcabouço legal que orienta a atuação das instituições reguladoras.

Por fim, o terceiro eixo analisa o Sistema Financeiro Nacional, com ênfase no varejo financeiro brasileiro e no papel do Banco Central do Brasil. Este tópico permite compreender como a autoridade monetária tem ajustado suas políticas às diretrizes nacionais de proteção de dados, bem como avaliar os efeitos dessas medidas na mitigação de riscos cibernéticos e na proteção dos dados dos consumidores.

A articulação entre esses três eixos fornece a base teórica necessária para analisar, de forma integrada, a atuação do Banco Central do Brasil diante dos desafios impostos pela economia digital, contribuindo para o alcance dos objetivos propostos nesta dissertação.

3.1 CAPITALISMO DE VIGILÂNCIA E A NOVA ORDEM DIGITAL: ENTRE CONTROLE, PLATAFORMAS FINANCEIRAS E COLONIALISMO DE DADOS

O conceito de capitalismo de vigilância foi desenvolvido pela pesquisadora estadunidense e professora emérita de Harvard, Shoshana Zuboff em sua obra “A era do

capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder" (2020). Zuboff (2020) define esse fenômeno como uma nova forma de capitalismo em que as empresas coletam, analisam e utilizam dados pessoais dos indivíduos para prever e influenciar comportamentos, transformando essas informações em produtos para monetização. Esse processo não se limita à simples coleta de dados; envolve a manipulação das interações humanas e a construção de perfis detalhados que permitem a segmentação e a personalização de ofertas.

Inspirada em autores como Durkheim, Marx, Weber, Hannah Arendt, Teodor Adorno, Karl Polanyi, Jean-Paul Sartre e Stanley Milgram, a autora se propõe a mapear uma nova lógica em vigor no capitalismo de vigilância, tendo como foco as empresas Google, Facebook e Microsoft. A autora não se propõe a fazer uma crítica abrangente dessas empresas, mas sim a utilizá-las como exemplos para analisar as práticas do capitalismo de vigilância em si. Para isso, ela utiliza diversas fontes, como entrevistas com cientistas de dados de várias empresas de tecnologia de ponta e startups no Vale do Silício, além de discursos, conferências, vídeos, programas e políticas dessas empresas (Zuboff, 2020).

O capitalismo de vigilância se diferencia do capitalismo tradicional por seu foco na extração de dados comportamentais, que se tornaram uma mercadoria valiosa, considerado por muitos como "novo petróleo" (Vianna, 2021). Zuboff (2020) argumenta que essa prática representa uma violação da privacidade e da autonomia dos indivíduos, levantando questões éticas e políticas significativas sobre o poder que as grandes empresas exercem sobre a vida cotidiana.

Essa nova forma de capitalismo, conforme delineado pela autora, emerge como uma nova e complexa configuração econômica que transforma dados pessoais em mercadorias valiosas, manipulando e influenciando comportamentos humanos em uma escala sem precedentes. Nesse contexto, diversas características definem essa prática, revelando a profundidade da coleta massiva de dados e a capacidade de prever ações futuras. Desde a invisibilidade dos processos de coleta até a vigilância constante sobre os indivíduos, essas características não apenas levantam questões éticas, mas também desafiam conceitos fundamentais de privacidade e autonomia (Zuboff, 2020).

Dentre suas características, o capitalismo de vigilância, conforme descrito por Zuboff (2020), é marcado pela **coleta massiva de dados**, que se tornou uma prática comum entre as empresas de tecnologia. Essa coleta não se limita a informações explícitas fornecidas pelos usuários, mas inclui uma ampla gama de dados gerados por suas interações online. Muitas vezes, os indivíduos não têm consciência da extensão da coleta, que acontece em segundo

plano, enquanto navegam na internet ou utilizam aplicativos. Essa característica revela uma nova forma de apropriação da vida privada, onde os dados pessoais são tratados como ativos econômicos, frequentemente sem o consentimento informado dos usuários (Zuboff, 2020, Silveira, 2018; Machado, 2018).

Um exemplo evidente dessa coleta massiva é a maneira como o Facebook reúne informações sobre seus usuários, tema explorado no documento “Privacidade Hackeada” de Amer e Noujaim (2019). A plataforma não apenas coleta dados das interações realizadas dentro de sua rede social, mas também rastreia atividades em sites externos que possuem botões de "Curtir" ou que utilizam o Facebook Login (Gonzalez; Roeder; Mcgill, 2017). Com isso, a empresa consegue construir perfis detalhados sobre os interesses e comportamentos dos usuários, permitindo segmentações e direcionamentos que podem ser utilizados para fins publicitários (Zuboff, 2020, Amer; Noujaim, 2019).

Alguns estudos, como os de Fuchs (2017) López, C. et al (2018), Hanna, Rohm e Crittenden (2011), Bharati e Chaudhury (2012) e Cohen (2013) analisam como as empresas utilizam o Facebook para coletar dados de usuários e segmentar suas campanhas de marketing. Os autores destacam que a coleta de dados pelo Facebook permite que as empresas segmentem seus públicos-alvo de maneira altamente eficaz, resultando em campanhas de marketing mais direcionadas. No entanto, os mesmos alertam para o potencial de violação da privacidade dos usuários e a necessidade de implementação de práticas transparentes e éticas na coleta e utilização de dados.

Outra característica fundamental do capitalismo de vigilância é a **predição e manipulação de comportamentos**. Conforme contextualizado por Carvalho (2019) “O uso da tecnologia refina e extrai dos dados para que eles se tornem predição de comportamentos, ou seja, para atuarem na previsibilidade dos passos do usuário” (Carvalho, 2019, p. 55). As empresas utilizam algoritmos avançados para analisar os dados coletados e prever ações futuras, o que lhes permite não apenas entender os hábitos dos usuários, mas também influenciá-los. Essa capacidade de previsão transforma a forma como as empresas se relacionam com os consumidores, levando a interações mais personalizadas, mas também manipuladoras, que podem afetar a autonomia dos indivíduos (Morellato; Santos, 2021; Carvalho, 2019).

Um exemplo dessa manipulação é a forma como a Amazon recomenda produtos. A plataforma utiliza o histórico de compras e navegação de cada usuário para sugerir itens que ele pode estar inclinado a comprar (Gonçalves, 2024). Essa prática, gera o que os autores Huang e Benyoucef (2018) definem como "compra impulsiva" como uma decisão de compra

não planejada, que ocorre de forma rápida e muitas vezes emocional, impulsionada por estímulos externos. Esse comportamento é frequentemente catalisado por fatores como a apresentação de produtos, promoções ou recomendações personalizadas, que podem ativar desejos imediatos nos consumidores. A compra impulsiva está associada a um sentimento de urgência e satisfação instantânea, levando os consumidores a adquirirem itens sem uma consideração profunda de suas necessidades reais ou do impacto financeiro de suas decisões (Huang; Benyoucef, 2018, Liu; Arora, 2013, Zhang; Zhao, 2015, Aral, Walker, 2015).

Essa personalização pode ser vista como uma forma de controle, onde os consumidores são guiados a tomar decisões de compra com base em análises algorítmicas, muitas vezes sem uma consideração consciente de suas próprias necessidades. Os autores Sing e Lyon (2012) estudam o caso específico da Amazon, sua pesquisa revela que a personalização pode criar uma sensação de controle nos consumidores. O estudo sugere que, embora a personalização possa melhorar a satisfação do cliente e a eficiência das compras, também é crucial que os consumidores estejam cientes das influências subjacentes em suas decisões, promovendo uma maior transparência nas práticas de recomendação. Ao final, os autores concluem que a personalização deve ser usada de maneira ética para equilibrar a experiência do consumidor com a proteção de sua autonomia nas decisões de compra.

A **economia da atenção** é outra característica marcante desse novo modelo econômico (Zuboff, 2020). "As plataformas digitais têm se mostrado como espaços competitivos onde a atenção do usuário é a nova moeda" (Santos; Oliveira, 2019, p. 10). As empresas competem ferozmente pela atenção dos usuários, desenvolvendo conteúdos projetados para maximizar o engajamento. Essa dinâmica resulta em uma constante luta por captar a atenção, levando as plataformas a priorizar conteúdos que provocam reações emocionais intensas, como a polarização e a desinformação, em detrimento de um diálogo informativo (Zuboff, 2020, Silva; Lima, 2019; Bentes, 2021).

Um exemplo disso pode ser observado no YouTube, que utiliza algoritmos para recomendar vídeos que mantêm os usuários assistindo por mais tempo. Pereira e Lima (2018) descrevem que o algoritmo do YouTube prioriza conteúdos que geram polarização, impactando a percepção dos usuários. A plataforma tende a favorecer conteúdos sensacionalistas ou polarizadores, pois esses tipos de vídeos são mais eficazes em prender a atenção dos espectadores. Como resultado, os usuários frequentemente se veem expostos a um ciclo de conteúdos que não apenas informam, mas também distorcem realidades, moldando suas percepções de maneira a aumentar o engajamento e a visualização (Pereira; Lima, 2018, Hwang, 2019, Moraes; Almeida, 2020).

A **desigualdade e a exclusão** também são características e consequências do capitalismo de vigilância (Zuboff, 2020). A forma como os dados são utilizados pode levar a discriminações e injustiças sociais, conforme discutido em diversas pesquisas como nas de Silveira (2017), Silveira e Santos (2019), Silveira (2019) e Borges (2020), especialmente quando algoritmos decidem o acesso a serviços e produtos. Essa característica reflete como a coleta de dados pode perpetuar e até agravar desigualdades existentes na sociedade, criando um ciclo vicioso onde determinados grupos são sistematicamente marginalizados (Silva, 2022).

Um exemplo disso se observa em algoritmos de crédito utilizados por instituições financeiras. Em seu estudo, Lopez, Bianchini e Tavares (2021) analisam como os sistemas de pontuação de crédito baseados em algoritmos podem introduzir riscos de discriminação e desigualdade no acesso a serviços financeiros. Os autores discutem a utilização de dados demográficos e comportamentais para avaliar a elegibilidade de indivíduos para empréstimos, destacando que tais dados podem reforçar preconceitos existentes e resultar em práticas discriminatórias. Nesse sentido, eles podem discriminar usuários com base em informações que não refletem adequadamente sua capacidade de pagamento. Isso resulta em taxas de juros mais altas ou na negação de crédito a minorias raciais ou a pessoas de comunidades menos favorecidas, exacerbando a desigualdade econômica e limitando oportunidades (O'neil, 2016, Noble, 2018, Moraes; Woszczyna, 2019).

Por fim, a **invisibilidade do processo de coleta de dados** é uma característica crítica do capitalismo de vigilância. A falta de transparência em relação a como os dados são coletados, utilizados e compartilhados muitas vezes impede que os usuários compreendam plenamente as implicações de suas interações digitais (Zuboff, 2020; Silveira, 2018). Em sua obra, Nissenbaum (2010) propõe uma abordagem contextual da privacidade, analisando como a coleta de dados em ambientes digitais muitas vezes falta transparência. Ela argumenta que os usuários não conseguem entender plenamente as implicações da coleta de dados devido à complexidade e obscuridade das políticas de privacidade. Isso cria um ambiente onde a vigilância se torna parte da vida cotidiana, mas permanece oculta sob camadas de complexidade técnica e terminologias jurídicas.

Um exemplo dessa invisibilidade é a maneira como os termos de uso das plataformas digitais são apresentados. Os artigos de Martins e Souza (2019) e Gomes (2019) analisam esse exemplo. Em seus achados, os autores destacam que muitas vezes, esses documentos são longos, complexos e repletos de jargões legais, fazendo com que os usuários aceitem políticas de privacidade sem realmente compreenderem os riscos envolvidos. Como resultado, eles se

tornam alvos de práticas de vigilância e manipulação sem estarem plenamente cientes da extensão do controle exercido sobre suas vidas.

A partir destas cinco características principais, compreende-se de um modo geral, que o capitalismo de vigilância depende intrinsecamente do capital de plataforma. Esse modelo econômico não apenas explora dados pessoais, mas também transforma as interações sociais em mercadorias, utilizando algoritmos para maximizar lucros e controlar comportamentos. As plataformas digitais, como Google, Facebook e, mais recentemente, os bancos digitais, têm se tornado essenciais na coleta, análise e monetização de dados pessoais. Essas plataformas funcionam como intermediárias que facilitam a interação entre usuários e serviços, enquanto ao mesmo tempo extraem valor dos dados gerados por essas interações.

As plataformas são estruturas que permitem a conexão entre diferentes grupos de usuários, proporcionando um ambiente onde serviços e produtos podem ser oferecidos. Elas se destacam pela sua capacidade de escalar rapidamente e pela sua flexibilidade, podendo operar sem a necessidade de uma presença física. No contexto financeiro, os bancos digitais são um exemplo claro de como esse modelo pode ser aplicado. Esses bancos operam exclusivamente online, sem agências físicas, o que elimina custos operacionais tradicionais e, ao mesmo tempo, possibilita uma coleta constante de dados sobre os hábitos e comportamentos de seus clientes (Pereira, 2019).

No entanto, essa inovação traz consigo desafios significativos. A ausência de agências físicas em bancos digitais significa que os usuários frequentemente interagem com sistemas automatizados e algoritmos para realizar transações, obter crédito e gerenciar suas finanças. Essa interação, característica do capitalismo de vigilância, intensifica a coleta de dados pessoais, muitas vezes sem que os usuários tenham plena consciência disso. Como afirmam autores como Meyer (2021), a falta de um suporte humano tangível não apenas gera desconfiança, mas também reforça um modelo onde as decisões algorítmicas podem ser obscuras e difíceis de contestar. Assim, a dinâmica das plataformas digitais não só redefine a experiência do cliente, mas também levanta questões sobre a privacidade e a equidade no acesso a serviços financeiros, perpetuando desigualdades existentes. Essa realidade exige uma reflexão crítica sobre as implicações sociais e éticas do uso de tecnologias automatizadas no setor financeiro.

Zuboff (2020) argumenta que, nesse contexto, a vigilância se torna uma forma de controle social, onde as plataformas financeiras utilizam dados para monitorar comportamentos e prever ações futuras. Essa prática não apenas afeta a autonomia do indivíduo, mas também transforma as decisões financeiras em processos algorítmicos, muitas

vezes opacos e difíceis de entender. Assim, os usuários se tornam alvos de um sistema que, em vez de oferecer suporte, limita suas opções com base em perfis de risco e padrões de comportamento (Sampaio, Costa, 2025).

Além disso, Lyon (2019) discute como a vigilância nas finanças pode invadir não apenas a vida privada, mas também a esfera pública, moldando percepções sociais e comportamentos coletivos. O controle sobre os dados financeiros contribui para um ambiente em que as informações pessoais são constantemente monitoradas, criando um ciclo de vigilância que pode levar à discriminação e exclusão social.

Neste cenário, Couldry e Mejias (2019) apresentam o conceito de "colonialismo de dados" na qual emerge como uma crítica à maneira como grandes plataformas digitais extraem e exploram dados de populações, especialmente aquelas que já são vulneráveis ou marginalizadas. Crawford (2022) enfatiza que o colonialismo de dados implica uma relação de dominação, onde as empresas de tecnologia coletam informações sem fornecer um retorno justo ou benefícios às comunidades que geram esses dados. Essa dinâmica não apenas perpetua desigualdades existentes, mas também transforma culturas e economias locais em meros dados a serem explorados.

Couldry e Mejias (2019) ainda aprofundam essa discussão ao argumentar que o colonialismo de dados resulta em uma forma de expropriação digital, onde a riqueza gerada pela coleta de dados não é compartilhada com as comunidades que contribuíram para sua criação. Esse fenômeno levanta questões éticas importantes sobre quem realmente se beneficia da coleta de dados e como as comunidades podem ser protegidas contra a exploração.

Adicionalmente, o colonialismo de dados, conforme discutido por Noble (2018) também tem impactos significativos na construção de identidades e na representação social. As plataformas não apenas coletam dados, mas moldam narrativas sobre os indivíduos com base em análises algorítmicas que frequentemente ignoram contextos culturais e sociais. Isso pode resultar em estereótipos prejudiciais e na marginalização ainda maior de grupos já vulneráveis. Gilliom e Monahan (2010) destacam que essa vigilância não é neutra; pelo contrário, é uma forma de controle que reconfigura as relações de poder na sociedade, onde aqueles que detêm os dados exercem influência sobre as narrativas e experiências dos outros. Além disso, o colonialismo de dados perpetua um ciclo de dependência, onde as comunidades, ao não terem controle sobre seus próprios dados, tornam-se cada vez mais vulneráveis à manipulação e à exploração.

Observa-se nesse sentido que se, em épocas passadas, o colonialismo era amplamente caracterizado pela extração de minérios e recursos naturais, atualmente observa-se uma transformação significativa nesse paradigma. A era contemporânea é marcada pela ascensão da extração de dados, que se estabelece como uma nova forma de exploração. De acordo com Faustino (2020), a coleta e o uso de dados pessoais assemelham-se a um garimpo, onde as plataformas digitais, operando muitas vezes sem qualquer consideração ética ou moral, "escavam" informações valiosas provenientes das interações diárias dos usuários. Esse processo resulta na conversão de experiências humanas ricas e complexas em meros números e dados estatísticos, negligenciando os contextos sociais, culturais e individuais que rodeiam cada um desses dados coletados (Faustino, 2020).

Lippold (2020) complementa essa análise ao destacar que a lógica da extração de dados não é nova, mas, de fato, reproduz velhas dinâmicas coloniais. Nesta dinâmica, os colonizadores historicamente se apropriaram dos recursos de comunidades subjugadas, extraindo riquezas sem oferecer benefícios significativos às populações que as sustentavam. A diferença crucial na era digital é que os "recursos" em questão agora são as informações pessoais e comportamentais dos indivíduos, que são coletadas em grande escala e frequentemente sem o consentimento informado. O autor ressalta que a ausência de regulamentação e de práticas transparentes na coleta de dados permite que essa nova forma de colonialismo opere sem as devidas restrições. Como resultado, perpetua-se um ciclo de exploração que marginaliza ainda mais aqueles que já estão em desvantagem, ampliando as disparidades sociais e reforçando desigualdades existentes na sociedade contemporânea. Esse panorama exige uma reflexão crítica sobre as implicações éticas da coleta de dados e uma busca por soluções que garantam proteção e justiça para todas as comunidades afetadas (Lippold, 2020).

Além disso, o fluxo de dados apresenta uma natureza unidirecional: países do Sul Global são monitorados, enquanto determinados países do Norte se beneficiam economicamente desse processo (Silveira, 2021). Essa característica, aliada à dependência tecnológica dos países do Sul em relação às soluções fornecidas pelo Norte, justifica que essa relação seja interpretada como uma forma de colonialidade (Silveira, 2021; Quijano, 2022). Conforme aponta Quijano (2022), mesmo com o avanço das democracias em várias regiões do mundo no século XXI — incluindo o Brasil, que após o período da ditadura militar instituiu uma constituição de princípios democráticos — as relações de poder continuam a favorecer os chamados países centrais, localizados na Europa e nos Estados Unidos. Em outras palavras, a democratização em territórios anteriormente colonizados não eliminou os

vínculos de colonialidade. A concentração massiva de dados nos Estados Unidos gera uma dependência significativa de outros países em relação a essa potência, já que estes se limitam a fornecer dados sem conseguir obter lucros equivalentes no mercado global de informações. Dessa forma, o mercado global de dados transforma diversos países, especialmente os do Sul, em meras fontes de dados e consumidores de tecnologias de vigilância, enquanto países como os Estados Unidos acumulam os dados coletados e os benefícios econômicos derivados deles.

Neste contexto contemporâneo do capitalismo de vigilância, a discussão sobre dois conceitos cruciais também se torna imprescindível: soberania digital e segurança digital. A soberania digital, como destacado por Crawford (2021), refere-se ao direito das comunidades de controlar suas próprias informações, permitindo que decidam como e onde seus dados são coletados e utilizados. Essa autonomia é fundamental para evitar a exploração por plataformas digitais que buscam lucrar com a extração indiscriminada de dados pessoais. Por outro lado, a segurança digital, conforme apontado por Lippold (2020), é vital para proteger essas informações contra acessos não autorizados e abusos, garantindo que os indivíduos possam interagir com o ambiente digital sem o temor de violação de privacidade. Juntas, a soberania e a segurança digital formam uma base essencial para promover um espaço virtual mais justo e equitativo, onde os direitos das comunidades são respeitados e não tratados como meras mercadorias no jogo de poder do capitalismo de vigilância (Faustino, 2020).

Por fim, o quadro 1 apresenta uma síntese dos principais conceitos apresentados nesta seção.

Quadro 1 - Síntese dos principais conceitos da seção 3.1

Conceito-chave	Autor(es)	Definição / Ideia central	Contribuição para o estudo
Capitalismo de vigilância	Zuboff (2020)	Forma contemporânea de capitalismo baseada na extração, análise e monetização de dados comportamentais para prever e influenciar comportamentos humanos.	Fundamenta a análise crítica das práticas organizacionais e regulatórias no setor financeiro, permitindo compreender a segurança digital como parte de uma lógica econômica de controle e monetização de dados.
Extração massiva de dados	Zuboff (2020); Fuchs (2017)	Coleta contínua e invisível de dados pessoais e comportamentais, muitas vezes sem consentimento informado, transformando a vida cotidiana em matéria-prima econômica.	Sustenta a discussão sobre assimetrias de poder entre organizações financeiras e usuários, evidenciando riscos à privacidade e à autonomia dos indivíduos.
Predição e manipulação de comportamentos	Zuboff (2020); Huang e Benyoucef (2018)	Uso de algoritmos para antecipar ações futuras e influenciar decisões dos usuários, como consumo e comportamento financeiro.	Permite problematizar o uso de algoritmos no varejo financeiro, especialmente em decisões automatizadas de crédito, consumo e risco.

Economia da atenção	Zuboff (2020); Santos e Oliveira (2019)	Modelo econômico em que a atenção dos usuários se torna um ativo central, levando plataformas a maximizar engajamento por meio de conteúdos persuasivos.	Ajuda a compreender como plataformas financeiras e digitais moldam comportamentos e decisões, reforçando práticas de vigilância contínua.
Discriminação algorítmica e exclusão	O'Neil (2016); Noble (2018); Lopez et al. (2021)	Uso de algoritmos que reproduzem e ampliam desigualdades sociais, especialmente em decisões como concessão de crédito.	Contribui para a análise das consequências sociais e organizacionais da automação no setor financeiro.
Invisibilidade do processo de coleta de dados	Zuboff (2020); Nissenbaum (2010)	Falta de transparência nos processos de coleta e uso de dados, dificultando a compreensão dos usuários sobre como suas informações são exploradas.	Reforça a necessidade de análise crítica das políticas de segurança e privacidade adotadas pelas instituições financeiras.
Vigilância financeira	Lyon (2019); Zuboff (2020)	Monitoramento contínuo das práticas financeiras dos indivíduos, transformando decisões econômicas em processos algorítmicos opacos.	Sustenta a discussão sobre controle, autonomia e governança no setor financeiro brasileiro.
Colonialismo de dados	Couldry e Mejias (2019); Crawford (2022) Lippold (2020)	Processo de extração e exploração de dados que reproduz lógicas coloniais, apropriando-se de informações sem retorno justo às populações.	Permite analisar criticamente as regulamentações e práticas de segurança digital como possíveis mecanismos de reprodução de desigualdades globais e locais.

Fonte: Elaborado pela autora

3.2 SEGURANÇA E SOBERANIA DIGITAL: PROTEÇÃO DE DADOS NA ERA DA INFORMAÇÃO

A segurança digital é um aspecto essencial na era da informação, caracterizada pela crescente interconexão entre sistemas, dispositivos e usuários. Em um cenário onde a digitalização permeia todos os setores da sociedade, desde serviços públicos até atividades comerciais, a proteção de dados e a segurança das infraestruturas digitais tornaram-se prioritárias para garantir a integridade e a confidencialidade das informações. As ameaças cibernéticas, que vão desde ataques de ransomware até vazamentos de dados, representam riscos significativos tanto para indivíduos quanto para organizações. A natureza evolutiva dessas ameaças exige uma abordagem proativa na implementação de medidas de segurança digital (Grove, 2021).

Os princípios fundamentais da **segurança digital incluem a confidencialidade, integridade e disponibilidade da informação.** Conforme apresentado por Anderson (2020), a confidencialidade diz respeito à proteção de dados contra acessos não autorizados, enquanto a integridade refere-se à precisão e completude das informações. A disponibilidade, por sua

vez, assegura que os dados e sistemas estejam acessíveis quando necessário. Para garantir esses princípios, é essencial que as organizações adotem uma combinação de políticas, práticas e tecnologias, incluindo criptografia, autenticação multifator e monitoramento contínuo de atividades suspeitas (Anderson, 2020).

Nesse sentido, um aspecto crítico da segurança digital é a infraestrutura tecnológica. A utilização de firewalls, sistemas de detecção de intrusões e criptografia são medidas fundamentais para proteger tanto redes quanto dados. Como afirmado por Anderson (2020), tecnologias avançadas, como inteligência artificial e aprendizado de máquina, podem ser utilizadas para detectar e responder a ameaças em tempo real, contribuindo significativamente para a segurança cibernética. No Brasil, a Estratégia Nacional de Cibersegurança do Brasil (E-CIBER) lançada em agosto de 2025, como atualização da estratégia anterior de 2020, estabelece diretrizes que buscam promover a resiliência das infraestruturas digitais, assegurando que o país esteja preparado para enfrentar os desafios impostos pelas ameaças cibernéticas.

Zuboff (2020) enfatiza que a crescente vigilância e coleta de dados por empresas de tecnologia podem ameaçar a soberania dos Estados, pois a informação deixa de estar sob controle nacional. A crescente digitalização das sociedades contemporâneas impõe a necessidade de uma abordagem robusta em segurança digital, que está diretamente relacionada à soberania digital de um Estado.

O conceito de soberania digital refere-se à capacidade de um Estado ou nação de controlar suas infraestruturas digitais, dados e informações, além das políticas que regem o uso e a proteção desses recursos. Este conceito tem ganhado destaque no Brasil e no cenário global, especialmente em um contexto onde a dependência de tecnologias digitais e plataformas online está em constante crescimento. Em um mundo interconectado, questões de privacidade, segurança e controle de dados emergem como aspectos cruciais da soberania nacional.

Uma das dimensões mais relevantes da soberania digital é a proteção da privacidade dos cidadãos. À medida que dados pessoais são coletados e utilizados por empresas e governos, a capacidade de um Estado de regulamentar o uso dessas informações torna-se fundamental.

Em nível global, iniciativas como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia (2016) têm servido de modelo para países que buscam fortalecer suas legislações de proteção de dados. O GDPR não apenas estabelece normas rígidas para o tratamento de dados pessoais, mas também incorpora conceitos de responsabilidade e

transparência, promovendo uma cultura de respeito à privacidade. A adoção de regulamentações semelhantes em outros países é uma tendência crescente, refletindo a importância da segurança digital em um mundo interconectado.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) é um exemplo de iniciativa que busca garantir direitos relacionados à privacidade e ao tratamento de dados pessoais, refletindo a importância de políticas robustas para a soberania digital. A LGPD, instituída pela Lei nº 13.709/2018, tem como objetivo principal a proteção dos dados pessoais dos indivíduos. Conforme seus Artigo 1º e 2º:

> Esta Lei dispõe sobre o tratamento de dados pessoais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018).

> A proteção de dados pessoais é um direito fundamental do ser humano, assegurado pela Constituição Federal, e deve ser garantido em todas as relações que envolvam o tratamento de dados pessoais. (BRASIL, 2018).

A Lei Geral de Proteção de Dados (LGPD) estabelece uma definição abrangente para o que se considera dados pessoais, descrevendo-os como qualquer informação que se relacione a uma pessoa natural, seja ela identificada ou identificável. Essa definição não se limita a informações óbvias, como nome e endereço, mas também abrange uma variedade de dados que podem ser utilizados para identificar um indivíduo, incluindo, mas não se limitando a, endereços de e-mail, dados de localização, números de telefone e outros identificadores pessoais. A aplicação da LGPD é ampla, estendendo-se a todas as operações de tratamento de dados realizadas por pessoas físicas ou jurídicas, independentemente de sua natureza, abrangendo tanto o setor público quanto o privado.

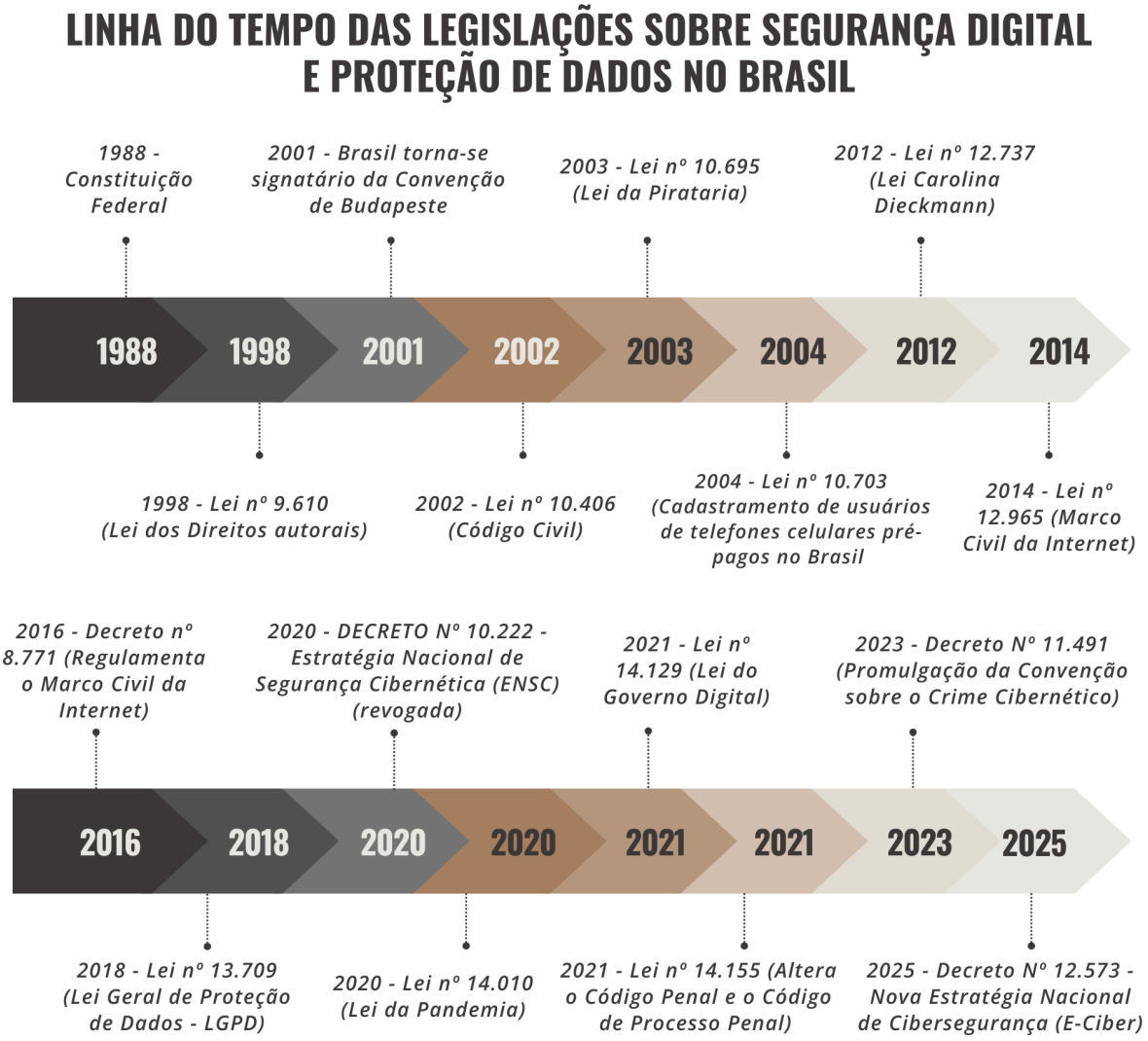
A LGPD também institui um conjunto de princípios que devem ser rigorosamente observados no tratamento de dados pessoais, entre os quais se destacam a finalidade, a necessidade e a transparência. O princípio da finalidade implica que os dados devem ser coletados para propósitos específicos, legítimos e informados ao titular. O princípio da necessidade, por sua vez, estabelece que apenas os dados estritamente necessários para a realização da finalidade pretendida devem ser tratados. Já o princípio da transparência exige que os titulares sejam devidamente informados sobre como seus dados serão utilizados, garantindo, assim, maior clareza e confiança nas práticas de tratamento de dados. Além disso,

a LGPD assegura aos titulares direitos fundamentais, incluindo, mas não se limitando a, acesso a seus dados, correção de informações incompletas ou imprecisas, eliminação de dados desnecessários e a possibilidade de portabilidade dos dados a outros serviços ou plataformas.

Ademais, a LGPD estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD), uma entidade responsável por zelar pela proteção dos dados pessoais e garantir o cumprimento da legislação. A ANPD atua como um órgão regulador, dotado de autoridade para supervisionar e fiscalizar as práticas de tratamento de dados, além de promover a conscientização sobre a importância da proteção de dados pessoais. Sua atuação é crucial para assegurar que tanto o setor público quanto o privado sigam as diretrizes estabelecidas pela LGPD, criando um ambiente em que os direitos dos titulares sejam respeitados e a privacidade seja efetivamente protegida. A criação da ANPD é um passo significativo na construção de um arcabouço legal que visa fortalecer a confiança da sociedade nas interações digitais.

De maneira geral, a evolução das legislações brasileiras nesse campo reflete a crescente preocupação com a privacidade dos cidadãos e a integridade das informações. Desde a implementação de normas que regulam o uso de dados pessoais até a criação de mecanismos de proteção contra ciberataques, a linha do tempo das legislações, conforme apresenta-se a seguir, revela um percurso de adaptação às novas tecnologias e às demandas sociais. Este panorama legislativo não apenas estabelece diretrizes para empresas e órgãos públicos, mas também busca garantir direitos fundamentais dos indivíduos em um ambiente digital em constante transformação. A Figura 1, apresentada abaixo, descreve uma linha do tempo das legislações que abordam segurança digital e proteção de dados no Brasil.

Figura 1 - Linha do Tempo das Legislações sobre Segurança Digital e Proteção de Dados no Brasil



Fonte: Elaborado pela autora

1988 - Constituição Federal: A Constituição de 1988 é um marco fundamental para os direitos individuais no Brasil. No artigo 5º, ela garante a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, reconhecendo a importância da privacidade e estabelecendo bases para futuras legislações sobre proteção de dados. Este artigo é um pilar para a proteção de dados pessoais e segurança digital no Brasil.

1998 - Lei nº 9.610 (Lei dos direitos autorais): Esta lei regula os direitos autorais e estabelece normas para a proteção de obras intelectuais, incluindo aquelas em formato digital. A Lei nº 9.610 protege a propriedade intelectual, o que é essencial para a segurança digital,

pois estabelece que o uso de conteúdos digitais deve ser feito com a autorização dos detentores dos direitos autorais, mitigando riscos de plágio e pirataria.

2001 - Assinatura da Convenção de Budapeste: O Brasil se torna signatário da Convenção sobre Cibercrime, que estabelece diretrizes para a cooperação internacional no combate a crimes cibernéticos. A convenção visa padronizar legislações e práticas entre os países signatários, facilitando a troca de informações e a assistência mútua em investigações relacionadas a crimes digitais. Apesar de o Brasil ter assinado a Convenção de Budapeste sobre o Crime Cibernético em 23 de novembro de 2001, só a promulgou e ratificou internamente anos depois, em 2021 e 2023.

2002 - Lei nº 10.406 (Código Civil): O Código Civil brasileiro introduz princípios sobre responsabilidade civil que são relevantes em casos de danos causados por crimes cibernéticos. Estabelece que as pessoas são responsáveis por atos que causem danos a outrem, incluindo aqueles realizados por meio de tecnologias digitais, enfatizando a necessidade de proteção e reparação em casos de violação de direitos.

2003 - Lei nº 10.695 (Lei da Pirataria): Esta lei alterou o Código Penal para tipificar de forma mais rigorosa a violação de direitos autorais. A principal mudança foi a criação de parágrafos ao artigo 184 do Código Penal, que prevê punições mais severas (reclusão de 2 a 4 anos e multa) para casos de violação com intuito de lucro, como a reprodução ou distribuição ilegal de obras intelectuais, interpretações ou fonogramas. Além disso, a lei também tratou de questões processuais, como a forma de se proceder em cada tipo de crime de direitos autorais.

2004 - Lei nº 10.703: É a lei que dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos no Brasil e dá outras providências. Ela determina que as empresas de telecomunicações pré-pagas mantenham um cadastro atualizado dos seus usuários, incluindo informações como nome completo, CPF ou CNPJ. A lei também prevê penalidades para o não cumprimento da obrigação, incluindo multas, e determina que os dados do cadastro devem ser disponibilizados às autoridades judiciais quando solicitado.

2012 - Lei nº 12.737 (Lei Carolina Dieckmann): Esta lei tipifica uma série de crimes cibernéticos, como a invasão de dispositivos eletrônicos e a disseminação de vírus. A lei leva o nome da atriz Carolina Dieckmann, cuja intimidade foi violada por meio da divulgação de fotos íntimas. A legislação estabelece penalidades para invasões de dispositivos, fortalecendo a proteção dos dados pessoais e a privacidade dos cidadãos.

2014 - Lei nº 12.965 (Marco Civil da Internet): Considerado um marco na regulação da internet no Brasil, este conjunto de leis estabelece princípios para o uso da internet, como a neutralidade da rede e a proteção dos dados pessoais. O Marco Civil garante a privacidade dos

usuários e estabelece a responsabilidade dos provedores de internet em relação ao tratamento de dados, definindo direitos e deveres que devem ser respeitados.

2016 - Decreto nº 8.771: O Decreto regulamenta o Marco Civil da Internet e estabelece diretrizes sobre a neutralidade da rede, a guarda e proteção de dados por provedores, e procedimentos para a requisição de dados. O decreto define as exceções à neutralidade, os procedimentos para provedores de conexão e de aplicações sobre como guardar e proteger dados, e a necessidade de ordem judicial para a requisição de dados cadastrais pela administração pública, com exigência de transparência nas solicitações.

2018 - Lei nº 13.709 (Lei Geral de Proteção de Dados - LGPD): A LGPD é a principal legislação brasileira sobre proteção de dados pessoais, estabelecendo diretrizes claras para o tratamento de dados por entidades públicas e privadas. A lei garante direitos aos titulares dos dados, como acesso, correção e eliminação de informações, e institui a Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar e regulamentar o cumprimento da lei.

2020 - Estratégia Nacional de Segurança Cibernética (ENSC): A ENSC foi lançada pelo governo federal para fortalecer a resiliência das infraestruturas críticas do Brasil frente a ameaças cibernéticas. A estratégia define ações para prevenir, detectar e responder a incidentes de segurança cibernética, promovendo a colaboração entre setores públicos e privados e enfatizando a capacitação de profissionais na área. Essa estratégia foi revogada pela nova E-Ciber, aprovada pelo Decreto nº 12.573/2025.

2020 - Lei nº 14.010 (Lei da Pandemia): Esta lei foi criada em resposta à pandemia de COVID-19, e alterou a entrada em vigor de partes da LGPD. A principal mudança foi que a vigência das sanções administrativas previstas na LGPD foi adiada para 1º de agosto de 2021, enquanto a legislação original previa a vigência total em maio de 2021, conforme o Art. 15.

2021 - Lei nº 14.129 (Lei de Governo Digital): A Lei de Governo Digital promove a transformação digital dos serviços públicos, estabelecendo diretrizes para a prestação de serviços online de maneira segura. A legislação enfatiza a segurança da informação e a proteção de dados, garantindo que os serviços digitais sejam acessíveis e respeitem os direitos dos cidadãos.

2021 - Lei nº 14.155: A Lei alterou o Código Penal e o Código de Processo Penal para tornar mais graves crimes eletrônicos como invasão de dispositivo informático, furto e estelionato. As principais mudanças incluem o aumento das penas para esses crimes e a inclusão de qualificadoras, como o uso de fraude eletrônica e a prática do crime contra idosos

ou vulneráveis. Além disso, a lei definiu a competência judicial para esses crimes com base no domicílio da vítima.

2023 - Decreto Nº 11.491 (Promulgação da Convenção sobre o Crime Cibernético) - O Decreto de 12 de abril de 2023, promulga a Convenção sobre o Crime Cibernético no Brasil, tornando-a parte da legislação nacional. A convenção foi firmada pelo Brasil em 2001 e aprovada pelo Congresso Nacional em 2021, com o decreto sendo a etapa final de sua promulgação interna para entrar em vigor no país. A medida visa estabelecer regras de cooperação internacional para combater crimes cibernéticos, que incluem tipificação de delitos, obtenção de dados, interceptação e extradição.

2025 - Decreto Nº 12.573, de 4 de agosto de 2025: A E-Ciber (Estratégia Nacional de Cibersegurança 2025) é uma política pública que visa fortalecer a cibersegurança no Brasil, protegendo a soberania nacional, os direitos fundamentais dos cidadãos e a resiliência dos serviços essenciais e das infraestruturas críticas, por meio de ações coordenadas de desenvolvimento tecnológico, formação profissional, pesquisa científica e cooperação internacional.

Além da proteção de dados, a soberania digital também envolve a segurança cibernética. Morozov (2013) argumenta que a segurança cibernética deve ser considerada uma questão de soberania nacional, pois a fragilidade das redes pode comprometer não apenas a economia, mas também a segurança do Estado. No Brasil, iniciativas como a Estratégia Nacional de Segurança Cibernética (ENSC) visam fortalecer a defesa cibernética, promovendo a capacitação de profissionais e a criação de protocolos de segurança (BRASIL, 2020).

Um dos tipos mais comuns de ataque cibernético é o phishing, que envolve a criação de mensagens fraudulentas, geralmente por e-mail, para enganar os usuários a fornecer informações pessoais ou financeiras. De acordo com Anderson (2020), o phishing pode ser altamente eficaz, pois muitas vezes utiliza técnicas de engenharia social para parecer legítimo. Os atacantes costumam se passar por instituições confiáveis, criando uma falsa sensação de segurança para as vítimas.

Um exemplo comum de phishing no setor financeiro é a criação de e-mails fraudulentos que parecem ser enviados por bancos, como o incidente envolvendo o Banco Central do Brasil em 2020, onde cibercriminosos utilizaram técnicas de phishing para roubar informações de contas bancárias de clientes. Os hackers enviaram e-mails fraudulentos que pareciam ser comunicados oficiais do banco, levando os usuários a fornecerem seus dados pessoais e senhas em um site falso.

Esses e-mails geralmente contêm uma mensagem que alerta o usuário sobre uma atividade suspeita em sua conta, como uma tentativa de login não reconhecida ou a necessidade de verificar informações pessoais. O e-mail inclui um link que supostamente leva a uma página de login do banco. No entanto, essa página é uma imitação cuidadosamente elaborada do site legítimo, projetada para enganar os usuários. Ao inserir suas credenciais, como nome de usuário e senha, o usuário acaba fornecendo essas informações diretamente aos cibercriminosos. Esse tipo de ataque pode ter consequências graves, resultando em roubo de identidade, acesso não autorizado a contas bancárias e perdas financeiras significativas.

Outro ataque frequente é o ransomware, onde um software malicioso é instalado nos sistemas da vítima, criptografando dados essenciais e exigindo um resgate para a recuperação das informações. Conforme observado por Stallings e Katz (2018), o ransomware pode causar danos significativos, resultando em perdas financeiras e interrupções operacionais para empresas e organizações. O aumento da popularidade do trabalho remoto durante a pandemia de COVID-19 contribuiu para um aumento nos casos de ransomware, uma vez que muitos usuários estão em ambientes menos seguros.

Um exemplo notório de ataque de ransomware ocorreu em maio de 2021, quando o grupo de cibercriminosos conhecido como DarkSide atacou a Colonial Pipeline, uma das maiores operadoras de oleodutos dos Estados Unidos. O ataque resultou na criptografia de dados críticos da empresa, levando à paralisação temporária das operações e causando escassez de combustível em várias regiões do país (Sullivan, 2021).

Após o ataque, os cibercriminosos exigiram um resgate em criptomoedas para fornecer a chave de descriptografia e permitir a recuperação dos dados. A Colonial Pipeline acabou pagando cerca de 4,4 milhões de dólares para recuperar o acesso aos seus sistemas. Esse incidente não apenas gerou perdas financeiras significativas, mas também causou interrupções em toda a cadeia de suprimentos de combustível, evidenciando os impactos potenciais do ransomware em setores críticos (Sullivan, 2021).

Além destes, os ataques de negação de serviço (DoS) e suas variantes, como o DDoS (Distributed Denial of Service), têm se tornado cada vez mais comuns. Esses ataques visam tornar um serviço ou rede indisponível ao sobrecarregá-los com tráfego excessivo. Segundo Ferreira (2019), os ataques DDoS são particularmente preocupantes, pois podem derrubar websites inteiros, afetando negócios e serviços críticos. Eles são frequentemente realizados por grupos de hackers ou até mesmo como forma de protesto.

Um exemplo notório de ataque DDoS ocorreu em 2016, quando o provedor de DNS (Sistema de Nomes de Domínio) da empresa Dyn foi alvo de um ataque em larga escala que

afetou diversos serviços online, incluindo Twitter, Netflix e Spotify. O ataque comprometeu a infraestrutura da Dyn, resultando em interrupções significativas no acesso a esses serviços por várias horas. Esse incidente foi realizado por meio de uma botnet composta por dispositivos IoT (Internet das Coisas), demonstrando como vulnerabilidades em dispositivos conectados podem ser exploradas para gerar tráfego excessivo e sobrecarregar serviços (Krebs, 2016).

Outra técnica de ataque que tem ganhado notoriedade é a exploração de vulnerabilidades em softwares e sistemas. Esses ataques aproveitam falhas de segurança que não foram corrigidas, permitindo que os invasores acessem sistemas e informações sensíveis. Um exemplo marcante desse tipo de ataque ocorreu em 2017, quando o ransomware WannaCry se espalhou globalmente, explorando uma vulnerabilidade no sistema operacional Windows conhecida como EternalBlue.

Esse ataque afetou mais de 200.000 computadores em mais de 150 países, criptografando dados e exigindo resgates para a recuperação das informações. A vulnerabilidade, que havia sido descoberta pela NSA e posteriormente vazada, não tinha sido corrigida em muitos sistemas, o que facilitou a propagação do malware. Empresas, hospitais e instituições governamentais foram severamente impactados (Zarskay, 2018).

Segurança cibernética e soberania digital são, portanto, dimensões inseparáveis. Se a soberania digital implica a capacidade de um Estado controlar sua infraestrutura, suas regras e seus fluxos de informação, a segurança cibernética representa o alicerce técnico que torna esse controle possível. Sem resiliência contra phishing, ransomware, ataques DDoS ou exploração de vulnerabilidades — como demonstram os exemplos nacionais e internacionais — qualquer tentativa de autodeterminação digital fica comprometida. Governos, instituições financeiras e provedores de serviços críticos tornam-se dependentes de estruturas tecnológicas frágeis ou vulneráveis, o que amplia riscos de ingerência externa, paralisação econômica e violação massiva de dados pessoais. Assim, ao fortalecer suas políticas de proteção, resposta a incidentes e defesa cibernética, o Brasil não apenas protege usuários e instituições, mas também consolida sua autonomia no ambiente digital. A segurança cibernética deixa, portanto, de ser um mero requisito técnico e se torna um pilar essencial da soberania digital, garantindo que o país exerça plenamente sua capacidade de governar, regular e proteger seu ecossistema informacional.

Outro aspecto importante da soberania digital é a regulação das grandes plataformas de tecnologia. Nos últimos anos, gigantes como Google, Facebook e Amazon têm exercido um poder significativo sobre a economia digital e as informações dos usuários. O controle que essas empresas exercem pode ameaçar a soberania digital dos Estados, uma vez que suas

operações transcendem fronteiras. De acordo com DeNardis (2014), a governança da internet deve ser repensada para garantir que os Estados possam regular e fiscalizar o uso de suas infraestruturas digitais. No Brasil, debates sobre a regulação das plataformas digitais estão se intensificando, com propostas que visam criar um marco legal mais robusto para enfrentar essas questões

No que se refere ao setor financeiro, a digitalização das transações financeiras trouxe benefícios significativos, como a conveniência e a agilidade nos processos. No entanto, também expôs vulnerabilidades que podem ser exploradas por criminosos digitais, levantando questões críticas sobre a segurança financeira.

Estudos apontam que o aumento da digitalização das finanças também está relacionado ao crescimento das fraudes e dos ciberataques. De acordo com o relatório da Federação Brasileira de Bancos (FEBRABAN, 2021) o Brasil registrou um aumento de 80% nas tentativas de fraudes digitais em 2020, com cerca de R$5 bilhões desviados por meio de crimes cibernéticos. Esse cenário reflete a necessidade urgente de uma abordagem robusta para a segurança financeira. As instituições financeiras estão investindo cada vez mais em tecnologias de cibersegurança, como inteligência artificial e machine learning, para detectar comportamentos suspeitos e prevenir fraudes em tempo real (Silva; Moraes, 2020).

Um exemplo de inovação nas transações digitais é o sistema de pagamentos instantâneos conhecido como Pix, lançado pelo Banco Central do Brasil em novembro de 2020. Com o Pix, os usuários podem realizar transferências e pagamentos em tempo real, 24 horas por dia, utilizando apenas um smartphone. Desde sua implementação, o Pix ganhou rápida adesão, com mais de 130 milhões de usuários cadastrados até 2023, representando cerca de 62% da população brasileira (BANCO CENTRAL DO BRASIL, 2023). Contudo, essa popularidade também atraiu criminosos. De acordo com dados da Febraban, 51% das tentativas de fraudes em 2021 foram relacionadas a transações via Pix, com golpes como o "phishing" e fraudes envolvendo engenharia social se tornando comuns (FEBRABAN, 2022).

Adicionalmente, a pesquisa realizada pela Confederação Nacional de Dirigentes Lojistas (CNDL, 2022) revelou que 64% dos consumidores brasileiros se sentem inseguros ao realizar transações financeiras online. Nesse sentido, destaca-se ainda que muitos consumidores ainda não têm conhecimento sobre as melhores práticas de segurança digital, o que os torna vulneráveis a golpes e fraudes. Segundo a pesquisa da IBM (2021), 75% das pessoas afirmaram não ter recebido orientações adequadas sobre como proteger suas informações financeiras.

No Brasil, o Banco Central (BC) exerce um papel fundamental na regulação e supervisão do mercado financeiro, configurando-se como a principal autoridade responsável pela promoção da estabilidade do sistema financeiro nacional. As atribuições do BC abrangem não apenas a implementação de políticas monetárias, mas também a criação de normas que visam proteger os consumidores e assegurar a integridade das operações financeiras, especialmente no contexto digital contemporâneo. A evolução das tecnologias financeiras, exemplificada pela introdução do sistema de pagamentos instantâneos, o Pix, e o surgimento de fintechs, demanda uma adaptação contínua por parte do BC frente aos desafios emergentes nesse ambiente dinâmico.

Por fim, o quadro 2 apresenta uma síntese dos principais conceitos apresentados nesta seção.

Quadro 2 - Síntese dos principais conceitos da seção 3.2

Conceito-chave	Autor(es)	Definição / Ideia central	Contribuição para o estudo
Proteção de dados pessoais	LGPD – Lei nº 13.709/2018	Garantia de direitos fundamentais relacionados à privacidade, liberdade e autodeterminação informacional.	Base normativa central para avaliar práticas organizacionais de tratamento de dados no setor financeiro.
Segurança digital	Grove (2021); Anderson (2020)	Conjunto de políticas, práticas e tecnologias destinadas a proteger dados, sistemas e infraestruturas digitais contra ameaças cibernéticas.	Fundamenta a análise das políticas organizacionais e regulatórias de proteção de dados no setor financeiro.
Princípios da segurança digital	Anderson (2020)	Confidencialidade (acesso restrito), integridade (exatidão dos dados) e disponibilidade (acesso quando necessário).	Oferece critérios analíticos para avaliar a efetividade das práticas de segurança adotadas pelas instituições financeiras.
Infraestrutura de segurança cibernética	Anderson (2020); Stallings e Katz (2018)	Uso de firewalls, criptografia, sistemas de detecção de intrusão, IA e monitoramento contínuo para proteção de redes e dados.	Sustenta a discussão sobre a dimensão técnica da segurança digital como elemento organizacional estratégico.
Soberania digital	Zuboff (2020); Crawford (2021)	Capacidade de Estados e sociedades controlarem suas infraestruturas digitais, dados e políticas informacionais.	Permite analisar o papel do Estado brasileiro na regulação do ambiente digital financeiro.
Segurança financeira digital	Febraban (2021); Silva e Moraes (2020)	Proteção das transações financeiras digitais frente ao crescimento de fraudes e cibercrimes.	Conecta segurança digital à estabilidade do varejo financeiro e à confiança dos usuários.
Proteção de dados pessoais	LGPD – Lei nº 13.709/2018	Garantia de direitos fundamentais relacionados à privacidade, liberdade e autodeterminação informacional.	Base normativa central para avaliar práticas organizacionais de tratamento de dados no setor financeiro.

Fonte: Elaborado pela autora

3.3 SISTEMA FINANCEIRO NACIONAL: UMA ANÁLISE DO SISTEMA DE VAREJO FINANCEIRO BRASILEIRO A PARTIR DO BANCO CENTRAL DO BRASIL

O Sistema Financeiro Nacional (SFN) é o conjunto de instituições, normas e instrumentos que operam de forma integrada com o objetivo de organizar, regular e viabilizar a intermediação financeira no Brasil. Sua função principal é promover o fluxo eficiente de recursos entre os agentes superavitários, que possuem capital disponível para investimento, e os agentes deficitários, que necessitam de financiamento para o desenvolvimento de suas atividades produtivas, comerciais ou de consumo (Assaf Neto, 2021). Dessa forma, o SFN é essencial para a estabilidade do sistema econômico, o crescimento sustentável e a execução das políticas monetária, fiscal e cambial do país.

O SFN teve sua estrutura institucional formalmente estabelecida com a promulgação da Lei nº 4.595, de 31 de dezembro de 1964, que organizou e disciplinou as atividades monetárias, bancárias e creditícias no Brasil. Essa legislação representou um marco na modernização do sistema financeiro nacional, ao reunir em um único instrumento jurídico as diretrizes para a regulação e supervisão do setor. Entre suas inovações mais relevantes, destaca-se a criação do Conselho Monetário Nacional (CMN) como órgão máximo do sistema, incumbido de formular a política da moeda e do crédito e de orientar o desenvolvimento econômico equilibrado do país (BRASIL, 1964).

Além disso, a mesma lei instituiu o Banco Central do Brasil (BC), conferindo-lhe o papel de autoridade monetária e executora das diretrizes estabelecidas pelo CMN. O BC passou a concentrar competências antes atribuídas a diferentes órgãos, como a Superintendência da Moeda e do Crédito (SUMOC), o Banco do Brasil e o Tesouro Nacional, promovendo uma maior centralização, eficiência e autonomia na condução da política econômica. Essa reorganização institucional foi fundamental para conferir maior estabilidade e previsibilidade ao funcionamento do sistema financeiro, bem como para fortalecer os instrumentos de política monetária, creditícia e cambial (BRASIL, 1964).

Conforme contextualizado por Silva (2004), a criação do SFN por meio da Lei nº 4.595/1964 foi motivada pela necessidade de reorganizar o sistema financeiro diante das transformações estruturais da economia brasileira, especialmente durante o processo de industrialização e urbanização acelerada nas décadas de 1950 e 1960. O antigo arranjo

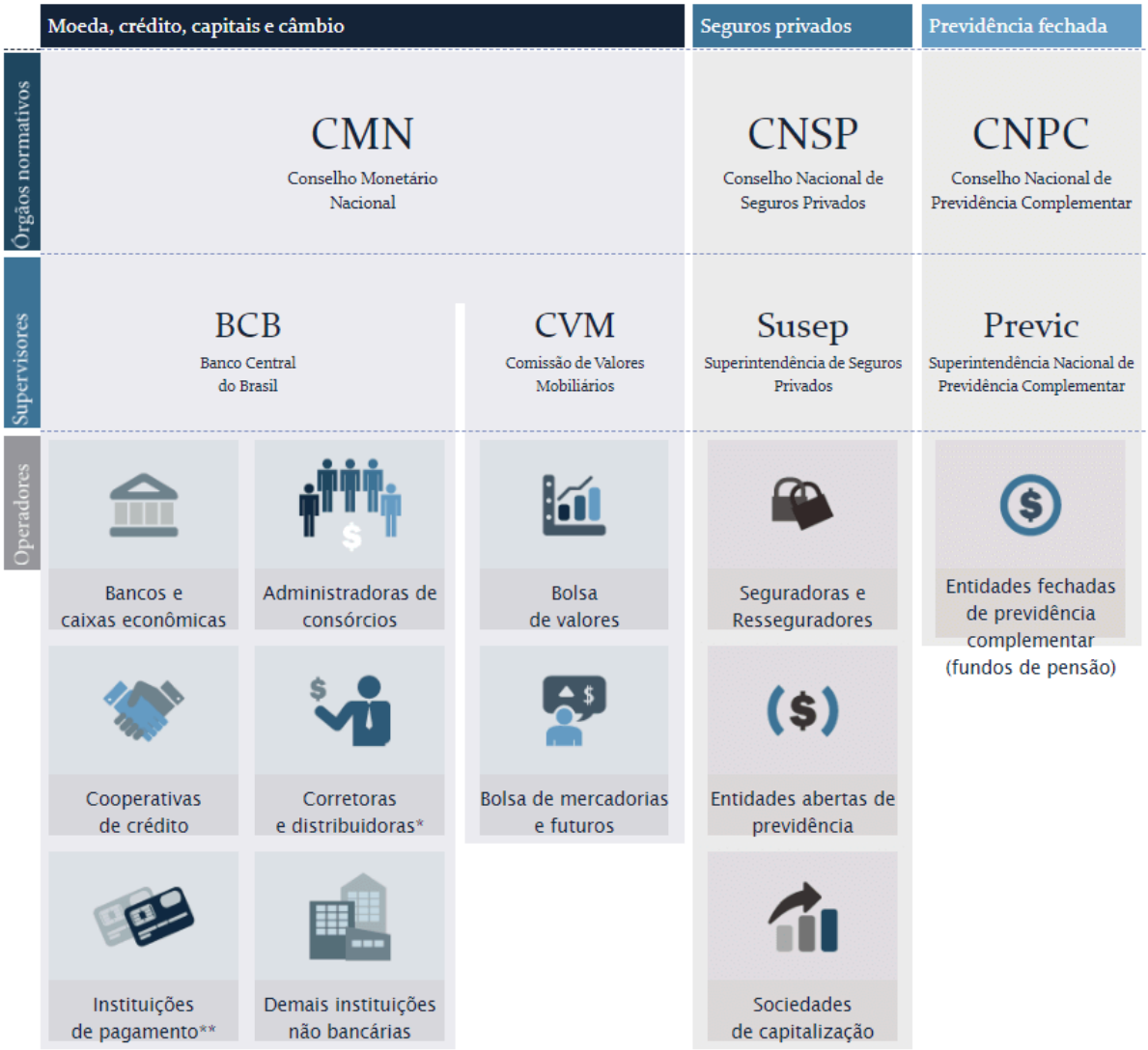
institucional apresentava fragilidades, como a dispersão normativa, a sobreposição de funções entre órgãos e a ausência de uma autoridade monetária claramente definida. Nesse contexto, a nova legislação buscou estabelecer um modelo mais racional e funcional, com ênfase na estabilidade da moeda, no controle da inflação e na eficiência do crédito (Silva, 2004).

A estrutura do SFN pode ser dividida em três níveis: órgãos normativos, entidades supervisoras e operadores financeiros. Os órgãos normativos são responsáveis por formular as diretrizes e políticas que orientam o funcionamento do sistema. O principal deles é o Conselho Monetário Nacional (CMN), que estabelece as bases da política monetária, creditícia e cambial, além de definir normas para o bom funcionamento das instituições financeiras. Além do CMN, também atuam como órgãos normativos o Conselho Nacional de Seguros Privados (CNSP), que regulamenta o setor de seguros, e o Conselho Nacional de Previdência Complementar (CNPC), que estabelece diretrizes para a previdência complementar fechada (BANCO CENTRAL DO BRASIL, 2025).

As entidades supervisoras, por sua vez, são responsáveis por aplicar e fiscalizar o cumprimento das normas definidas pelos órgãos normativos. Entre as principais instituições supervisoras destaca-se o Banco Central do Brasil (BC), que executa a política monetária, controla a emissão de moeda, fiscaliza instituições financeiras e atua na regulação do sistema bancário. Outro órgão de grande relevância é a Comissão de Valores Mobiliários (CVM), que supervisiona e regula o mercado de capitais, garantindo a transparência das informações e a segurança dos investidores. Complementam esse grupo a Superintendência de Seguros Privados (SUSEP), responsável pela fiscalização dos mercados de seguros, capitalização e previdência complementar aberta, e a Superintendência Nacional de Previdência Complementar (PREVIC), que atua na supervisão dos fundos de pensão (BANCO CENTRAL DO BRASIL, 2025).

O terceiro nível do SFN é composto pelos operadores financeiros, ou seja, as instituições que atuam diretamente na intermediação de recursos financeiros. Entre elas estão os bancos comerciais, bancos de investimento, cooperativas de crédito, sociedades de crédito, corretoras, distribuidoras de valores mobiliários e as chamadas fintechs. Essas instituições desempenham o papel de captar recursos junto aos poupadores e aplicá-los junto aos tomadores de crédito, promovendo a circulação de capital e contribuindo para o desenvolvimento econômico do país (BANCO CENTRAL DO BRASIL, 2025).

Figura 2 - Estrutura do Sistema Financeiro Nacional (SFN)



Fonte: Banco Central do Brasil (2025).

O Sistema Financeiro Nacional atua em diferentes mercados que, apesar de distintos, são interdependentes. O mercado monetário lida com operações de curtíssimo prazo entre instituições financeiras e o Banco Central, sendo utilizado para controlar a liquidez da economia. O mercado de crédito envolve operações de empréstimo e financiamento voltadas a consumidores e empresas. O mercado de capitais é destinado à negociação de títulos e valores mobiliários, como ações e debêntures, sendo uma importante fonte de financiamento para o setor produtivo. Já o mercado cambial abrange as transações envolvendo moedas estrangeiras, essencial para o comércio exterior e investimentos internacionais. Por fim, o mercado de seguros e previdência oferece instrumentos de proteção patrimonial e planejamento de longo prazo (BANCO CENTRAL DO BRASIL, 2025).

Dentro da estrutura do SFN, o sistema de varejo financeiro brasileiro constitui o conjunto de instituições, produtos e serviços voltados ao atendimento das necessidades financeiras de pessoas físicas e de micro e pequenas empresas. Esse segmento, representa a interface direta entre o cidadão comum e o SFN, sendo responsável por possibilitar o acesso a contas bancárias, meios de pagamento, crédito, investimentos e seguros.

A escolha do Banco Central do Brasil como unidade central de análise neste estudo decorre de seu papel singular no arranjo institucional do SFN. Embora o SFN seja composto por diferentes instâncias — órgãos normativos, entidades supervisoras e operadores — apenas o BC acumula simultaneamente funções regulatórias, fiscalizatórias e de supervisão prudencial direta sobre a maior parte das instituições que compõem o varejo financeiro, incluindo bancos comerciais, instituições de pagamento e fintechs. Isso confere ao BC uma posição estratégica para compreender como normas de proteção de dados e segurança digital são formuladas, operacionalizadas e internalizadas pelo setor. Ao contrário do CMN, que estabelece diretrizes gerais, ou da CVM, cuja atuação concentra-se no mercado de capitais, o BC atua no núcleo operacional da vida financeira cotidiana dos brasileiros, regulando instituições responsáveis por contas correntes, cartões, meios de pagamento, crédito pessoal e transações digitais — justamente onde os dados pessoais são mais intensamente coletados e processados.

Além disso, o BC tem sido o principal agente governamental responsável por traduzir os princípios da LGPD e das estratégias nacionais de cibersegurança em normas específicas para o setor financeiro. A partir de 2017, com o fortalecimento das diretrizes internacionais de segurança cibernética e, posteriormente, com a entrada em vigor da LGPD, observa-se um aumento significativo na publicação de resoluções, instruções normativas e circulares que tratam direta ou indiretamente da proteção de dados sensíveis. Dessa forma, analisar o BC significa investigar o ponto onde a proteção de dados deixa o campo da lei geral e passa a se transformar em obrigações técnicas concretas para instituições financeiras. É nesse nível que os princípios abstratos de privacidade se materializam em requisitos de segregação de bases de dados, auditorias, continuidade de negócios, governança interna, certificações de nuvem e mecanismos de reporte de incidentes — temas centrais para a mitigação de riscos digitais.

A escolha do varejo financeiro como recorte setorial se justifica porque esse é o segmento em que a vulnerabilidade do cidadão é maior e onde os impactos de políticas de segurança digital se fazem sentir de forma mais imediata. O varejo financeiro concentra milhões de transações diárias, envolvendo clientes que, em grande parte, não possuem conhecimento técnico para avaliar riscos cibernéticos e dependem da eficácia das instituições

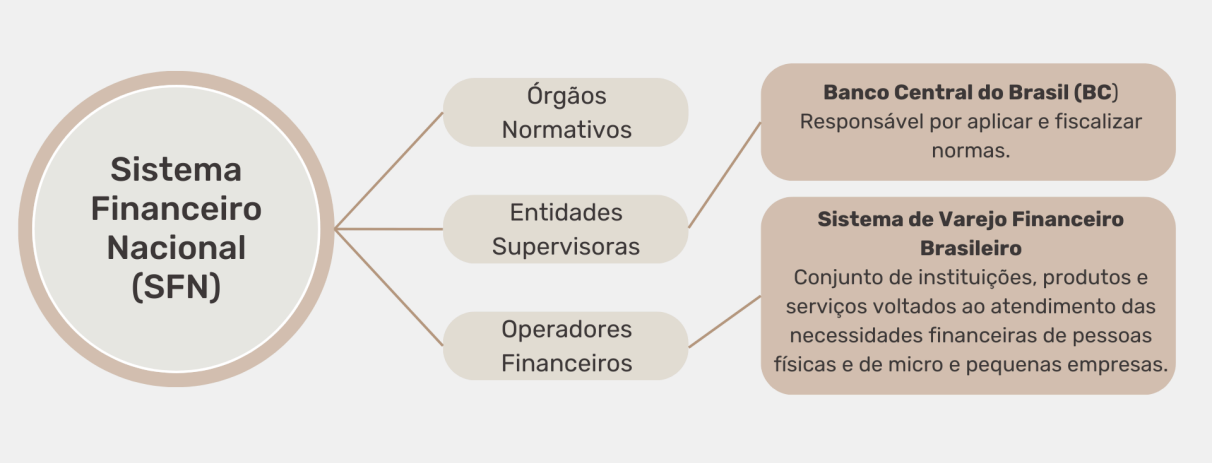
e da atuação do regulador para garantir a integridade de seus dados e seu patrimônio. É também nesse segmento que se encontram os maiores volumes de dados pessoais e financeiros sensíveis, além de ser o principal alvo de fraudes, golpes digitais e ataques cibernéticos, conforme reiteradamente demonstrado por pesquisas de entidades como CNDL (2022) e FEBRABAN (2021, 2022).

Outra justificativa relevante é que o varejo financeiro tem sido o principal laboratório de inovação digital do Brasil — Open Banking/Open Finance, PIX, pagamentos instantâneos, carteiras digitais e plataformas de crédito automatizado. Essa rápida digitalização ampliou exponencialmente a superfície de exposição a riscos cibernéticos e tornou a proteção de dados um elemento estrutural do funcionamento do setor. Portanto, investigar como as medidas regulatórias do BC dialogam com as práticas de segurança adotadas por essas instituições é essencial para compreender se o arcabouço regulatório atual é capaz de acompanhar a velocidade das transformações tecnológicas e os desafios emergentes do capitalismo de vigilância.

Por fim, o recorte BC, associado ao varejo financeiro não é apenas operacionalmente coerente, mas cientificamente estratégico. Ele permite observar a relação entre regulação, práticas organizacionais e proteção do consumidor em um campo de alta complexidade técnica, elevado fluxo de dados sensíveis e intensa dependência tecnológica. Além disso, esse recorte oferece condições ideais para analisar tensões contemporâneas fundamentais, como: (a) o equilíbrio entre inovação financeira e segurança digital; (b) os limites da regulação frente à terceirização e uso de nuvem internacional; (c) os riscos de assimetria informacional e vigilância algorítmica; (d) a presença de práticas típicas do capitalismo de vigilância dentro de um setor altamente regulado; e (e) os desafios relacionados à soberania digital.

A Figura 3 ilustra a posição exata do objeto de pesquisa dentro da estrutura do Sistema Financeiro Nacional.

Figura 3 - Escopo do estudo



Fonte: Elaborado pelo autora

Com o avanço tecnológico, o varejo financeiro brasileiro passou por uma profunda transformação digital. O surgimento do PIX, em 2020, por exemplo, revolucionou os pagamentos de varejo, proporcionando transferências instantâneas e sem custo para pessoas físicas, o que ampliou significativamente a inclusão financeira (FISERV, 2022). Paralelamente, o movimento de Open Finance vem permitindo maior integração e transparência entre instituições financeiras, ampliando a concorrência e a personalização dos serviços oferecidos.

De acordo com o BC, o sistema de varejo compreende os serviços financeiros que envolvem grande volume de transações de baixo valor, como transferências, pagamentos, depósitos, saques e concessão de crédito ao consumo (BANCO CENTRAL DO BRASIL, 2021). Dessa forma, o varejo financeiro tem como principal característica a massificação — ou seja, a oferta de produtos padronizados e de fácil acesso a uma ampla base de clientes. As instituições participantes desse sistema incluem os bancos comerciais, as cooperativas de crédito, as sociedades de crédito, financiamento e investimento, e, mais recentemente, as fintechs, que introduziram novas tecnologias e modelos de negócio no setor. Todas essas entidades operam sob autorização e supervisão do Banco Central do Brasil.

> O Banco Central do Brasil (BC) é uma autarquia federal, sem vinculação ou subordinação ao Ministério, com autonomia técnica, operacional, administrativa e financeira. Seus objetivos fundamentais são: garantir a estabilidade de preços; zelar pela estabilidade e pela eficiência do sistema financeiro; suavizar as oscilações do nível de atividade econômica; e estimular o pleno emprego (BANCO CENTRAL DO BRASIL, 2024).

Em seu histórico, o BC passou por um longo processo de amadurecimento antes de sua fundação, refletindo a crescente percepção da necessidade de uma instituição que exercesse o papel de "banco dos bancos". Essa conscientização remonta ao período anterior ao século XX, quando já se vislumbrava a criação de um banco central com a capacidade exclusiva de emitir papel-moeda e atuar como banqueiro do Estado. A história do sistema monetário brasileiro pode ser traçada desde 1694, com a criação da Casa da Moeda, que estabeleceu as bases para a organização financeira do país. Em 1808, com a chegada do príncipe regente D. João ao Brasil, surgiram discussões sobre a necessidade de um banco que acumulasse funções de banco central e comercial, culminando na fundação do Banco do Brasil no mesmo ano (BANCO CENTRAL DO BRASIL, 2023).

O Banco do Brasil, estruturado como um banco central misto, tinha atribuições de banco de depósitos, desconto e emissão, além de ser responsável pela comercialização de produtos da administração pública. Esse acúmulo de funções é apontado como um dos fatores que retardaram a criação de um banco central independente. A evolução econômica mundial ao longo dos anos reforçou a necessidade de uma estrutura que organizasse a oferta de moeda e supervisionasse o sistema financeiro (BANCO CENTRAL DO BRASIL, 2023).

Até 1945, todas as funções de autoridade monetária estavam sob a responsabilidade do Banco do Brasil, o que evidenciou a carência de uma organização específica para esse fim. Em 2 de fevereiro de 1945, o governo de Getúlio Vargas estabeleceu, por meio do Decreto nº 7.293, a Superintendência da Moeda e do Crédito (SUMOC), que tinha a missão de regular o tumultuado mercado financeiro e combater a inflação. A Sumoc assumiu importantes responsabilidades, como a fixação de percentuais de reservas obrigatórias dos bancos comerciais e a supervisão da política cambial (BANCO CENTRAL DO BRASIL, 2023).

No entanto, o Banco do Brasil continuou a desempenhar funções governamentais, incluindo o controle das operações de comércio exterior e a execução de operações de câmbio. O Tesouro Nacional, por sua vez, atuava como órgão emissor de papel-moeda (BANCO CENTRAL DO BRASIL, 2023).

Em dezembro de 1964, a Lei nº 4.595 criou o Banco Central do Brasil, que se tornou uma autarquia federal integrante do SFN. O Banco Central iniciou suas atividades em março de 1965, conforme o estabelecido no artigo 65 da mesma lei. Após sua criação, foram implementados mecanismos que permitiram ao BC desempenhar efetivamente seu papel de "banco dos bancos". Em 1985, ocorreu um reordenamento financeiro governamental que separou as funções do Banco Central, Banco do Brasil e Tesouro Nacional. Essa

reestruturação culminou em 1988, quando as funções de autoridade monetária foram progressivamente transferidas do Banco do Brasil para o Banco Central, enquanto atividades atípicas desse último foram transferidas para o Tesouro Nacional (BANCO CENTRAL DO BRASIL, 2023).

A Constituição Federal de 1988 trouxe avanços significativos para a atuação do Banco Central, conferindo à União a competência exclusiva para emitir moeda e estabelecendo a necessidade de aprovação prévia pelo Senado Federal para a nomeação do presidente e diretores do BC. Além disso, a Constituição proibiu a concessão de empréstimos diretos ou indiretos ao Tesouro Nacional, visando garantir a independência da autoridade monetária. O artigo 192 da Constituição previu a elaboração de uma Lei Complementar que substituísse a Lei nº 4.595/64, reestruturando as atribuições do Banco Central e aprimorando seu funcionamento (BANCO CENTRAL DO BRASIL, 2023).

O BC é uma autarquia de natureza especial, criado pela Lei nº 4.595/1964 e com autonomia estabelecida pela Lei Complementar nº 179/2021. Para manter a inflação sob controle, o BC executa a estratégia estabelecida pelo CMN, órgão responsável por elaborar as políticas de moeda e de crédito no país. Criado em 1964, pela mesma lei que criou o Banco Central, o CMN é composto pelo ministro da Fazenda, que o preside; o presidente do BC; e o ministro do Planejamento e Orçamento (BANCO CENTRAL DO BRASIL, 2024). As tarefas a cargo do BC são:

Quadro 3 - Tarefas a cargo do Banco Central do Brasil

Inflação baixa e estável	Manter a inflação sob controle, ao redor da meta, é objetivo fundamental do BC. A estabilidade dos preços preserva o valor do dinheiro, mantendo o poder de compra da moeda. Para alcançar esse objetivo, o BC utiliza a política monetária, política que se refere às ações do BC que visam afetar o custo do dinheiro (taxas de juros) e a quantidade de dinheiro (condições de liquidez) na economia.
Sistema financeiro seguro e eficiente	Faz parte da missão do BC assegurar que o sistema financeiro seja sólido (tenha capital suficiente para arcar com seus compromissos) e eficiente.
Banco do governo	O BC detém as contas mais importantes do governo e é o depositório das reservas internacionais do país.
Banco dos bancos	As instituições financeiras precisam manter contas no BC. Essas contas são monitoradas para que as transações financeiras aconteçam com fluidez e para

	que as próprias contas não fechem o dia com saldo negativo.
Emissor do dinheiro	O BC gerencia o meio circulante, que nada mais é do que garantir, para a população, o fornecimento adequado de dinheiro em espécie.

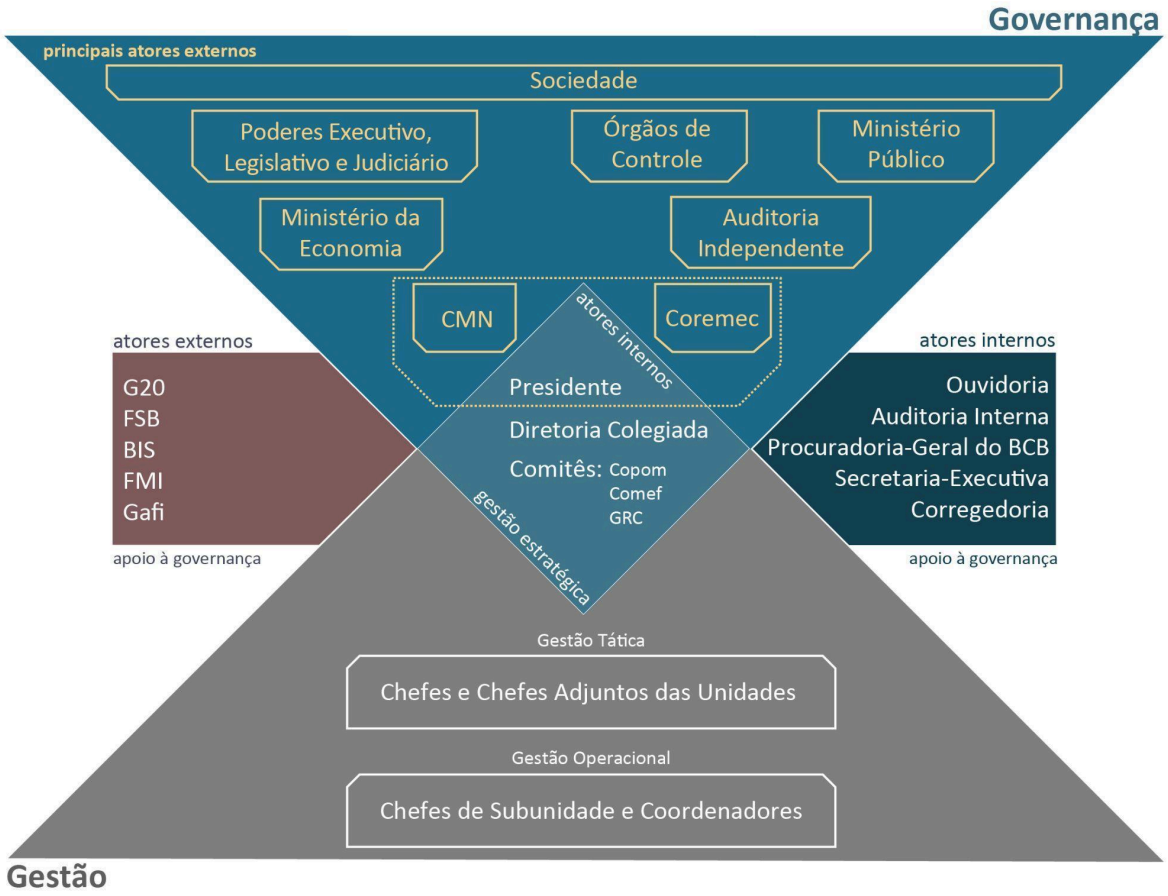
Fonte: Banco central do Brasil (2024)

No que se refere a estrutura de governança, o BC é dirigido por seu presidente e seus diretores, que compõem a Diretoria Colegiada, todos indicados pelo presidente da República e aprovados pelo Senado Federal. Além da Diretoria Colegiada, a estrutura de governança do BC é composta pelos seguintes comitês:

- Comitê de Política Monetária (Copom): reúne-se, ordinariamente, oito vezes por ano para definir a meta para a taxa básica de juros da economia – a Selic. Também divulga, trimestralmente, o Relatório de Inflação. Os comunicados das decisões, as atas das reuniões e as apresentações técnicas são publicadas na página do BC na internet, sendo as últimas reservadas por período de quatro a oito anos.
- Comitê de Estabilidade Financeira (Comef): estabelece diretrizes para manutenção da estabilidade financeira e prevenção da materialização do risco sistêmico – o risco de ocorrência de interrupção de serviços financeiros essenciais às famílias e às empresas que prejudique significativamente a economia brasileira.
- Comitê de Governança, Riscos e Controles (GRC): define diretrizes e estratégias relativas à governança corporativa e à gestão de riscos e controles internos, e adota medidas para a sistematização de práticas nessas áreas.

A estrutura de governança é complementada por atores externos e por instâncias internas de apoio à governança, como a Auditoria Interna, Ouvidoria, Corregedoria, Procuradoria-Geral e Secretaria-Executiva, conforme descrito na figura abaixo:

Figura 4 - Estrutura de governança do Banco Central do Brasil



Fonte: Banco central do Brasil, 2024

Além da própria sociedade, os principais atores externos que contribuem, orientam, cobram e fiscalizam a governança do BC são a auditoria independente, o Conselho Monetário Nacional (CMN), o Ministério da Economia, o Conselho de Recursos do Sistema Financeiro Nacional (CRSFN), o Ministério Público Federal (MPF), a Controladoria-Geral da União (CGU) e o Tribunal de Contas da União (TCU).

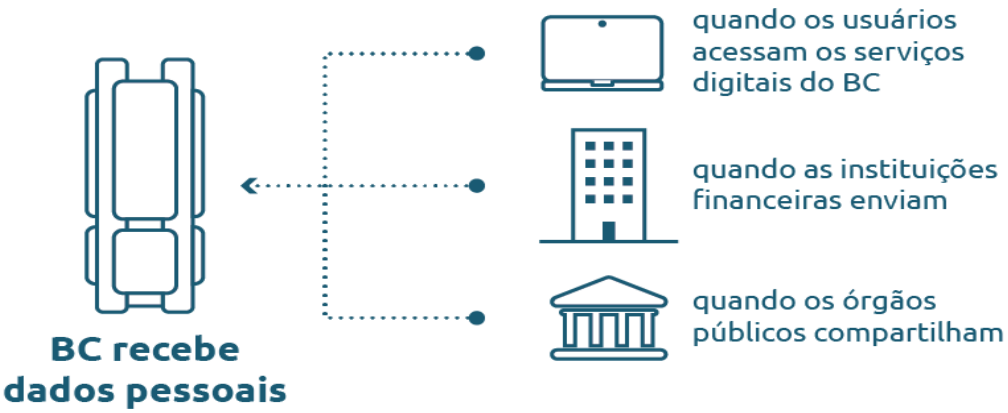
O BC também compartilha experiências e segue recomendações de governança de vários organismos internacionais, com destaque para o Banco de Compensações Internacionais (BIS), G-20, o Conselho de Estabilidade Financeira (FSB), o Fundo Monetário Internacional (FMI) e o Grupo de Ação Financeira (GAFI).

No que se refere à proteção de dados, o BC atua com base na LGPD. O BC, no âmbito das suas competências, trabalha com dados pessoais de diversos tipos e naturezas para desenvolver suas atividades. No Banco Central, os dados são usados principalmente para: executar políticas públicas previstas em leis e regulamentos ou permitidas em contratos, convênios ou instrumentos similares; cumprir alguma norma; avaliar os serviços, identificar

problemas, melhorar a segurança e a navegação nas páginas, aplicativos e serviços digitais; e dar proteção ao crédito.

O tratamento de dados pessoais realizados pelo Banco Central acontece da seguinte forma:

Figura 5 - Recebimento de dados pessoais pelo BC



Fonte: Banco central do Brasil, 2024

Figura 6 - Tratamento de dados pessoais pelo BC

Fonte: Banco central do Brasil, 2024

A partir destes, o BC adotou algumas medidas de segurança, conforme descrito na Figura 7.

Figura 7 - Medidas de segurança adotadas pelo BC

Fonte: Banco central do Brasil, 2024

Com base na LGPD, o BC adota ações para fortalecer os controles e os sistemas de proteção de dados, os quais são apresentados em um Relatório de Impacto à Proteção de Dados Pessoais. A Política de Conformidade (Compliance) do Banco Central do Brasil (PCO-BC) tem entre seus objetivos assegurar que as atividades do Banco Central do Brasil (BC) sejam conduzidas em conformidade com as normas aplicáveis à Instituição, sob a coordenação do Departamento de Riscos Corporativos e Referências Operacionais (Deris). Nesse sentido, de acordo com o art. 38, caput, da Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), a qualquer momento a Autoridade de Proteção de Dados Pessoais (ANPD) pode determinar ao BC que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis.

No que se refere às políticas normativas de segurança digital, o BC se orienta principalmente pela resolução BCB n° 85 de 8/4/2021, na qual:

> 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 de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil. (Redação dada, a partir de 1º/3/2024, pela Resolução BCB nº 368, de 25/1/2024.)

Essa resolução atualizada, apresenta sobre a implementação e divulgação da Política de Segurança Cibernética e Plano de Ação e de Resposta a Incidentes do BC, além de dispor sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Além dessa resolução principal, o BC dispõe de várias resoluções e instruções normativas que abordam elementos relativos à segurança digital.

Sendo assim, é importante discutir como essa estrutura do sistema de varejo financeiro nacional tem operado a partir das diretrizes de regulamentação institucionalizadas pelo Banco Central do Brasil no sentido tanto de compreender a adequação às normas de proteção de dados e segurança digital, assim como avaliar os efeitos desse processo para os consumidores de produtos financeiros em nosso país. Para tanto, na próxima seção deste trabalho será apresentado como o estudo foi realizado para responder essa questão.

Por fim, o quadro 4 apresenta uma síntese dos principais conceitos apresentados nesta seção.

Quadro 4 - Síntese dos principais conceitos da seção 3.3

Conceito-chave	Autor(es)	Definição / Ideia central	Contribuição para o estudo
Sistema Financeiro Nacional (SFN)	Assaf Neto (2021); Lei nº 4.595/1964	Conjunto integrado de instituições, normas e instrumentos responsáveis pela intermediação financeira, organização do crédito e execução das políticas monetária, fiscal e cambial.	Delimita o campo institucional no qual se inserem as práticas regulatórias e organizacionais analisadas no estudo.
Estrutura institucional do SFN	Banco Central do Brasil (2025)	Organização do SFN em três níveis: órgãos normativos, entidades supervisoras e operadores financeiros.	Permite compreender a posição estratégica do Banco Central como elo entre normatização e prática organizacional.
Sistema de Varejo Financeiro	Banco Central do Brasil (2025)	Segmento do SFN voltado a serviços financeiros de massa, com alto volume de transações de baixo valor destinadas a pessoas físicas e MPEs.	Delimita empiricamente o setor onde a coleta e o tratamento de dados pessoais são mais intensos.

Transformação digital do varejo financeiro	BC (2021); Fiserv (2022)	Digitalização acelerada de serviços financeiros, com uso intensivo de plataformas digitais, pagamentos instantâneos e automação.	Contextualiza o aumento da superfície de exposição a riscos cibernéticos.
Banco Central do Brasil (BC)	Lei nº 4.595/1964; LC nº 179/2021	Autoridade monetária com autonomia técnica, operacional e administrativa.	Posiciona o BC como ator central da governança da segurança digital no setor financeiro.

Fonte: Elaborado pela autora

4. PROCEDIMENTOS METODOLÓGICOS

Esse estudo, de natureza qualitativa, tem como objetivo **compreender como as medidas de proteção de dados do Banco Central buscam mitigar os riscos de segurança digital no setor de varejo financeiro brasileiro.** A opção por uma abordagem qualitativa deve-se ao fato de que ela permite captar a complexidade dos fenômenos sociais a partir das perspectivas dos indivíduos, valorizando a interpretação de significados e experiências (Creswell, 2007). Tal metodologia recorre a técnicas como entrevistas, observações e análise documental, possibilitando a coleta de informações em ambientes naturais e a investigação aprofundada das interações sociais e de seus contextos.

O método de coleta de dados utilizado neste estudo foi a pesquisa documental. Adotou-se aqui a perspectiva de Hodder (2012), na qual os documentos podem ser considerados artefatos a medida em que são produtos culturais que carregam significados e refletem as práticas sociais de seu tempo. Ele argumenta que, ao tratar os documentos como artefatos, é possível explorar não apenas o seu conteúdo, mas também sua forma, contexto de produção e as relações de poder que eles representam (Hodder, 2012).

Para Hodder (2012), a pesquisa documental envolve a análise de textos, artefatos e outros registros que permitem explorar as complexas relações que se formam entre seres humanos e as coisas que os cercam. Ele enfatiza a importância de considerar o contexto social, cultural e histórico desses documentos, ressaltando que a interpretação deve levar em conta as práticas e significados atribuídos aos objetos em diferentes sociedades (Hodder, 2012).

Assim, a pesquisa documental não é apenas uma busca por informações, mas um processo de entendimento das dinâmicas entre sujeitos e objetos, revelando como essas interações moldam a experiência humana e as narrativas culturais (Hodder, 2012). Essa

abordagem holística, enriquece a pesquisa documental ao incentivar uma reflexão crítica sobre como entende-se a produção de conhecimento e a construção da história.

Essa abordagem permite a análise de uma variedade de documentos relevantes, como legislações, políticas institucionais, relatórios e estudos de caso, que podem revelar como as legislações brasileiras foram incorporadas no SFN, reguladas pelo BC e incorporada nas práticas e normas do setor de varejo financeiro no Brasil. Ao considerar não apenas os textos legais, mas também as interações entre diferentes agentes sociais, a pesquisa documental possibilita entender as dinâmicas entre a convenção e as respostas dos diversos stakeholders, como instituições financeiras, reguladores e consumidores.

Além disso, a ênfase de Hodder (2012) na interpretação contextualizada dos documentos ajuda a captar as particularidades culturais e sociais do Brasil, permitindo uma análise mais rica das adaptações locais às diretrizes internacionais. Essa perspectiva também promove uma reflexão crítica sobre como as políticas de segurança digital estão sendo moldadas não apenas por influências externas, mas também pelas especificidades do contexto brasileiro, como a vulnerabilidade a ciberataques e as diferenças no nível de conscientização sobre segurança digital.

Assim, a pesquisa documental, ao integrar diferentes fontes e contextos, oferece uma compreensão abrangente e detalhada dos impactos das medidas de proteção de dados tomadas pelo governo brasileiro após a Constituição de 1988 e medidas de mitigação de risco implementadas BC, enquanto órgão que regulamenta as práticas de transações do varejo financeiro, permitindo identificar não apenas os efeitos diretos nas políticas de segurança digital, mas também as interações complexas que permeiam esse processo no setor do varejo financeiro no Brasil.

Nesse sentido, o corpus de análise foi composto por dois conjuntos de elementos, 1) os documentos que regulamentam as políticas de segurança digital no campo do varejo financeiro no Brasil, como legislações específicas instituídas no Brasil, 2) além das normas e relatórios do Banco Central do Brasil, que desempenha um papel fundamental na regulamentação e supervisão do mercado financeiro brasileiro, garantindo a estabilidade econômica e a proteção dos consumidores. Utilizar as legislações brasileiras e documentos e relatórios do BC como corpus de análise permite uma compreensão detalhada e baseada em evidências de como a regulamentação e as políticas evoluem e como isso influencia o setor financeiro de varejo no Brasil.

Inicialmente, a coleta de dados nas legislações brasileiras foi realizada com base na linha do tempo das normas relacionadas à proteção de dados e à segurança digital no Brasil

(Figura 1). Cada uma dessas legislações foi acessada individualmente para a realização das buscas. Foram definidos cinco termos-chave com o objetivo de identificar trechos que abordassem especificamente essa temática. Considerando que a terminologia pode variar entre as diferentes legislações, também foram incluídos termos semelhantes nas buscas, conforme segue:

1. Banco Central - Banco.
2. Crime Cibernético - Crimes Cibernéticos - Crimes Informáticos - Cibercrime - Crime Digital - Infração Cibernética - Delitos Informáticos - Crimes de Violação de Dispositivo Informático.
3. Proteção de dados - Proteção dos dados, Proteção a dados, Proteção de seus dados, Dados.
4. Segurança Digital - Digital, Digitais.
5. Soberania digital

Após a definição dos termos, procedeu-se à realização das buscas correspondentes, cujos resultados foram sistematizados em um quadro, conforme apresentado no Anexo 1. O Quadro 5 apresenta uma síntese quantitativa dos resultados obtidos.

Quadro 5 - Resultados da busca dos termos chave nas regulamentações brasileiras

REGULAMENTAÇÃO	**Termos:** Banco Central	**Termos:** Crime Cibernético	**Termos:** Proteção de dados	**Termos:** Segurança Digital	**Termos:** Soberania Digital
Constituição Federal de 1988	17 resultados	-	10 resultados	2 resultados	-
Lei nº 9.610 (Lei dos direitos autorais)	-	-	8 resultados	-	-
Lei nº 10.406 (Código Civil)	1 resultado	-	8 resultados	2 resultados	-
Lei nº 10.695 (Lei da Pirataria)	-	-	-	-	-
Lei Nº 10.703 (Cadastramento de usuários de telefones celulares pré-pagos)	-	-	3 resultados	-	-
Lei nº 12.737 (Lei Carolina Dieckmann)	-	2 resultados	2 resultados	-	-
Lei nº 12.965 (Marco Civil da Internet)	-	-	22 resultados	4 resultados	-
Decreto nº 8.771 (Regulamenta o Marco Civil da Internet)	-	-	20 resultados	-	-
Lei nº 13.709 (Lei Geral de	7 resultados	-	255	1 resultado	-

Proteção de Dados - LGPD)			resultados		
Estratégia Nacional de Segurança Cibernética (ENSC) (revogado)	-	-	-	-	-
Lei nº 14.010 (Lei da Pandemia)	-	-	-	-	-
Lei nº 14.129 (Lei de Governo Digital)	-	-	104 resultados		-
Lei nº 14.155	-	1 resultado	1 resultado	-	-
Decreto Nº 11.491 (Convenção sobre o Crime Cibernético)	-	11 resultados	91 resultados	1 resultado	-
Decreto Nº 12.573 (E-Ciber)	-	8 resultados	4 resultados	5 resultados	-

Fonte: elaborado pela autora a partir dos dados da pesquisa

O segundo conjunto de dados compreende as normas e regulamentações emitidas pelo Banco Central do Brasil relacionadas aos temas de proteção de dados e segurança digital. Para a obtenção desses documentos, realizou-se uma busca no portal do BC, especificamente na seção destinada à consulta de normas, conforme ilustrado na Figura 8.

Figura 8 – Interface da seção de busca de normas do portal do Banco Central do Brasil utilizada para a coleta dos dados

Fonte: Banco central do Brasil (2025)

Nesta ferramenta de busca do Banco Central do Brasil, foram empregados dois termos principais: proteção de dados e segurança digital. Para ambas as buscas, utilizaram-se

os seguintes filtros: tipo de documento — “todos”; conteúdo — “proteção de dados” na primeira busca e “segurança digital” na segunda; período — de 1º de janeiro de 1988 a 1º de outubro de 2025; e situação — “em vigor”.

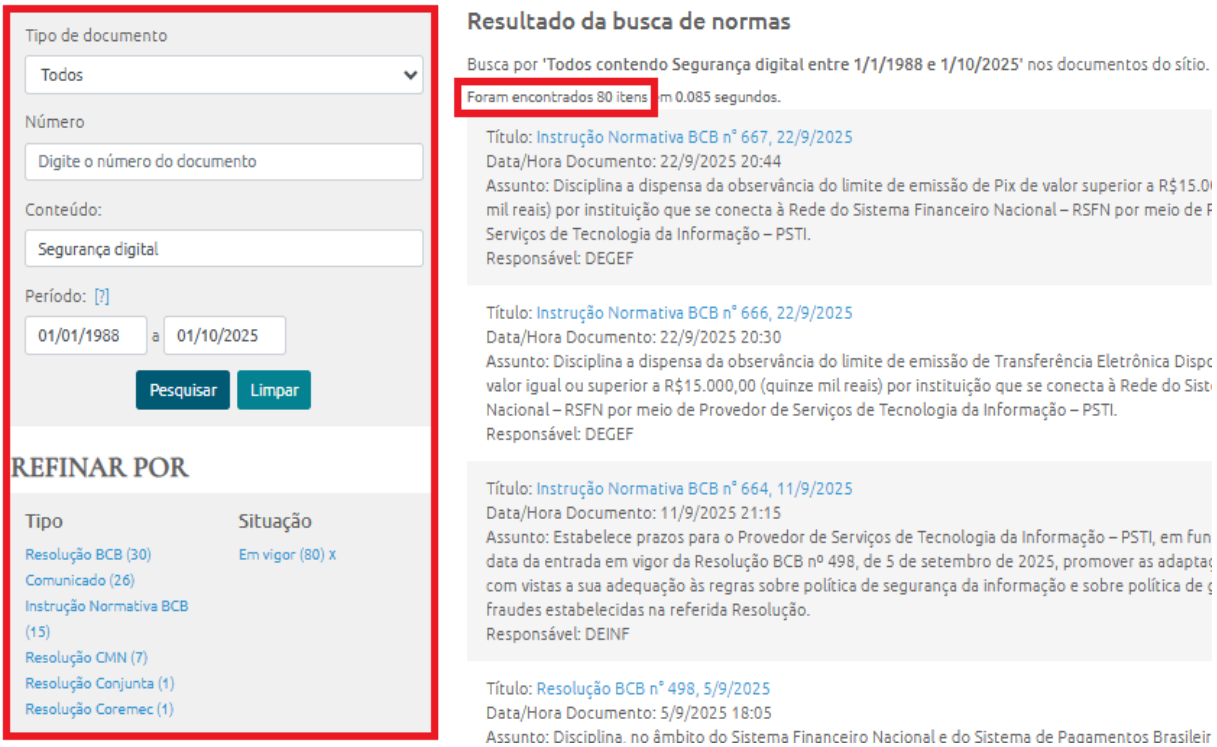
A pesquisa com o termo proteção de dados resultou em um total de 118 documentos encontrados, conforme ilustrado na Figura 9.

Figura 9 – Resultados da busca pelo termo “proteção de dados” no portal do Banco Central do Brasil

Fonte: Banco central do Brasil (2025)

Por sua vez, a busca pelo termo segurança digital resultou em um total de 80 itens encontrados, conforme ilustrado na Figura 10.

Figura 10 – Resultados da busca pelo termo “segurança digital” no portal do Banco Central do Brasil



Fonte: Banco central do Brasil (2025)

Os resultados obtidos nas duas buscas foram sistematizados em tabelas, conforme o Anexo 2. Identificaram-se 118 ocorrências para o termo “proteção de dados” e 80 para “segurança digital”. Em seguida, realizou-se um processo de filtragem, mediante a leitura integral de cada resultado, com o objetivo de identificar aqueles alinhados à temática da pesquisa. O critério de seleção considerou apenas as regulamentações com trechos diretamente relacionados à proteção de dados e à segurança digital, uma vez que, em muitos casos, os termos pesquisados apareciam nos textos das resoluções apenas de forma tangencial, sem pertinência ao escopo do estudo. Após essa análise, foram selecionados 33 resultados referentes ao termo “proteção de dados” e 24 ao termo “segurança digital”, conforme apresentado nos quadros 6 e 7.

Quadro 6 - Identificação das 33 resoluções com o termo “proteção de dados” que possuem relação com a temática estudada

Título	Data	Assunto	Respon.
Instrução Normativa BCB n° 667	22/09/25	Disciplina a dispensa da observância do limite de emissão de Pix de valor superior a R$15.000,00 por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.	DEGEF
Instrução Normativa BCB n° 666	22/09/25	Disciplina a dispensa da observância do limite de emissão de Transferência Eletrônica Disponível – TED de valor igual ou superior a R$15.000,00 (quinze mil reais) por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.	DEGEF
Instrução Normativa BCB n° 664	11/09/25	Estabelece prazos para o Provedor de Serviços de Tecnologia da Informação – PSTI, em funcionamento na data da entrada em vigor da Resolução BCB nº 498, de 5 de setembro de 2025, promover as adaptações necessárias com vistas a sua adequação às regras sobre política de segurança da informação e sobre política de gestão de fraudes estabelecidas na referida Resolução.	DEINF
Resolução BCB n° 498	05/09/25	Disciplina, no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI e dá outras providências.	DINOR, DIRAD, DIFIS, DIORF
Instrução Normativa BCB n° 637	13/06/25	Divulga a versão 8.0 do Manual de Experiência do Cliente no Open Finance.	DENOR
Resolução BCB n° 454	30/01/25	Dispõe sobre a Estratégia de Uso de Software e de Serviços de Computação em Nuvem do Banco Central do Brasil.	DIRAD
Resolução BCB n° 447	19/12/24	Altera as Circulares ns. 3.634, 3.635, 3.636, 3.637, 3.638, 3.639 e 3.641, de 4 de março de 2013, 3.809, de 25 de agosto de 2016, 3.846, de 13 de setembro de 2017, 3.861 e 3.863, de 7 de dezembro de 2017, 3.876, de 31 de janeiro de 2018, e 3.979, de 30 de janeiro de 2020, e as Resoluções BCB ns. 54, de 16 de dezembro de 2020, 111, de 6 de julho de 2021, 139, de 15 de setembro de 2021, 199, 200, 201 e 202, de 11 de março de 2022, 229, de 12 de maio de 2022, 265, de 25 de novembro de 2022, 291, de 8 de fevereiro de 2023, 303, de 16 de março de 2023, 307, de 23 de março de 2023, 313, de 26 de abril de 2023, 319, de 18 de maio de 2023, 331, de 27 de junho de 2023, e 356, de 28 de novembro de 2023, para incluir em seus escopos de aplicação as sociedades corretoras de títulos e valores mobiliários, as sociedades distribuidoras de títulos e valores mobiliários e as sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.	DINOR
Resolução BCB n° 400	04/07/24	Dispõe sobre as diretrizes para o estabelecimento da Estrutura de Governança do Open Finance.	DINOR
Resolução BCB n° 386	05/06/24	Divulga a Política de Conformidade (Compliance) do Banco Central do Brasil – PCO-BCB.	DIREX
Resolução BCB n° 368	25/01/24	Altera as Resoluções BCB ns. 28, de 23 de outubro de 2020; 65, de 26 de janeiro de 2021; 85, de 8 de abril de 2021; 93, de 6 de maio de 2021; 155, de 14 de outubro de 2021; e 260, de 22 de novembro de 2022, para incluir em seus escopos de aplicação as sociedades corretoras de títulos e valores mobiliários, as sociedades	DINOR

		distribuidoras de títulos e valores mobiliários e as sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.	
Resolução BCB n° 366	17/01/24	Divulga o Regulamento do Sistema de Informações Banco Central (Sisbacen).	DIRAD
Resolução CMN n° 5.105	28/09/23	Estabelece diretrizes mínimas para a disciplina das condições de constituição e de funcionamento, para a autorização para constituição e funcionamento e para a supervisão das atividades das sociedades corretoras de títulos e valores mobiliários, das sociedades corretoras de câmbio e das sociedades distribuidoras de títulos e valores mobiliários.	DINOR
Resolução Conjunta n° 6	23/05/23	Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.	SECRE
Resolução CMN n° 5.076	18/05/23	Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, e a Resolução nº 4.606, de 19 de outubro de 2017.	DINOR
Instrução Normativa BCB n° 374	26/04/23	Divulga procedimentos, prazos, documentos e informações necessários para a instrução de pedidos de autorização relacionados ao funcionamento dos Sistemas de Mercado Financeiro (SMF) no âmbito do Sistema de Pagamentos Brasileiro (SPB), e os tipos de alterações nos SMF e em seus regulamentos que representam risco relevante à sua segurança, à sua eficiência ou à solidez e ao normal funcionamento do SPB ou do Sistema Financeiro Nacional (SFN).	DEORF
Resolução BCB n° 304	20/03/23	Aprova o Regulamento que disciplina, no âmbito do Sistema de Pagamentos Brasileiro, o funcionamento dos sistemas de liquidação, o exercício das atividades de registro e de depósito centralizado de ativos financeiros e a constituição de ônus e gravames sobre ativos financeiros registrados ou depositados, e consolida normas sobre a matéria.	SECRE
Resolução BCB n° 287	24/01/23	Divulga a Política de Segurança da Informação do Banco Central do Brasil (PSIBC).	SECRE
Resolução BCB n° 286	24/01/23	Institui o Regulamento de Governança do Portal de Internet do Banco Central do Brasil.	SECRE
Resolução BCB n° 265	25/11/22	Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de conglomerado prudencial classificado como Tipo 3 enquadrado nos Segmento 2 (S2), 3 (S3) ou 4 (S4).	SECRE
Resolução BCB n° 250	05/10/22	Divulga o novo Regulamento do Comitê de Governança da Informação (CGI).	SECRE
Resolução BCB n° 249	05/10/22	Divulga a Política de Governança da Informação do Banco Central do Brasil.	SECRE
Instrução Normativa BCB n° 305	15/09/22	Divulga a versão 4.0 do Manual de Segurança do Open Finance.	DENOR
Resolução BCB n° 204	22/03/22	Dispõe sobre o compartilhamento de dados de operações registradas no Sistema de Operações do Crédito Rural e do Proagro (Sicor).	SECRE
Resolução BCB n° 201	11/03/22	Dispõe sobre a metodologia facultativa simplificada para apuração do requerimento mínimo de Patrimônio de Referência Simplificado (PRS5) para os conglomerados prudenciais classificados como do Tipo 3, sobre os requisitos para opção por essa metodologia e sobre a estrutura simplificada de gerenciamento contínuo de riscos.	SECRE

Resolução BCB n° 198	11/03/22	Dispõe sobre o requerimento mínimo de Patrimônio de Referência de Instituição de Pagamento (PRIP) de conglomerado do Tipo 2, nos termos da Resolução BCB nº 197, de 11 de março de 2022, e de instituição de pagamento não integrante de conglomerado prudencial, e sobre a metodologia de apuração desses requerimentos e a respectiva estrutura de gerenciamento contínuo de riscos.	SECRE
Resolução BCB n° 85	08/04/21	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 de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.	SECRE
Resolução CMN n° 4.893	26/02/21	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 autorizadas a funcionar pelo Banco Central do Brasil.	SECRE
Resolução Conjunta n° 1	04/05/20	Dispõe sobre a implementação do Open Finance.	-
Circular n° 3.970	28/11/19	Estabelece os critérios gerais de comunicação eletrônica de dados no âmbito do Sistema Financeiro Nacional (SFN), dispõe sobre os requisitos e as vedações aplicáveis ao Provedor de Serviços de Tecnologia da Informação (PSTI) e dá outras providências.	SECRE
Circular n° 3.909	16/08/18	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 de pagamento autorizadas a funcionar pelo Banco Central do Brasil.	SECRE
Resolução CMN n° 4.606	19/10/17	Dispõe sobre a metodologia facultativa simplificada para apuração do requerimento mínimo de Patrimônio de Referência Simplificado (PRS5), os requisitos para opção por essa metodologia e os requisitos adicionais para a estrutura simplificada de gerenciamento contínuo de riscos.	SECRE
Resolução CMN n° 4.557	23/02/17	Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.	SECRE
Resolução CMN n° 4.282	04/11/13	Estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), de que trata a Lei nº 12.865, de 9 de outubro de 2013.	SECRE

Fonte: elaborado pela autora a partir dos dados da pesquisa

Quadro 7 - Identificação das 24 resoluções com o termo “segurança digital” que possuem relação com a temática estudada

Título	Data	Assunto	Respon.
Instrução Normativa BCB n° 667	22/09/25	Disciplina a dispensa da observância do limite de emissão de Pix de valor superior a R$15.000,00 por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.	DEGEF
Instrução Normativa BCB n° 666	22/09/25	Disciplina a dispensa da observância do limite de emissão de Transferência Eletrônica Disponível – TED de valor igual ou superior a R$15.000,00 (quinze mil reais) por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.	DEGEF
Instrução Normativa BCB n° 664	11/09/25	Estabelece prazos para o Provedor de Serviços de Tecnologia da Informação – PSTI, em funcionamento na data da entrada em vigor da Resolução BCB nº 498, de 5 de setembro de 2025, promover as adaptações necessárias com vistas a sua adequação às regras sobre política de segurança da informação e sobre política de gestão de fraudes estabelecidas na referida Resolução.	DEINF
Resolução BCB n° 498	05/09/25	Disciplina, no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI e dá outras providências.	DINOR, DIRAD, DIFIS, DIORF
Instrução Normativa BCB n° 633	05/06/25	Divulga a versão 3.7 do Manual de Segurança do Pix, que compõe o Regulamento do Pix.	DECEM
Resolução BCB n° 481	04/06/25	Institui o Posto de Controle do Banco Central do Brasil – PCBC, para armazenamento de informações classificadas em grau de sigilo e acesso a essas informações, e aprova o seu regulamento.	PRESI
Resolução BCB n° 454	30/01/25	Dispõe sobre a Estratégia de Uso de Software e de Serviços de Computação em Nuvem do Banco Central do Brasil.	DIRAD
Resolução BCB n° 366	17/01/24	Divulga o Regulamento do Sistema de Informações Banco Central (Sisbacen).	DIRAD
Resolução BCB n° 340	21/09/23	Divulga o novo Regimento Interno do Banco Central do Brasil.	DIRAD
Resolução CMN n° 5.076	18/05/23	Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, e a Resolução nº 4.606, de 19 de outubro de 2017.	DINOR
Resolução BCB n° 304	20/03/23	Aprova o Regulamento que disciplina, no âmbito do Sistema de Pagamentos Brasileiro, o funcionamento dos sistemas de liquidação, o exercício das atividades de registro e de depósito centralizado de ativos financeiros e a constituição de ônus e gravames sobre ativos financeiros registrados ou depositados, e consolida normas sobre a matéria.	SECRE
Resolução BCB n° 287	24/01/23	Divulga a Política de Segurança da Informação do Banco Central do Brasil (PSIBC).	SECRE
Resolução BCB n° 265	25/11/22	Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de conglomerado prudencial classificado como Tipo 3 enquadrado nos Segmento 2 (S2), 3 (S3) ou 4 (S4).	SECRE
Resolução BCB	05/10/22	Divulga a Política de Governança da Informação do Banco Central	SECRE

n° 249		do Brasil.	
Instrução Normativa BCB n° 305	15/09/22	Divulga a versão 4.0 do Manual de Segurança do Open Finance.	DENOR
Comunicado n° 39.153	15/09/22	Comunica a descontinuidade do procedimento de validação de credenciamento de acesso ao Extrato do Registro de Informações no Banco Central do Brasil (Sistema Registrato) por aplicativo de instituições financeiras.	DEATI
Resolução BCB n° 150	06/10/21	Consolida normas sobre os arranjos de pagamento, aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências.	SECRE
Resolução BCB n° 124	05/08/21	Institui procedimentos para acesso de entes públicos ao Cadastro de Clientes do Sistema Financeiro Nacional (CCS) e divulga Regulamento para adesão dos interessados.	SECRE
Comunicado n° 37.320	25/06/21	Comunica publicação de nova versão do Manual de Segurança do SFN e divulga procedimentos e prazos para a implantação da nova versão do protocolo de segurança das mensagens e dos arquivos do Catálogo de Serviços do SFN que trafegam na Rede do Sistema Financeiro Nacional (RSFN).	DEINF
Resolução BCB n° 1	12/08/20	Institui o arranjo de pagamentos Pix e aprova o seu Regulamento.	SECRE
Resolução Conjunta n° 1	04/05/20	Dispõe sobre a implementação do Open Finance.	-
Resolução CMN n° 4.474	31/03/16	Dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil, bem como sobre o procedimento de descarte das matrizes físicas dos documentos digitalizados e armazenados eletronicamente.	SECRE
Comunicado n° 18.655	02/07/09	Divulga nova versão do Regulamento do Grupo Técnico de Segurança da Rede do Sistema Financeiro Nacional.	DEINF
Comunicado n° 10.193	03/10/02	Divulga o regulamento do Grupo Técnico de Segurança do Sistema de Pagamentos Brasileiro.	DEINF

Fonte: elaborado pela autora a partir dos dados da pesquisa

Em seguida, para a etapa de realização das análises, adotou-se a técnica interpretativa. Segundo Minayo (1996), essa abordagem busca compreender o significado atribuído pelos sujeitos aos dados produzidos em pesquisas sociais, enfatizando a interpretação das experiências, percepções e práticas. Trata-se de um procedimento que ultrapassa a mera descrição dos fatos, voltando-se à construção de significados e à contextualização das informações dentro dos universos socioculturais investigados.

A autora ainda destaca que a análise interpretativa é fundamental para captar as nuances das interações sociais, permitindo ao pesquisador identificar padrões, relações e sentidos subjetivos que atravessam os comportamentos e práticas sociais. O processo exige

uma leitura cuidadosa do material empírico, orientada para apreender as intenções, significados e racionalidades que os participantes atribuem às suas vivências (Minayo, 1996).

Essa técnica mostra-se especialmente pertinente em pesquisas qualitativas, como o estudo aqui desenvolvido, nas quais a complexidade das experiências humanas requer uma abordagem aprofundada e reflexiva. A análise interpretativa favorece uma compreensão mais ampla e densa dos fenômenos investigados, ao possibilitar a identificação da dinâmica social e dos contextos que conformam as realidades dos indivíduos (Minayo, 1996).

A etapa analítica desta pesquisa foi estruturada de acordo com os dois recortes centrais que compõem o objetivo do estudo. O primeiro eixo consiste na identificação de como a proteção de dados e a segurança digital foram sendo construídas e regulamentadas nas legislações brasileiras, análise desenvolvida na seção 5.1. Nesse eixo, buscou-se compreender a evolução normativa, os princípios consolidados, as exigências legais e a forma como o ordenamento jurídico passou a incorporar, de maneira crescente, mecanismos de proteção informacional como parte da governança estatal e da tutela dos direitos fundamentais.

O segundo eixo analítico, aprofundado na seção 5.2, concentra-se nas resoluções do Banco Central do Brasil relacionadas à proteção de dados e à segurança digital. Nessa etapa, examinaram-se não apenas o alinhamento dessas normativas às legislações brasileiras — em especial a LGPD e demais diretrizes nacionais de segurança cibernética —, mas também a forma como o Banco Central estrutura seus requisitos regulatórios, como operacionaliza a proteção de dados no âmbito do Sistema de Pagamentos e do setor de varejo financeiro, e se tais medidas efetivamente contribuem para mitigar riscos de segurança digital. Além disso, analisou-se como essas normativas dialogam com os conceitos de soberania digital e capitalismo de vigilância, evidenciando tensões, limites e potencialidades dentro da regulação financeira.

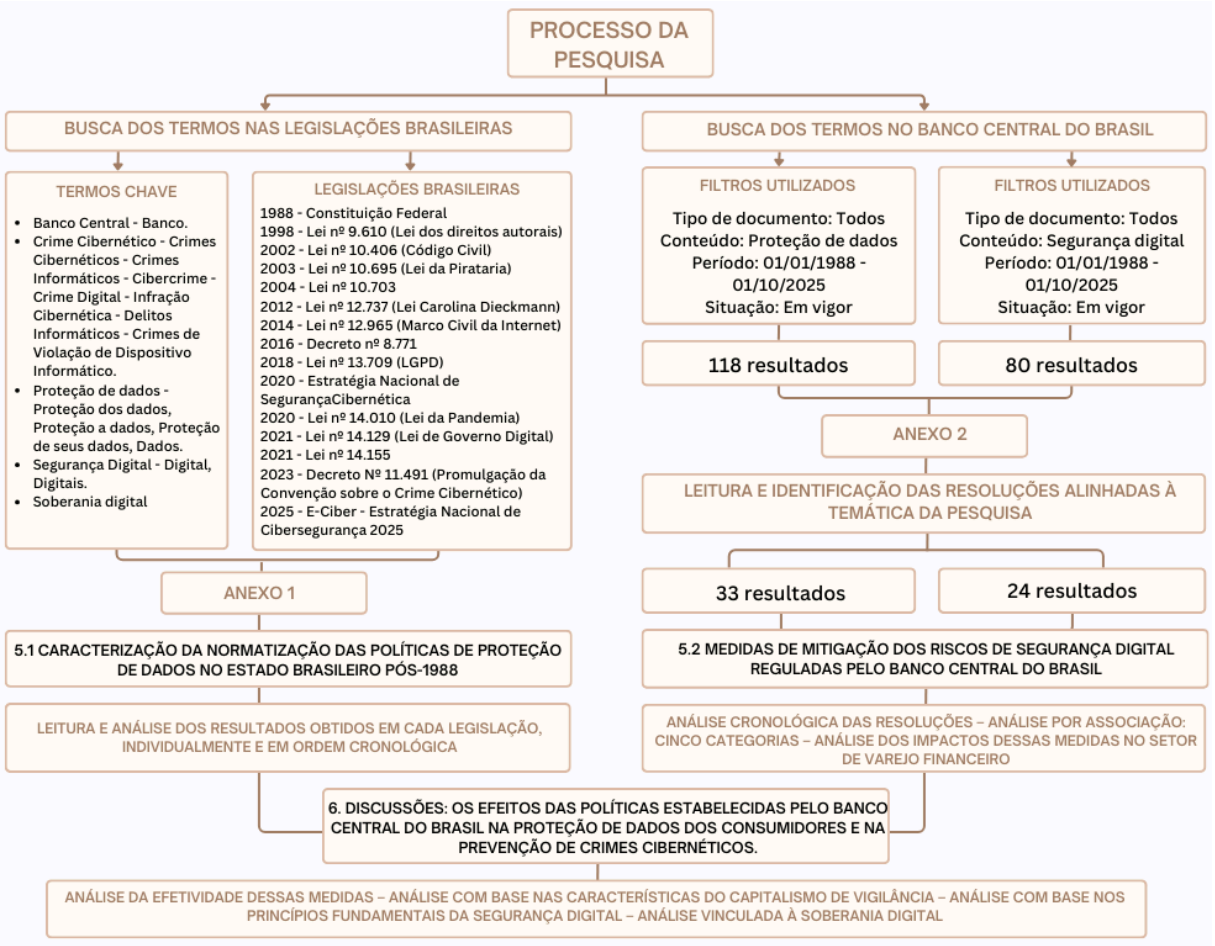
Por fim, as análises dos dois eixos foram integradas na etapa de discussão dos resultados, apresentada na seção 6. Essa integração permitiu comparar os padrões normativos gerais com a implementação específica realizada pelo Banco Central, identificar convergências e lacunas e avaliar, de forma mais ampla, em que medida a proteção de dados prevista em lei se traduz — ou não — em segurança digital efetiva no contexto do setor de varejo financeiro brasileiro. Essa abordagem articulada oferece uma compreensão mais robusta do fenômeno e sustenta as conclusões apresentadas no capítulo final da dissertação.

A partir desses elementos, buscou-se também identificar como as principais características do capitalismo de vigilância, pensando como elemento teórico deste estudo, — tais como coleta massiva de dados, predição e manipulação de comportamentos, economia da

atenção, desigualdades e exclusões, invisibilidade dos processos de coleta, colonialismo de dados, soberania digital e segurança cibernética — têm sido operacionalizadas no sistema de varejo financeiro brasileiro, sobretudo em decorrência da adequação das normas nacionais aplicadas e fiscalizadas pelo Banco Central do Brasil.

Nesse sentido, a figura 11 apresenta o processo metodológico da pesquisa de modo sintetizado.

Figura 11 - Processo metodológico da pesquisa



Fonte: Elaborado pela autora.

5. RESULTADOS DA PESQUISA

Os resultados e discussões da pesquisa foram organizados em três seções, cada uma estruturada para responder a um dos objetivos específicos do estudo. A seção 5.1, denominada "Caracterização da normatização das políticas de proteção de dados no Estado brasileiro pós-1988", buscou atender o primeiro objetivo específico: Caracterizar como as políticas de

proteção de dados e segurança digital estão normatizadas pelo estado brasileiro pós constituição de 1988. A seção 5.2, intitulada “medidas de mitigação dos riscos de segurança digital reguladas pelo Banco Central do Brasil”, foi dedicada ao segundo objetivo específico: Identificar como o Banco Central do Brasil tem ajustado suas políticas para atender às diretrizes nacionais instituídas para a proteção de dados e prevenção de crimes cibernéticos. Por fim, a seção 6, denominada “Discussões: os efeitos das políticas estabelecidas pelo Banco Central do Brasil na proteção de dados dos consumidores e na prevenção de crimes cibernéticos.”, foi desenvolvida para atender o terceiro objetivo específico do estudo: Compreender os efeitos dessas políticas estabelecidas pelo Banco Central do Brasil na prevenção de crimes cibernéticos e na proteção de dados dos consumidores.

5.1 CARACTERIZAÇÃO DA NORMATIZAÇÃO DAS POLÍTICAS DE PROTEÇÃO DE DADOS NO ESTADO BRASILEIRO PÓS-1988

A normatização da proteção de dados no Brasil, a partir da Constituição de 1988, revela um movimento histórico marcado pela crescente digitalização da vida social, econômica e política, pela expansão do papel do Estado regulador e, simultaneamente, pela intensificação das dinâmicas de vigilância descritas por Shoshana Zuboff no conceito de capitalismo de vigilância (Zuboff, 2020). A consolidação das políticas de proteção de dados no Estado brasileiro se desenvolveu de forma gradual, e buscou se consolidar progressivamente, à medida que legislações setoriais e gerais foram sendo promulgadas, cada uma respondendo a transformações tecnológicas, econômicas e institucionais específicas. Nesse percurso, ganhou destaque o papel do setor financeiro e, em especial, o do Banco Central do Brasil, cujas regulações sobre segurança digital e proteção de dados anteciparam muitas das tendências posteriormente consagradas pela legislação geral, como a Lei Geral de Proteção de Dados (LGPD).

No marco constitucional de 1988, a proteção dos dados aparece de forma indireta, ancorada no conjunto de direitos fundamentais relacionados à privacidade, intimidade e sigilo. O artigo 5º da Constituição estabelece, por exemplo, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”, e garante também “o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas” (BRASIL, 1988, art. 5º, X e XII). O constituinte de 1988 não poderia prever que, décadas depois, a maior parte da

vida cotidiana — relações sociais, consumo, deslocamentos, compromissos financeiros e até preferências subjetivas — seria mediada digitalmente.

Embora não trate de "dados pessoais" nos termos contemporâneos, a Constituição fornece o fundamento jurídico que permitiu que legislações posteriores desenvolvessem proteção específica para informações digitais, especialmente no contexto de sistemas informatizados, redes eletrônicas e bancos de dados governamentais e privados. A lógica constitucional de defesa da dignidade da pessoa humana estabelece, portanto, o alicerce para as interpretações modernas de proteção informacional.

No entanto, a própria Constituição de 1988 já contém elementos que tensionam o princípio da privacidade, especialmente quando se observa o papel do sistema financeiro. O sigilo bancário, por exemplo, previsto no art. 5º, XII, como forma de proteção das comunicações telemáticas, é relativizado por leis complementares posteriores que autorizam o compartilhamento de informações financeiras com órgãos de fiscalização. Esse ponto revela a primeira ambiguidade: o mesmo Estado que protege a privacidade também cria dispositivos para acessar e monitorar informações sensíveis — especialmente financeiras — quando necessário. Esse movimento seria ampliado ao longo das décadas seguintes.

Nos anos 1990 e início dos anos 2000, o arcabouço normativo se concentrou em legislações setoriais que tangenciavam o tema digital, especialmente no campo das telecomunicações e dos serviços bancários. Normas que mencionavam termos como "dados", "digitais" ou "informáticos" estavam majoritariamente associadas à regulação técnica ou operacional, não à proteção jurídico-institucional da informação. Esse período revela um estágio inicial em que a digitalização era percebida mais como infraestrutura do que como fenômeno jurídico próprio.

O Código Civil de 2002 introduziu elementos para a proteção jurídica de informações pessoais. O artigo 21 estabelece que "a vida privada da pessoa natural é inviolável" (BRASIL, 2002, art. 21) e que o juiz tomará medidas para impedir ou fazer cessar atos contrários a esse direito. Embora não trate de dados digitais, o Código Civil reforça a necessidade de salvaguarda de elementos vinculados à identidade pessoal, ao mesmo tempo em que oferece instrumentos de responsabilização civil para danos causados por uso indevido de informações. Esse fundamento foi essencial, nos anos subsequentes, para litígios envolvendo vazamento de dados, exposição indevida nas redes sociais e práticas abusivas de empresas que coletam informações de consumidores — práticas estas que se tornariam centrais no capitalismo de vigilância descrito por Zuboff, no qual dados pessoais são apropriados como matéria-prima para fins econômicos (Zuboff, 2020).

A Lei nº 10.695/2003, conhecida como Lei da Pirataria, foi um dos primeiros diplomas legais a prever mecanismos de proteção para conteúdos digitais pirateados e softwares distribuídos ilegalmente. Contudo, a abordagem continua restrita à proteção de bens intelectuais, e não à proteção dos indivíduos enquanto sujeitos de dados. A legislação desse período revela um Estado preocupado com a defesa de interesses econômicos, não com a garantia de direitos informacionais. Embora não trate diretamente de dados pessoais, a lógica de criminalização da violação de sistemas digitais e da distribuição indevida de arquivos antecede discussões posteriores sobre cibersegurança, integridade de sistemas e responsabilidade por ataques cibernéticos.

Em complemento, a Lei nº 10.703/2004, ainda pouco explorada na literatura, determina a obrigatoriedade de cadastro de usuários de telefonia pré-paga, introduzindo no debate nacional a relação entre identificação do usuário, rastreabilidade e combate ao crime. Esse tipo de exigência evidencia o equilíbrio delicado entre segurança e privacidade: a criação de cadastros massivos de dados pessoais, ainda que com finalidade legítima, alimenta justamente as estruturas de vigilância que Zuboff (2020) denuncia, nas quais informações sobre cidadãos se tornam instrumentos de controle público e privado.

A partir da década de 2010, entretanto, observa-se um salto qualitativo. A análise das normas contendo expressões como “crime cibernético”, “delitos informáticos”, “proteção de dados” e “segurança digital” indica a crescente preocupação estatal com riscos digitais. A promulgação de leis voltadas à criminalização de condutas informáticas introduziram princípios e diretrizes que fortaleceram os direitos dos usuários e estabeleceram obrigações quanto à guarda, tratamento e segurança dos dados. Esse marco normativo inaugurou uma fase de maior sistematização regulatória.

O ano de 2012 é marcado pela promulgação da Lei nº 12.737, conhecida como Lei Carolina Dieckmann. A lei tipifica crimes cibernéticos e define como delito “invadir dispositivo informático alheio, conectado ou não à rede de computadores mediante violação indevida de mecanismo de segurança” (BRASIL, 2012, art. 154-A). O dispositivo amplia a proteção do indivíduo contra ataques digitais, reconhecendo a vulnerabilidade estrutural dos sistemas informatizados. A criminalização da invasão demonstra que o Estado passa a compreender o risco real associado ao ambiente digital e incorpora, no campo penal, a proteção dos dados pessoais e do sigilo das informações armazenadas em meios eletrônicos. Contudo, essa lei revela uma visão limitada dos riscos: considera crime apenas a invasão não autorizada, ignorando o fato de que a extração sistemática de dados por plataformas privadas

acontece, muitas vezes, sob a aparência de consentimento, embora o usuário raramente compreenda as implicações do ato de consentir.

Em 2014, o Marco Civil da Internet (Lei nº 12.965) inaugura uma nova fase na normatização digital brasileira. Descrito como uma "Constituição da Internet", o Marco Civil introduz princípios fundamentais para o ecossistema digital, tais como a neutralidade da rede, a proteção da privacidade e a garantia da guarda adequada de dados. O artigo 7º é emblemático ao afirmar que o usuário tem direito à "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" e à "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial" (BRASIL, 2014, art.7º). Além disso, estabelece que provedores devem manter registros de acesso sob parâmetros definidos, reforçando a necessidade de segurança na guarda de dados.

Apesar do caráter avançado, o Marco Civil ainda mantém uma estrutura de ambivalência: ao mesmo tempo que protege o usuário, também exige da provedora a guarda de registros de acesso, conforme o art. 13, por até um ano, criando uma base massiva de dados que pode ser acessada mediante ordem judicial. Esse mecanismo, embora justificado como instrumento de investigação criminal, revela como a legislação cria simultaneamente proteção e vigilância. Além disso, o Marco Civil surge em um momento em que grandes plataformas digitais já haviam consolidado métodos sofisticados de coleta de dados. Assim, seus princípios, embora avançados, já nascem em descompasso com a velocidade das transformações tecnológicas — um ponto crítico ressaltado por autores que analisam a legislação à luz da vigilância digital. No setor financeiro, essa ambivalência se torna ainda mais complexa. O sistema financeiro brasileiro já estava profundamente digitalizado no início dos anos 2000, com sistemas de pagamento eletrônicos, registros contábeis digitalizados e integração entre instituições financeiras e o Banco Central.

Contudo, aqui emerge uma crítica fundamental: apesar de se apresentar como mecanismo de proteção, a regulação do Banco Central também amplia as capacidades de monitoramento sistêmico das instituições financeiras e do próprio Estado. A crescente automatização do setor, aliada à ampliação do uso de inteligência artificial, cria ecossistemas em que consumidores têm pouca clareza sobre como seus dados financeiros — considerados sensíveis pela LGPD — são processados, analisados, compartilhados e utilizados na construção de perfis comportamentais.

Após o Marco Civil, o Decreto nº 8.771/2016 regulamenta aspectos importantes da lei, especificando obrigações técnicas e administrativas relacionadas à segurança e à proteção de

dados. O decreto estabelece diretrizes para padrões mínimos de segurança, como “controle restrito de acesso a dados pessoais” e “mecanismos de autenticação multifatorial” (BRASIL, 2016, art. 13). Essa positivação de parâmetros técnicos de segurança é essencial, especialmente para setores intensivos em dados, como o sistema financeiro. O Banco Central já possuía normativas próprias sobre segurança da informação, como a Resolução CMN nº 4.658/2018 (posteriormente atualizada), mas o Decreto 8.771/2016 fortaleceu a coerência nacional, harmonizando práticas públicas e privadas. A lógica da segurança digital aqui assume contornos claros: não basta assegurar direitos; é necessário garantir mecanismos concretos de proteção.

Em 2018, o Brasil vive um marco histórico com a aprovação da Lei nº 13.709, a Lei Geral de Proteção de Dados (LGPD). A LGPD consolida princípios sofisticados de governança de dados, inspirados no modelo europeu (GDPR) e determina a criação da Autoridade Nacional de Proteção de Dados (ANPD). Seu artigo 2º estabelece fundamentos para a disciplina da proteção de dados pessoais, entre eles: “o respeito à privacidade”, “a autodeterminação informativa”, “a inviolabilidade da intimidade, da honra e da imagem” e “os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais” (BRASIL, 2018, art. 2º). E, no art. 6º, princípios como “finalidade”, “necessidade” e “transparência” (BRASIL, 2018, art. 6º).

A lei cria obrigações claras para o tratamento de dados tanto por agentes públicos quanto privados e estabelece princípios como finalidade, adequação, necessidade e segurança, criando inclusive mecanismos como o “relatório de impacto à proteção de dados”. A segurança digital aparece como obrigação explícita: o artigo 46 determina que “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados” (BRASIL, 2018, art. 46). Pela primeira vez, proteção de dados e segurança digital se tornam políticas de Estado unificadas em uma norma de caráter geral.

Além disso, seu art. 5º, X, define dado pessoal sensível como aquele “relativo à vida financeira”, reconhecendo expressamente a vulnerabilidade das informações bancárias (BRASIL, 2018, art. 5º). Contudo, a LGPD é implementada em um contexto no qual instituições financeiras já utilizavam massivamente dados comportamentais para fins de análise de risco, personalização de ofertas e decisões de crédito automatizadas. Assim, o diploma legal, embora imprescindível, enfrenta o desafio de regular um ecossistema que já havia naturalizado práticas típicas do capitalismo de vigilância.

Essa assimetria é exatamente o que Zuboff (2020) descreve como característica do capitalismo de vigilância. Nas palavras da autora, trata-se de um regime econômico que "instrumentaliza a experiência humana como matéria-prima gratuita para tradução em dados comportamentais" (Zuboff, 2020, p. 18-19). No setor financeiro brasileiro, essa dinâmica se intensifica com o advento do PIX, das fintechs, do banco digital e, mais recentemente, com o Open Banking e o Open Finance.

Com a chegada do PIX, do Open Banking e do atual Open Finance, o sistema financeiro passa a operar sob uma lógica hiperconectada, em que dados deixam de ser apenas registros contábeis para se tornarem ativos estratégicos de competição. A promessa de empoderamento do consumidor — capaz de "portar" seus dados entre instituições — é inegavelmente ambígua. Embora o art. 4º da LGPD estabeleça o "direito à portabilidade", a capacidade real de que indivíduos compreendam, fiscalizem e controlem esses fluxos é limitada. Como afirma Zuboff, "o capitalismo de vigilância prospera exatamente sobre a incapacidade dos cidadãos de conhecer plenamente aquilo que sobre eles é conhecido" (Zuboff, 2020, p. 19). No setor financeiro, essa distância é ainda maior, dada a complexidade dos modelos algorítmicos utilizados.

Em 2020, a Estratégia Nacional de Segurança Cibernética (ENSC) amplia o repertório estatal de respostas ao risco digital. O documento reconhece que a proteção de infraestruturas críticas, a gestão de incidentes e o fortalecimento da soberania digital são essenciais para a segurança nacional. A ENSC afirma explicitamente que o Brasil deve "garantir a resiliência de sistemas essenciais e proteger dados estratégicos" (BRASIL, 2020) — linguagem que aproxima a política de cibersegurança das estruturas de governança de dados pessoais. O ano de 2020 também é marcado pela Lei nº 14.010, a chamada Lei da Pandemia, que, ao estabelecer regras temporárias para relações privadas, incluiu dispositivos sobre tratamento de dados em contexto emergencial, reconhecendo a relevância da proteção informacional em um cenário de vigilância ampliada. A pandemia evidenciou a centralidade dos dados pessoais — especialmente os dados sensíveis de saúde — como elementos de políticas públicas, abrindo espaço para discussões profundas sobre limites éticos e jurídicos da coleta massiva de informações em situações críticas.

Ainda em direção ao fortalecimento da digitalização estatal, a Lei nº 14.129/2021, conhecida como Lei de Governo Digital, estabelece diretrizes para a modernização da administração pública, com forte ênfase na transformação digital, na interoperabilidade de sistemas e na oferta digital de serviços públicos. O artigo 3º da lei estabelece princípios como a "segurança da informação, privacidade e proteção de dados" (BRASIL, 2021, art. 3º) como

elementos obrigatórios para políticas públicas digitais. A digitalização do Estado, ao mesmo tempo que amplia acesso e eficiência, também aumenta a quantidade de dados sob custódia governamental, ampliando a necessidade de salvaguardas robustas. Essa dinâmica reforça, mais uma vez, o diagnóstico de Zuboff (2020) sobre como instituições públicas e privadas passam a operar em lógicas contínuas de coleta, processamento e vigilância de dados, muitas vezes sob a justificativa de eficiência e inovação.

A Lei nº 14.155/2021 aprofunda a esfera penal relacionada aos crimes cibernéticos, tipificando condutas como fraude eletrônica e definindo penas mais severas quando cometidas por meio de dispositivos digitais. Essa legislação responde à explosão de golpes digitais, especialmente no sistema financeiro, onde fraudes bancárias, phishing e invasões de contas digitais se tornaram frequentes. Ao fortalecer a responsabilização penal, o Estado busca reforçar a dimensão repressiva da política de proteção de dados.

Em 2023, o Decreto nº 11.491 promulgou a Convenção sobre o Cibercrime, conhecida como Convenção de Budapeste, instrumento internacional que estabelece padrões para investigação, prevenção e repressão de crimes cibernéticos, na qual o Brasil havia se tornado signatário em 2001. Com essa promulgação, o Brasil assume formalmente a obrigação de cooperar internacionalmente em investigações, compartilhamento de evidências digitais, rastreamento de atividades criminosas transnacionais e harmonização de práticas legais com outros países signatários. Essa internacionalização da política de segurança digital reforça o caráter estratégico dos dados, uma vez que informações sensíveis podem ser acessadas, processadas e transferidas entre diferentes jurisdições, ampliando o alcance das medidas de proteção e fiscalização.

Contudo, essa integração internacional também levanta debates críticos relevantes. Primeiro, surge uma questão de soberania digital, já que a cooperação internacional pode exigir que o Brasil adote padrões ou protocolos que limitem a autonomia na gestão de seus próprios dados e infraestruturas críticas. Segundo, há implicações diretas para a privacidade dos cidadãos, pois a troca de informações transnacional aumenta os riscos de exposição de dados pessoais, exigindo mecanismos rigorosos de proteção para que o compartilhamento não viole direitos fundamentais consagrados na Constituição Federal e na LGPD . Por fim, a dependência de tecnologias e protocolos internacionais evidencia uma vulnerabilidade estratégica: o Brasil, ao participar desse sistema global, precisa garantir que seus recursos tecnológicos, capacidade de fiscalização e legislação estejam adequadamente alinhados para não se tornar um elo frágil na rede de cibersegurança internacional.

Dessa forma, a promulgação da Convenção de Budapeste evidencia tanto o avanço regulatório brasileiro no combate a crimes cibernéticos quanto as tensões críticas entre proteção, soberania e privacidade, mostrando que a inserção do país em regimes globais de cooperação cibernética exige equilíbrio delicado entre segurança e direitos individuais.

A culminação desse processo histórico ocorre em 2025, com a publicação do Decreto nº 12.573, que institui a Estratégia Nacional de Cibersegurança (E-Ciber 2025). Esse decreto representa um marco regulatório ao consolidar a segurança digital como um elemento estratégico de soberania do Estado brasileiro, reconhecendo que a proteção de dados pessoais não é apenas uma questão de privacidade individual, mas também um componente central da autonomia tecnológica e econômica do país (BRASIL, 2025, art. 4º). Ao incluir explicitamente a proteção de dados pessoais na definição de "soberania digital", o decreto posiciona a segurança cibernética como instrumento de governança nacional, alinhando interesses estratégicos, econômicos e de defesa.

O E-Ciber 2025 não se limita à proteção de infraestruturas críticas; ele também estabelece diretrizes para capacitação tecnológica, intercâmbio de informações entre órgãos públicos e privados, e protocolos de resposta a incidentes de grande escala. Dessa forma, o decreto amplia o escopo da proteção de dados para além do setor financeiro, integrando diferentes setores estratégicos da economia e do Estado. Para o setor financeiro, isso significa que medidas de segurança não se restringem à conformidade legal com a LGPD ou às normas do Banco Central, mas passam a fazer parte de uma estratégia nacional de mitigação de riscos cibernéticos em larga escala.

Contudo, essa centralidade da proteção de dados na soberania digital também gera tensões críticas. Ao vincular direitos individuais à segurança nacional, existe o risco de que a proteção legal dos consumidores se sobreponha às necessidades estratégicas do Estado ou a práticas de monitoramento ampliado. Em outras palavras, enquanto o E-Ciber 2025 fortalece a capacidade do país de proteger informações e prevenir crimes cibernéticos, ele também amplia a ambivalência entre proteção e vigilância, especialmente em setores como o financeiro, onde o Banco Central supervisiona sistemas digitais de grande complexidade e impacto.

Além disso, a E-Ciber 2025 evidencia uma busca por integração tecnológica e interoperabilidade internacional, alinhando-se a padrões globais de cibersegurança. Essa perspectiva fortalece a posição do Brasil no combate a crimes cibernéticos transnacionais, mas exige atenção crítica: a dependência de tecnologias, protocolos e práticas internacionais

pode gerar vulnerabilidades estratégicas, tornando a soberania digital parcial e condicionada à cooperação global.

Assim, o Decreto nº 12.573 representa a etapa mais avançada do arcabouço legal brasileiro em proteção de dados e segurança digital: consolida normas nacionais, define a cibersegurança como política de Estado e estabelece bases para a atuação coordenada do Banco Central e demais órgãos reguladores, mas simultaneamente mantém desafios críticos relacionados à autonomia do consumidor, privacidade e equilíbrio entre segurança e vigilância.

A análise das legislações identificadas permite observar um processo evolutivo marcado por três movimentos principais: (i) o reconhecimento progressivo da proteção de dados como dimensão da privacidade e dos direitos fundamentais; (ii) a institucionalização de práticas e obrigações de segurança digital no setor público e privado; e (iii) a construção de instrumentos jurídicos voltados ao enfrentamento de crimes cibernéticos e à defesa da soberania digital.

Em síntese, a evolução normativa brasileira pós-1988 revela um avanço inegável na proteção de dados, mas também uma série de tensões críticas:

- Ambivalência entre proteção e vigilância: a legislação protege formalmente a privacidade, mas permite mecanismos de monitoramento extensivos;
- Descompasso temporal entre tecnologia e legislação: leis como o Marco Civil e a LGPD surgem depois que práticas de coleta e análise de dados já estavam consolidadas;
- Assimetria de poder: instituições financeiras e plataformas digitais possuem conhecimento e capacidade de exploração de dados muito superiores aos consumidores;
- Integração público-privada: políticas de cibersegurança e regulação financeira consolidam a vigilância integrada de dados pessoais;
- Desafios internacionais: cooperação global e convenções internacionais ampliam o acesso de terceiros aos dados brasileiros, complicando a soberania digital.

Por fim, os textos legais que mencionam o Banco Central do Brasil revelam que, nas últimas décadas, o setor financeiro tornou-se um dos principais espaços de normatização da segurança digital, antecipando diretrizes posteriormente adotadas em outras áreas do Estado. Termos como “sigilo de dados”, “segurança digital”, “dados financeiros” e “infrações

cibernéticas" aparecem de modo recorrente em resoluções e circulares, evidenciando que o sistema financeiro funcionou como laboratório regulatório — um espaço no qual o Estado testou e refinou políticas antes de sua incorporação geral ao arcabouço jurídico.

Nesse sentido, o BC desempenha um papel central na proteção de dados e na segurança digital no setor financeiro, atuando como regulador, supervisor e garantidor da estabilidade do sistema financeiro nacional. A Constituição Federal de 1988, em seu artigo 192, caput, estabelece que "a política monetária, a política de crédito e a fiscalização das instituições financeiras são atividades do Estado, desempenhadas por autoridade competente"(BRASIL, 1988, art. 192, caput),conferindo base legal à atuação do BC.

O papel do Banco Central, portanto, é duplo: ele regula, fiscaliza e protege, mas também concentra informações estratégicas em nível sistêmico. A efetividade dessas medidas depende de fiscalização rigorosa, transparência das instituições e da capacidade do consumidor de exercer seus direitos, sob pena de a proteção de dados se tornar formalidade, sem impacto real sobre a autonomia individual.

5.2 MEDIDAS DE MITIGAÇÃO DOS RISCOS DE SEGURANÇA DIGITAL REGULADAS PELO BANCO CENTRAL DO BRASIL

O presente capítulo pretende responder ao segundo objetivo específico do estudo buscando identificar quais foram as medidas de segurança digital identificadas na pesquisa no Banco Central do Brasil, a que elas se propõem e como elas funcionam para o setor do varejo financeiro no Brasil. A análise busca não apenas descrever o conteúdo de cada resolução, circular ou instrução normativa, mas discutir seu papel na conformação de uma arquitetura institucional de segurança, refletindo seus avanços, limitações e possíveis tensões. A seguir, inicia-se a análise das normas identificadas nas buscas pelos termos "proteção de dados" e "segurança digital", conforme apresentado nos quadros 6 e 7 (páginas 59 e 62).

A busca pelo termo "proteção de dados" resultou em 33 normas, incluindo instruções normativas, resoluções e circulares, com destaque para a Instrução Normativa BCB nº 666/2025, que estabelece diretrizes para o tratamento de dados pessoais, incluindo anonimização e consentimento explícito, e para a Resolução BCB nº 498/2025, que impõe requisitos obrigatórios para controles de segurança da informação em instituições financeiras. A busca pelo termo "segurança digital" identificou 24 normas, muitas coincidentes com os resultados anteriores, destacando-se a Instrução Normativa BCB nº 667/2025, que detalha

planos de resposta a incidentes e protocolos de reporte de falhas, e a Resolução BCB nº 454/2025, que trata de planos de continuidade de negócios.

A partir da observação cronológica das normas identificadas pode-se compreender que desde 2013, o BC tem intensificado sua atuação regulatória no campo da segurança digital, com normatizações que ganharam maior densidade a partir de 2017 e picos significativos entre 2022 e 2025, período coincidente com a implementação da LGPD e da Estratégia Nacional de Cibersegurança. Esse movimento sugere um processo contínuo de adequação, em que o BC procura alinhar o sistema financeiro brasileiro às diretrizes nacionais e internacionais de proteção de dados e prevenção de crimes cibernéticos.

A evolução normativa do BC sob uma ótica cronológica revela uma trajetória de amadurecimento regulatório: enquanto normas anteriores, como a Resolução CMN nº 4.282/2013, traziam diretrizes mais gerais de segurança da informação, os documentos recentes incorporam detalhamentos técnicos e obrigações específicas para proteção de dados sensíveis, planos de resiliência digital, monitoramento contínuo e gestão de riscos de fornecedores terceirizados. Esse movimento não apenas fortalece a proteção de consumidores e a resiliência institucional, mas também evidencia o esforço do BC em criar um arcabouço regulatório compatível com os desafios emergentes do ciberespaço financeiro, onde ataques digitais, fraudes e vazamentos de dados são riscos sistêmicos de alta criticidade.

Contudo, a efetividade dessas medidas depende da capacidade das instituições de internalizar políticas complexas, integrar tecnologias avançadas, treinar equipes e manter protocolos atualizados diante de ameaças em constante evolução. Por um lado, a normatização detalhada contribui para a previsibilidade, transparência e padronização de procedimentos de proteção de dados; por outro, impõe desafios operacionais, principalmente para instituições de menor porte e fintechs, que precisam alocar recursos tecnológicos e humanos significativos para atender a tais exigências (Zuboff, 2020).

Dentro desse contexto, com base nas resoluções obtidas na busca, o conjunto de medidas consolidadas pelo BC foram organizadas em **cinco categorias** buscando organizar os achados da pesquisa, a saber: gestão de dados pessoais, segurança digital e resiliência de sistemas, planos de continuidade de negócios, supervisão interna e o reporte de incidentes de segurança, e gestão de riscos de terceiros. Essa organização permite não apenas compreender a lógica normativa, mas também examinar criticamente os efeitos práticos e as tensões implícitas entre segurança, inovação e governança. Ao longo desta seção, cada categoria será analisada detalhadamente, considerando seus fundamentos, aplicações no varejo financeiro e limitações.

A classificação dos resultados da pesquisa baseou-se em um critério temático-analítico, construído a partir da leitura sistemática das resoluções identificadas na busca. Após mapear as regulamentações, princípios e diretrizes emitidas pelo BC associadas a temática do estudo, procedeu-se à agrupação das medidas por afinidade temática e funcional, ou seja, pelo propósito regulatório predominante associado a cada dispositivo normativo.

Como primeira categoria, a **gestão de dados pessoais** constitui o alicerce das políticas de proteção digital do BC, especialmente à luz LGPD, que entrou em vigor em 2020 e estabeleceu princípios claros para tratamento, armazenamento e compartilhamento de informações pessoais. Entre as normas recentes, a Instrução Normativa BCB nº 666/2025 destaca-se ao estabelecer diretrizes explícitas para o tratamento de dados pessoais no sistema financeiro. De acordo com seu artigo 3º:

> As instituições devem implementar políticas de proteção de dados pessoais, incluindo anonimização e obtenção de consentimento explícito do titular para tratamento de informações sensíveis (BCB, 2025, art. 3º).

No contexto do varejo financeiro, essas normas se traduzem na adoção de mecanismos sofisticados de controle, como formulários digitais para consentimento informado, sistemas de anonimização de transações para análises estatísticas e restrição de acesso interno a informações sensíveis. Embora essas práticas promovam maior segurança e rastreabilidade, sua implementação exige tecnologia avançada e treinamento contínuo das equipes. Mais ainda, a anonimização de dados, embora prevista como ferramenta de proteção, apresenta limitações reconhecidas por Narayanan e Shmatikov (2008) e Solove (2011), que demonstram a possibilidade de reversão da anonimização em ambientes com grandes volumes de dados correlacionáveis, típico do setor bancário.

O consentimento explícito, por sua vez, é problemático em razão das assimetrias de poder entre instituições e consumidores. Conforme argumenta Zuboff (2020), frequentemente os usuários são submetidos a "escolhas simuladas" (fake choice), em que a aceitação de termos torna-se condição para acesso a serviços essenciais, reduzindo a efetiva autonomia do titular. Nesse sentido, embora a norma fortaleça o princípio formal de proteção de dados, na prática o controle do consumidor permanece limitado, e a proteção real depende da aplicação rigorosa de mecanismos internos de auditoria.

Além disso, a gestão de dados pessoais enfrenta desafios operacionais significativos. A complexidade de sistemas de logs de acesso, monitoramento interno e pseudonimização de

informações aumenta exponencialmente com o tamanho da instituição e o volume de transações. Woods e Simpson (2017) alertam que sistemas complexos apresentam “falhas normais”, isto é, a combinação inevitável de erros humanos e técnicos, que podem comprometer a proteção mesmo com políticas rigorosas. Ao mesmo tempo, Ayres e Braithwaite (1992) indicam que a multiplicidade de exigências regulatórias tende a gerar compliance formal, centrado na documentação e no cumprimento mínimo de regras, sem necessariamente transformar a cultura organizacional.

Dessa forma, a gestão de dados pessoais no setor financeiro brasileiro, mesmo com avanços normativos, permanece atravessada por contradições. Existe um esforço legítimo de alinhamento com a LGPD, mas o predomínio da lógica prudencial, a complexidade operacional e a assimetria entre instituições e consumidores limitam a eficácia prática das normas. Assim, a regulação do BC revela um campo em construção, no qual os avanços coabitam com fragilidades estruturais e desafios para a efetiva proteção do consumidor.

Como segunda categoria, a **segurança digital e resiliência de sistemas** no sistema financeiro brasileiro tornou-se um eixo central da regulação do BC, refletindo o reconhecimento de que instituições financeiras são alvos constantes de ataques cibernéticos sofisticados e que falhas em sistemas críticos podem gerar impactos sistêmicos significativos. Nesse contexto, a Resolução BCB nº 498/2025 estabelece medidas obrigatórias para a proteção de ativos digitais, definindo que:

> As instituições financeiras devem adotar controles de segurança compatíveis com a criticidade dos ativos digitais, incluindo autenticação robusta, criptografia de dados e monitoramento contínuo de sistemas (BCB, 2025, art. 2º).

Complementando essas disposições, a Instrução Normativa BCB nº 667/2025 detalha os planos de resposta a incidentes, incluindo detecção, contenção, mitigação e reporte imediato de falhas ao BC. Esses mecanismos não apenas visam reduzir o impacto de ataques, mas também garantir a continuidade operacional e a proteção do consumidor, reforçando a resiliência do sistema financeiro frente a ameaças cada vez mais complexas e persistentes.

No contexto do varejo financeiro, a aplicação dessas medidas é multifacetada. Bancos e fintechs implementam autenticação multifator para acessos de clientes, garantindo que credenciais de login isoladas não sejam suficientes para efetuar transações. A criptografia ponta a ponta em transferências digitais protege o fluxo de informações sensíveis, enquanto sistemas internos de monitoramento detectam padrões de fraude em tempo real, acionando

bloqueios automáticos e alertas imediatos (Anderson, 2020). Essa integração de tecnologia e processos representa um esforço coordenado para reduzir vulnerabilidades, garantindo que falhas de segurança não comprometam operações essenciais ou a confiança do público.

Entretanto, a efetividade dessas normas enfrenta desafios práticos. A complexidade tecnológica necessária para atender integralmente às exigências de autenticação, monitoramento e resposta a incidentes exige investimentos significativos em infraestrutura, pessoal especializado e manutenção contínua de sistemas. Além disso, a rápida evolução das técnicas de ataques cibernéticos impõe uma pressão constante sobre as instituições para atualizar protocolos e testar vulnerabilidades, criando um ciclo permanente de adaptação.

Além disso, ao centrar-se em controles técnicos e protocolos de resposta pós-incidente, a regulação tende a priorizar medidas corretivas em detrimento de estratégias estruturais de prevenção. Anderson (2020) argumenta que a segurança técnica, isoladamente, não garante proteção efetiva, especialmente em ambientes altamente interconectados e complexos como os sistemas financeiros digitais. Ataques sofisticados, como invasões coordenadas, exploração de vulnerabilidades de terceiros e fraude algorítmica, frequentemente escapam de controles tradicionais, indicando que a proteção do consumidor não pode depender exclusivamente de autenticação multifator, criptografia ou monitoramento automatizado.

Adicionalmente, os planos de resposta a incidentes, embora necessários, refletem uma lógica de regulação reativa. Perrow (1999) observa que sistemas complexos tendem a gerar "acidentes normais" e que a capacidade de previsão de crises é limitada. A ênfase do BC em reporte imediato e contenção de falhas é, portanto, coerente com essa lógica, mas não resolve os problemas estruturais que tornam ataques cibernéticos recorrentes, como a concentração de dados, dependência de sistemas terceirizados e integração de múltiplos aplicativos e serviços digitais.

A resiliência digital, entendida como a capacidade de absorver e se recuperar de incidentes, depende não apenas de controles técnicos, mas também de processos organizacionais, treinamento contínuo e cultura de segurança. Arner, Barberis e Buckley (2020) apontam que reguladores financeiros frequentemente subestimam a dimensão cultural da resiliência, limitando-se a exigir conformidade formal com normas técnicas. Essa abordagem formalista cria o risco de "compliance simbólico" (Ayres; Braithwaite, 1992), no qual instituições cumprem requisitos documentais sem promover mudanças efetivas na gestão de riscos.

Portanto, embora a segurança digital e a resiliência de sistemas sejam tratadas pelo BC com medidas detalhadas e sofisticadas, a eficácia dessas políticas depende de sua integração com práticas organizacionais, governança de terceiros, conscientização de usuários e atualização constante frente à evolução das ameaças. A regulação é necessária, mas não suficiente: o desafio real está em transformar obrigações formais em cultura institucional sólida, capaz de proteger dados, consumidores e operações de forma consistente.

Como terceira categoria, o conjunto de **planos de continuidade de negócios** constitui um elemento fundamental das políticas de segurança digital do BC, refletindo a necessidade de garantir que serviços financeiros essenciais permaneçam disponíveis mesmo diante de falhas, incidentes cibernéticos ou desastres naturais. A Resolução BCB nº 454/2025 estabelece que:

> As instituições devem implementar planos de continuidade de negócios que assegurem a prestação ininterrupta de serviços críticos em caso de falhas, incidentes cibernéticos ou desastres naturais (BCB, 2025, art. 1º).

Esses planos englobam procedimentos de contingência, backups criptografados, sistemas redundantes e rotas alternativas de processamento de transações. Além disso, incluem exercícios de simulação e testes de resiliência cibernética que permitem às instituições antecipar falhas, avaliar a eficácia das medidas adotadas e ajustar protocolos de forma contínua. Tal abordagem reforça a importância da previsibilidade operacional em um ambiente financeiro cada vez mais dependente de sistemas digitais complexos (Solove, 2011; Arner; Barberis; Buckley, 2020).

No varejo financeiro, os planos de continuidade de negócios se traduzem em práticas concretas, como o uso de data centers redundantes para processar transações bancárias, servidores alternativos para manter o funcionamento de aplicativos móveis e sistemas de backup criptografados para preservar informações críticas. Essas medidas garantem que transferências, pagamentos, consultas de saldo e outros serviços essenciais permaneçam disponíveis mesmo diante de falhas ou ataques. A execução dessas estratégias é particularmente relevante para fintechs e bancos digitais, cuja operação depende quase que exclusivamente de sistemas eletrônicos, tornando a continuidade do serviço um imperativo estratégico (Anderson, 2020).

Entretanto, a implementação dessas normas não é isenta de desafios. A complexidade técnica de manter sistemas redundantes, realizar backups regulares e atualizar planos de

contingência impõe custos significativos, especialmente para instituições de menor porte, que dependem de infraestrutura terceirizada e enfrentam restrições orçamentárias. Arner, Barberis e Buckley (2020) destacam que a dependência de provedores externos aumenta a vulnerabilidade sistêmica, exigindo que os reguladores ampliem a supervisão sobre terceirizados, tarefa complexa e contínua.

Além disso, ataques cibernéticos modernos evoluem rapidamente, exigindo atualização constante de protocolos e testes periódicos, o que pode gerar lacunas temporárias de segurança ou de eficácia operacional. Assim, essa categoria evidencia que os planos de continuidade de negócios, embora regulamentados, envolvem uma tensão entre segurança, custo e complexidade operacional. Eles funcionam como mecanismos preventivos que não apenas protegem consumidores, mas também mitigam riscos sistêmicos, prevenindo impactos que poderiam se propagar de uma instituição para o conjunto do setor financeiro.

Como quarta categoria, a **supervisão interna e o reporte de incidentes de segurança** configuram um dos pilares mais estratégicos da política de proteção digital do BC, pois permitem monitorar vulnerabilidades, mitigar riscos sistêmicos e assegurar a responsabilização das instituições financeiras. A Resolução CMN nº 5.105/2023 estabelece que:

> As instituições financeiras devem manter registros detalhados de incidentes de segurança, realizar auditorias periódicas e reportar ocorrências significativas ao Banco Central, permitindo análise sistêmica e tomada de medidas corretivas (CMN, 2023, art. 4º).

Aliado a essa, a Resolução Conjunta nº 6/2023 impõe a identificação, o registro e a comunicação de indícios de fraude em um dever contínuo e estruturado das instituições financeiras. O art. 2º institui a obrigação de manter um "sistema eletrônico que contemple […] o registro de dados e de informações sobre indícios de ocorrências ou de tentativas de fraudes", o que, na prática, cria uma infraestrutura de reporte compulsório e padronizado, incorporando mecanismos internos de monitoramento de incidentes. Esse sistema, além de registrar eventos, deve também permitir "a alteração e a exclusão dos dados" e "a consulta" pelas instituições, servindo como instrumento de supervisão interna e de retroalimentação dos controles de segurança. O art. 7º reforça essa dimensão ao exigir que as instituições criem "mecanismos de acompanhamento e de controle com vistas a assegurar a efetividade do cumprimento" da norma, incluindo "processos, testes e trilhas de auditoria" — elementos

centrais para a governança interna de incidentes. Ademais, o art. 8º determina que instituições mantenham "por dez anos, os dados e as informações compartilhados", consolidando uma base histórica de eventos que subsidia a supervisão interna, a investigação retrospectiva e a capacidade de resposta a incidentes complexos.

Essa diretriz evidencia que a segurança digital não pode ser encarada apenas como uma questão tecnológica isolada; ela requer governança robusta e processos internos claros. O registro detalhado de incidentes possibilita que padrões de vulnerabilidade sejam identificados, enquanto auditorias periódicas avaliam a eficácia de controles internos e garantem conformidade regulatória. Além disso, o reporte imediato ao BC permite uma resposta coordenada, mitigando impactos que poderiam se propagar para outras instituições ou para o sistema financeiro como um todo (Anderson, 2020; Zuboff, 2020).

No varejo financeiro, a implementação dessas normas se traduz em sistemas de monitoramento em tempo real, equipes dedicadas à análise de incidentes e protocolos claros para comunicação de falhas e ataques. Ferramentas automatizadas registram tentativas de invasão, acessos não autorizados e anomalias em transações, enquanto a comunicação imediata ao BC permite respostas coordenadas e mitigação de riscos sistêmicos.

Apesar de seu caráter essencial, essas medidas apresentam desafios operacionais e estratégicos. A manutenção de sistemas de monitoramento em tempo real e auditorias contínuas exige investimento em tecnologia, pessoal especializado e capacitação constante. Além disso, a centralização da supervisão no BC levanta questões sobre o equilíbrio entre governança institucional e autonomia operacional, refletindo tensões clássicas entre segurança sistêmica e liberdade corporativa (Zuboff, 2020).

A prática do reporte de incidentes também coloca em evidência um dilema ético e estratégico. Por um lado, aumenta a transparência e permite ao regulador atuar preventivamente; por outro, pode expor vulnerabilidades operacionais, afetar a reputação das instituições e gerar custos adicionais de conformidade. Ayres e Braithwaite (1992) destacam que, em ambientes regulatórios complexos, as organizações tendem a priorizar a conformidade formal em detrimento da cultura de segurança substantiva, adotando medidas que atendam aos requisitos documentais sem necessariamente fortalecer a resiliência efetiva dos sistemas.

No conjunto das normas analisadas, a Resolução BCB nº 366/2024 também destaca por regulamentar o Sistema de Informações Banco Central (Sisbacen), infraestrutura essencial para o funcionamento do SFN e ferramenta estratégica de supervisão do BC. O Sisbacen é descrito no art. 1º como "o conjunto de sistemas e recursos de tecnologia da informação do

Banco Central do Brasil […] para a captação, o tratamento e a divulgação de informações", além de disponibilizar dados a órgãos públicos e instituições financeiras, sempre "observados os preceitos de sigilo" (art. 1º, III). Em outras palavras, trata-se do principal repositório digital de informações regulatórias, financeiras e operacionais mantidas pelo BC — um núcleo tecnológico que conecta bancos, fintechs, cooperativas, órgãos governamentais e demais entidades autorizadas, sendo indispensável para a gestão de riscos, fiscalização prudencial e tomada de decisões de política monetária e supervisão.

O Sisbacen constitui a principal infraestrutura por meio da qual o BC consolida, avalia e supervisiona informações essenciais sobre o funcionamento das instituições financeiras. Ao definir que cabe ao Departamento de Tecnologia da Informação "estabelecer os critérios a serem observados nos processos informatizados de coleta, validação, tratamento, armazenamento e consulta às informações requeridas" (art. 5º, I), a norma reforça um modelo de supervisão baseado em trilhas de auditoria contínuas e altamente centralizadas. A gestão de segurança definida em dois níveis — "gerência-geral de segurança do Sisbacen" e "gerência setorial de segurança" (art. 12) — cria mecanismos de responsabilização explícita que permitem ao BC rastrear acessos, identificar anomalias e monitorar eventuais incidentes operacionais ou de segurança. Além disso, o registro obrigatório e arquivamento por cinco anos do "consentimento expresso" para cadastro de usuários (art. 14, §1º e §2º) introduz uma camada adicional de evidências para auditorias posteriores, ampliando a capacidade de reconstrução de eventos e investigações forenses em caso de acesso indevido ou vazamentos. Assim, a resolução reforça o papel do Sisbacen como ferramenta de monitoramento contínuo e de reporte estruturado, essencial para a detecção precoce de irregularidades, para a mitigação de incidentes cibernéticos e para a consolidação da supervisão prudencial digital no varejo financeiro brasileiro.

A **gestão de riscos de fornecedores e parceiros externos** compreende a quinta categoria, e constitui um elemento essencial da política de segurança digital do Banco Central do Brasil, especialmente em um cenário de crescente terceirização de serviços tecnológicos e digitalização do setor financeiro. A Resolução BCB nº 201/2022 estabelece que:

> As instituições devem avaliar e supervisionar fornecedores de serviços digitais e tecnológicos, garantindo que suas práticas de segurança estejam alinhadas às normas aplicáveis e que dados sensíveis não sejam expostos (BCB, 2022, art. 5º).

Consoante a essa, a Resolução BCB nº 85/2021 já mencionava a importância da gestão de riscos de fornecedores e parceiros externos ao tratar da contratação de serviços de processamento, armazenamento de dados e computação em nuvem. Antes da contratação, a instituição deve adotar procedimentos que contemplem "a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas" e verificar a capacidade do prestador de assegurar "o cumprimento da legislação e da regulamentação em vigor; o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço; [e] a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço" (arts. 12, II, a-c).

Além disso, essa resolução também previa que os contratos devem prever cláusulas que garantam "o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço" e a obrigação do contratado de "manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor" (art. 17, V e IX). Tais dispositivos evidenciam que a resolução orienta as instituições a identificar, avaliar e mitigar os riscos decorrentes da dependência de terceiros, garantindo maior controle sobre os serviços críticos e a proteção dos dados dos usuários finais.

Essas normas evidenciam uma compreensão de que a crescente dependência de terceiros — provedores de nuvem, processadores de pagamentos, APIs bancárias e plataformas digitais — introduz vulnerabilidades que podem comprometer tanto a segurança operacional quanto a privacidade de dados. Na prática, vulnerabilidades em fornecedores ou parceiros terceirizados podem gerar falhas críticas, expondo informações sensíveis de clientes e ameaçando a estabilidade operacional do sistema financeiro como um todo. Assim, a regulação busca criar uma cadeia de responsabilidade estendida, assegurando que todos os elos do ecossistema financeiro digital estejam alinhados a padrões rigorosos de segurança (Solove, 2011; Anderson, 2020).

No varejo financeiro, a gestão de riscos de terceiros se manifesta por meio de diligência prévia rigorosa na seleção de fornecedores tecnológicos, contratos detalhados com cláusulas de proteção de dados e monitoramento contínuo de prestadores de serviços. Essa supervisão envolve auditorias periódicas, verificação de certificações de segurança e testes de conformidade com normas regulatórias, garantindo que as instituições mantenham controle

sobre dados sensíveis mesmo quando operam em ambientes parcialmente terceirizados (Arner; Barberis; Buckley, 2020).

Um ponto crítico é o equilíbrio entre inovação e controle regulatório. O setor financeiro tem experimentado um crescimento acelerado de fintechs e plataformas digitais, cujo modelo de negócios depende de integração tecnológica ágil. A exigência de supervisão rigorosa de terceiros, embora necessária para proteção de dados e resiliência operacional, pode gerar entraves à inovação, tornando o processo de digitalização mais lento ou custoso. Isso evidencia uma tensão normativa intrínseca: como compatibilizar proteção de dados, segurança digital e resiliência do sistema com a dinâmica de inovação e competitividade do mercado? Zuboff (2020) alerta que políticas excessivamente centralizadoras podem gerar concentração de poder e reduzir a autonomia operacional das instituições, enquanto políticas insuficientes expõem o sistema a vulnerabilidades graves.

Dessa forma, a gestão de riscos de terceiros demonstra que a proteção digital e a segurança financeira não se limitam a regras internas, mas dependem de uma abordagem sistêmica e integrada. O BC, ao regulamentar esse aspecto, busca garantir que as instituições financeiras considerem não apenas seus próprios processos, mas toda a cadeia de serviços que sustenta suas operações digitais. No entanto, a eficácia dessa abordagem requer monitoramento contínuo, capacidade de adaptação frente a mudanças tecnológicas e equilíbrio entre regulação, inovação e competitividade.

A luz destas cinco categorias, as medidas de segurança digital implementadas pelo BC evidenciam um esforço regulatório que busca conciliar a proteção do consumidor, a resiliência do sistema financeiro e a conformidade com as diretrizes nacionais. No entanto, a atuação do BC também levanta questões críticas que precisam ser consideradas. A centralização do controle de informações estratégicas e dados sobre incidentes fortalece a capacidade de supervisão e detecção de vulnerabilidades sistêmicas, mas simultaneamente suscita debates sobre vigilância institucional e privacidade sistêmica, evidenciando a tensão entre segurança e autonomia das instituições financeiras (Zuboff, 2020).

A complexidade regulatória é outro ponto de atenção. A multiplicidade de normas — Instruções Normativas, Resoluções, Circulares e Comunicados —, embora necessária para detalhar obrigações técnicas e procedimentais, pode gerar desafios de interpretação e implementação, especialmente para fintechs e bancos de menor porte, que enfrentam limitações de recursos e capacidades técnicas (Arner; Barberis; Buckley, 2020).

Além disso, o desafio da efetividade prática permanece central. A robustez normativa por si só não garante segurança: é indispensável que as instituições financeiras atualizem

continuamente seus sistemas, invistam em tecnologia de ponta, capacitem suas equipes e cultivem uma cultura organizacional voltada à proteção de dados e à prevenção de ataques cibernéticos. Sem esses elementos, mesmo normas bem estruturadas podem ter eficácia limitada diante da rápida evolução das ameaças digitais (Anderson, 2020; Solove, 2011).

Em síntese, a atuação do BC reflete uma estratégia regulatória que atende às diretrizes nacionais de proteção de dados. Contudo, a regulação deve ser constantemente avaliada e ajustada, considerando impactos reais sobre o consumidor, adequação às normas e capacidade das instituições de se adaptar a ameaças emergentes. A efetividade do modelo depende, portanto, não apenas da clareza e abrangência das normas, mas também da maturidade tecnológica, da governança interna e da cultura organizacional das instituições reguladas, demonstrando que a segurança digital no varejo financeiro é simultaneamente normativa, estratégica e operacional.

6. DISCUSSÕES: OS EFEITOS DAS POLÍTICAS ESTABELECIDAS PELO BANCO CENTRAL DO BRASIL NA PROTEÇÃO DE DADOS DOS CONSUMIDORES E NA PREVENÇÃO DE CRIMES CIBERNÉTICOS.

Esta seção tem como objetivo alcançar o terceiro objetivo específico do estudo, que consiste em compreender os efeitos dessas políticas estabelecidas pelo Banco Central do Brasil apresentadas e discutidas na seção anterior, na proteção de dados dos consumidores e na prevenção de crimes cibernéticos.

O Brasil possui um arcabouço jurídico robusto no campo da proteção de dados pessoais, tendo a Lei Geral de Proteção de Dados Pessoais (LGPD) como principal marco regulatório. Essa lei estabelece direitos aos titulares de dados, obrigações para controladores e operadores, e prevê sanções em caso de descumprimento. Dentro desse contexto, o Banco Central do Brasil, na qualidade de regulador do sistema financeiro, tem editado diversas resoluções com o objetivo de orientar as instituições de pagamento, bancos e outros participantes do mercado quanto à proteção de dados, segurança digital e gestão de riscos.

Apesar do rigor formal dessas regulamentações, surge a questão sobre sua efetividade prática. Muitas das exigências descritas nas resoluções priorizam documentação, relatórios e formalização de políticas, elementos fundamentais para fins de supervisão, mas que não garantem necessariamente a implementação consistente das medidas de segurança no cotidiano das instituições (Silveira; Oliveira; Mozane, 2024). Além disso, embora o BC possua poder de fiscalização, a complexidade das operações financeiras e a presença de

fornecedores terceirizados, inclusive em outros países, podem limitar a supervisão contínua, deixando margens para vulnerabilidades. Dessa forma, enquanto as resoluções definem um padrão normativo mínimo de proteção, sua aplicação prática é crucial para que os dados de clientes estejam efetivamente protegidos.

As medidas regulatórias do BC têm impactos diretos sobre a segurança digital dos consumidores do varejo financeiro. Ao exigir políticas de governança, segregação de dados e controles de acesso adequados, as instituições reduzem os riscos de fraudes e vazamentos de informações sensíveis (Ferreira, 2024). Da mesma forma, ao estabelecer regras rigorosas para a contratação de serviços de computação em nuvem, inclusive definindo a necessidade de avaliação da capacidade do prestador de garantir confidencialidade e integridade dos dados, o regulador contribui para a proteção de informações pessoais de clientes (Tourinho, 2025).

No entanto, ainda existem pontos críticos, especialmente quando serviços terceirizados são contratados no exterior. A Resolução 85/2021 estabelece que a instituição deve garantir que a legislação do país onde o serviço será prestado não impeça o acesso aos dados pela instituição contratante ou pelo BC, mas, na prática, convênios internacionais ou restrições legais podem limitar esse acesso, deixando os dados potencialmente expostos. Esse desafio evidencia uma tensão entre a formalidade regulatória e a efetividade operacional da supervisão. Além disso, muitas instituições financeiras dependem de provedores globais de nuvem, cujas práticas de coleta, armazenamento e análise de dados podem não estar totalmente alinhadas aos padrões brasileiros, gerando riscos adicionais relacionados à soberania digital e à proteção efetiva do consumidor (Ferrarri; Faranda, 2024; Saal; Krawczyk; Moos, 2022).

Um exemplo disso ocorreu no dia 20 de outubro de 2025, quando o sistema de pagamentos instantâneos Pix apresentou instabilidade generalizada em diversas regiões do Brasil, coincidindo com uma falha global na Amazon Web Services (AWS). Usuários relataram interrupções em transferências e pagamentos, e plataformas de monitoramento de indisponibilidade de serviços registraram picos de até 272 reclamações por minuto (AGÊNCIA BRASIL, 2025; ESTADO DE MINAS, 2025). Nas redes sociais e em relatos de instituições financeiras, foram observadas lentidões significativas e falhas completas na realização de transações via Pix (INFOMONEY, 2025; ESTADO DE MINAS, 2025). Apesar de o BC afirmar que seus sistemas estavam operando normalmente naquele dia, a coincidência temporal entre a pane na AWS e a instabilidade do Pix indica que problemas na infraestrutura de nuvem podem afetar diretamente a disponibilidade e a confiabilidade dos

serviços de pagamentos, evidenciando riscos associados à dependência de provedores globais de infraestrutura tecnológica (INFOMONEY, 2025; SAMPI.NET.BR, 2025).

Adicionalmente, essas medidas têm implicações diretas para a soberania digital do Brasil. Ao assegurar que dados sensíveis de clientes permaneçam sob controle nacional e que fornecedores estrangeiros sejam avaliados quanto à conformidade legal, o regulador fortalece a autonomia do país sobre suas informações financeiras. Ao mesmo tempo, é necessário considerar o contexto do capitalismo de vigilância, em que dados se tornam ativos estratégicos para análise de comportamento e tomada de decisões comerciais. Nesse sentido, o BC precisa equilibrar a proteção dos consumidores com as demandas operacionais do setor, evitando que práticas de coleta e processamento de dados extrapolem os limites da privacidade individual.

Além do aspecto técnico e regulatório, a análise dessas medidas pode ser ampliada ao considerar a perspectiva do capitalismo de vigilância, conforme delineado por Zuboff (2020). Nesse contexto, o sistema financeiro digital, fortemente regulado, ainda opera em um ambiente em que dados pessoais são coletados massivamente, não apenas para fins operacionais, mas também para predição de comportamentos, análise de perfil de risco e oferta de produtos financeiros personalizados. A regulamentação do BC estabelece salvaguardas para proteger esses dados, mas não elimina completamente a coleta massiva ou a possibilidade de uso para manipulação de comportamentos, sobretudo quando terceirizações e tecnologias em nuvem estão envolvidas.

As cinco características do capitalismo de vigilância, conforme Zuboff (2020) — coleta massiva de dados, predição e manipulação de comportamentos, economia da atenção, desigualdade e exclusão, e invisibilidade do processo de coleta de dados — ainda podem se manifestar mesmo em um ambiente regulado. Por exemplo, enquanto as resoluções buscam assegurar a integridade e a confidencialidade dos dados, elas não restringem o potencial das instituições financeiras de utilizá-los para criar perfis detalhados de consumidores ou segmentar serviços de forma a reforçar desigualdades, nem tornam visível ao usuário o fluxo de coleta e processamento de suas informações.

Ao analisar as medidas do BC à luz do capitalismo de vigilância, é possível perceber que, mesmo com regulamentações robustas como a Resolução BCB nº 85/2021, os riscos associados à coleta e ao uso de dados permanecem relevantes. A primeira característica desse modelo, a coleta massiva de dados (Zuboff, 2020), está diretamente presente nas operações das instituições financeiras, que acumulam informações de clientes sobre transações, hábitos de consumo, localização, perfis de risco e interações digitais. As normas do BC, ao exigir

segregação de dados, controles de acesso e auditorias independentes (art. 12, II, g e h), procuram limitar o risco de vazamentos e acessos não autorizados. Entretanto, elas não restringem a própria coleta de dados em larga escala, que continua sendo uma prática intrínseca aos serviços financeiros digitais. Dessa forma, a regulamentação atua mais como um mecanismo de mitigação de riscos operacionais do que como barreira à acumulação massiva de informações pessoais.

Gonçalves (2023), ao discutir os impactos e desafios da LGPD no setor financeiro, enfatiza a complexidade de implementação de políticas de privacidade em instituições que dependem fortemente de dados para análise de crédito e serviços personalizados. Essa perspectiva reforça a análise do presente estudo, evidenciando que, embora o BC forneça diretrizes detalhadas para segurança digital e governança de dados, a efetiva proteção dos consumidores depende da correta aplicação da legislação por parte das instituições financeiras, da fiscalização regulatória e da transparência nos processos de coleta e processamento de informações. O autor reforça que a conformidade formal não é suficiente para garantir que os direitos dos titulares sejam respeitados, especialmente quando dados são utilizados para fins estratégicos ou comportamentais (Gonçalves; 2023).

A segunda característica, predição e manipulação de comportamentos, também permanece como uma realidade possível, mesmo sob regulamentação. Instituições financeiras utilizam algoritmos e modelos analíticos para segmentar clientes, ajustar limites de crédito, recomendar produtos financeiros e até identificar padrões de consumo que permitem prever comportamentos futuros. Embora a Resolução BCB nº 85/2021 imponha controles sobre a segurança e a integridade dos dados processados por prestadores terceirizados, ela não regula diretamente o uso dos dados para fins de modelagem comportamental ou marketing direcionado. Isso significa que, ainda que a privacidade e a confidencialidade dos dados sejam formalmente protegidas, os consumidores continuam sujeitos a formas de predição e manipulação, que fazem parte do ecossistema do capitalismo de vigilância.

A economia da atenção, terceira característica apresentada por Zuboff (2020), é menos evidente no sistema financeiro tradicional, mas se manifesta nos serviços digitais de pagamento, aplicativos bancários e plataformas de crédito online. O design dessas interfaces busca maximizar a interação do usuário, incentivando o engajamento contínuo, alertas de transações, notificações de promoções e ofertas personalizadas. A regulamentação do BC não impede essas práticas, mas as medidas de segurança, como autenticação forte e monitoramento de acessos (art. 12, II, h; art. 17, III), ajudam a proteger os consumidores de

abusos que poderiam ocorrer através da exploração da atenção para fins fraudulentos ou não autorizados.

A quarta característica, desigualdade e exclusão, está diretamente relacionada à forma como dados são utilizados para segmentar e priorizar clientes. A regulamentação brasileira, ao estabelecer padrões mínimos de proteção e exigir planos de continuidade operacional, reduz o risco de exclusão causada por falhas ou interrupções nos serviços. No entanto, ela não garante equidade na utilização dos dados, nem impede que algoritmos financeiros criem barreiras para determinados grupos sociais ou econômicos. Por exemplo, clientes com perfis de risco considerados mais elevados podem ter acesso restrito a produtos financeiros, independentemente da proteção de seus dados. Assim, a desigualdade estrutural inerente à economia de dados persiste, mesmo em um ambiente regulado.

Moraes e Woszczyna (2019) destacam que a automação e a utilização de algoritmos nos serviços financeiros podem reforçar processos de exclusão, determinando quem tem acesso a crédito, seguros e outros produtos, muitas vezes com base em perfis de risco derivados de dados massivos. Quando confrontamos essa perspectiva com a regulamentação do BC, observa-se que, embora medidas como a Resolução BCB nº 85/2021 busquem garantir a segurança e a integridade dos dados, elas não abordam diretamente a equidade na utilização dessas informações. Ou seja, a proteção formal dos dados não impede que algoritmos perpetuem desigualdades ou restrinjam o acesso de determinados grupos sociais, mostrando que a regulamentação atua mais sobre a mitigação de riscos operacionais do que sobre os impactos sociais do uso estratégico de dados (Moraes; Woszczyna, 2019)

A quinta e última característica, a invisibilidade do processo de coleta de dados, também permanece parcialmente intacta. As resoluções do BC exigem que as instituições de pagamento forneçam auditorias e relatórios de prestadores de serviço, e que mantenham registros detalhados das operações e acessos aos dados (arts. 12, II, e-f; art. 15). Contudo, para o usuário final, o fluxo de coleta, armazenamento e processamento das informações permanece opaco. O titular dos dados raramente possui visibilidade sobre como seus dados são combinados, analisados ou utilizados para decisões comerciais, mesmo quando a confidencialidade e integridade são formalmente garantidas. Portanto, embora a regulamentação aumente a transparência institucional e o controle regulatório, ela não elimina a invisibilidade do processo para os consumidores.

A discussão sobre colonialismo de dados apresentada por Faustino (2020) traz uma dimensão crítica sobre a extração e a concentração de dados em grandes corporações e plataformas tecnológicas. Embora a regulamentação do BC imponha salvaguardas de

segurança, segregação e auditoria, a apropriação e a centralização de dados sensíveis em grandes provedores de nuvem, inclusive estrangeiros, podem reproduzir dinâmicas de extração digital, onde o titular do dado mantém controle limitado sobre suas informações. Esse fenômeno evidencia que, mesmo em um ambiente regulado, persistem riscos estruturais relacionados à soberania digital e à autonomia do país sobre dados críticos do sistema financeiro.

A partir dessa análise, é possível perceber que as medidas do BC oferecem um nível de proteção formal e operacional, garantindo que instituições de pagamento e fornecedores terceiros implementem práticas de segurança cibernética, segregação de dados, continuidade de serviços e auditorias. No entanto, a proteção não é absoluta e apresenta limitações quando se trata da utilização estratégica de dados, da manipulação de comportamentos ou da visibilidade do processo de coleta, refletindo as tensões entre regulação, eficiência operacional e o capitalismo de vigilância.

Nesse sentido, Lippold (2020) argumenta que os dados devem ser entendidos como recursos estratégicos, cuja exploração define novas lógicas econômicas e de poder. Essa perspectiva permite interpretar a coleta e o processamento massivo de informações no sistema financeiro como uma forma de capital digital, cuja gestão segura e regulada é fundamental não apenas para proteger consumidores, mas também para assegurar a soberania digital. As medidas do BC, ao exigirem auditorias, segregação de dados e continuidade de serviços, representam esforços importantes nesse sentido, mas, como o autor enfatiza, o verdadeiro controle sobre os dados — e sua utilização ética e estratégica — é um desafio contínuo que transcende a simples formalidade regulatória (Lippold, 2020).

Ao tratar da cultura da vigilância, Lyon (2019) argumenta que a observação contínua e a coleta de dados estruturam um estilo de vida moderno, em que a exposição digital é inevitável e normalizada. No contexto financeiro, essa perspectiva ilumina como, mesmo sob regulamentação robusta, o capitalismo de vigilância permanece presente: dados sobre transações, hábitos de consumo e interações digitais são constantemente coletados e utilizados para predição de comportamentos (Lyon, 2019). As medidas do BC contribuem para mitigar riscos de vazamento e acesso não autorizado, mas não transformam a cultura da vigilância, evidenciando que a regulação atua mais na proteção formal e operacional do que na transformação do ambiente sociotécnico subjacente.

A análise das resoluções do BC revela que os princípios fundamentais da segurança digital — confidencialidade, integridade e disponibilidade da informação, conforme apresentados por Anderson (2020) e descritos na seção do referencial teórico — estão

incorporados de maneira explícita e estruturante no desenho regulatório aplicado ao setor financeiro. A confidencialidade, entendida como a proteção dos dados contra acessos não autorizados, é operacionalizada principalmente por meio da exigência de controles de acesso estritos, segregação de ambientes e políticas formais de gestão de identidades. A Resolução BCB nº 85/2021, por exemplo, determina que instituições financeiras adotem mecanismos robustos de autenticação e monitorem continuamente o comportamento de usuários internos e externos, aproximando-se diretamente das recomendações de Anderson sobre boas práticas de segurança. Esse alinhamento evidencia que o BC busca reforçar não apenas o cumprimento normativo, mas a construção de uma camada efetiva de proteção contra vulnerabilidades frequentemente exploradas em ataques cibernéticos.

No que diz respeito à integridade da informação, o BC estabelece requisitos que visam garantir a precisão, consistência e confiabilidade dos dados ao longo de todo o ciclo de tratamento. As resoluções demandam que instituições implementem processos de validação de transações, trilhas de auditoria, mecanismos de verificação de integridade e monitoramento de alterações não autorizadas — medidas que respondem ao princípio, destacado por Anderson (2020), de que a integridade é essencial para evitar manipulações maliciosas ou erros sistêmicos que comprometam a confiabilidade dos serviços financeiros. Essa diretriz é particularmente relevante em um ambiente no qual falhas na integridade podem gerar prejuízos imediatos, desinformação ou mesmo decisões algorítmicas equivocadas em produtos como crédito, seguros e pagamentos.

A disponibilidade, terceira dimensão central da segurança digital, também se manifesta de forma robusta nas normas do BC, que exigem a implementação de políticas de continuidade de negócios, redundância de sistemas, planos de resposta a incidentes e estratégias de recuperação de desastres. A preocupação com disponibilidade está ligada tanto à estabilidade operacional das instituições quanto à proteção dos consumidores, uma vez que interrupções em serviços bancários ou de pagamento afetam diretamente a confiança no sistema financeiro. Ao incorporar exigências rígidas para infraestrutura resiliente, o BC reforça o entendimento de Anderson (2020) de que a disponibilidade não é apenas um requisito operacional, mas um elemento indissociável da segurança digital em ecossistemas críticos.

Complementarmente, a infraestrutura tecnológica aparece como uma dimensão estruturante nas medidas regulatórias do BC. A exigência de firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS), monitoramento contínuo, criptografia de dados em repouso e em trânsito, e controles de segmentação de rede seguem diretamente as recomendações

clássicas apresentadas na literatura — incluindo Anderson (2020) — sobre os pilares técnicos da segurança digital. A regulamentação não apenas descreve esses mecanismos, mas os vincula à necessidade de avaliações periódicas de risco, testes de vulnerabilidade e auditorias independentes, evidenciando que a segurança não se limita à adoção de ferramentas, mas envolve sua integração coerente em uma arquitetura tecnológica abrangente.

Esses elementos sugerem que o BC internaliza a visão contemporânea segundo a qual segurança digital depende de camadas múltiplas — políticas, controles, infraestrutura, governança e monitoramento — funcionando de maneira integrada. A presença de exigências formais relacionadas à estrutura tecnológica reforça a preocupação do regulador em alinhar o sistema financeiro brasileiro a padrões internacionais de resiliência cibernética, mitigando riscos associados a ataques de larga escala, falhas de sistemas, acessos indevidos e interrupções de serviços críticos. Assim, observa-se uma convergência clara entre os princípios da segurança digital e a prática regulatória implementada pelo BC, ainda que persistam desafios relacionados à operacionalização dessas medidas por instituições de diferentes portes e capacidades técnicas.

Finalmente, a discussão sobre proteção de dados e segurança digital deve ser vinculada ao conceito de soberania digital, entendido como a capacidade de um país de garantir que dados estratégicos, informações sensíveis e decisões digitais críticas permaneçam sob jurisdição nacional e sob controle regulatório efetivo. O Brasil, ao estabelecer regulamentações detalhadas sobre segurança cibernética, proteção de dados e terceirizações, avança na construção de um ambiente digital mais controlado e autônomo. No entanto, a soberania digital não depende apenas de regras formais, mas também da capacidade de garantir que dados críticos permaneçam sob jurisdição nacional e que os cidadãos tenham controle efetivo sobre suas informações.

Embora o BC forneça um arcabouço normativo avançado, existem desafios operacionais, lacunas em supervisionamento internacional e limitações na fiscalização contínua que indicam que a soberania digital ainda precisa ser fortalecida, de modo a garantir que as medidas de proteção de dados não se limitem à formalidade, mas se traduzam em segurança efetiva para consumidores, operadores do varejo financeiro e para o sistema financeiro como um todo. É necessário avançar em mecanismos que aumentem a visibilidade do fluxo de dados para os titulares, controlem o uso de dados para fins de manipulação comportamental e fortaleçam a fiscalização de serviços terceirizados em nuvem internacional, garantindo que a proteção de dados se traduza em segurança efetiva para consumidores, operadores e para o próprio sistema financeiro.

Em um contexto geral, ao se comparar a experiência brasileira com práticas internacionais, estudos como os de Sampaio (2022), Vilela e Giolo Júnior (2023), Rocha e Canedo (2025) e Souza, Eugênio e Araújo (2025) evidenciam que existem diferenças significativas na forma como diferentes países abordam a proteção de dados e a segurança digital. Diversas nações têm desenvolvido estruturas regulatórias mais robustas e mecanismos institucionais mais avançados, o que também evidencia que o Brasil ainda enfrenta desafios estruturais na operacionalização efetiva dessas regulamentações.

Na União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) estabelece um arcabouço abrangente, que inclui princípios de minimização de dados, accountability, auditorias periódicas e sanções financeiras significativas em caso de descumprimento. Países como Alemanha e França complementam o GDPR com fiscalização técnica rigorosa, exigindo certificações de sistemas de processamento de dados e auditorias independentes, enquanto programas de "privacy by design" e "privacy by default" orientam a implementação de tecnologias alinhadas aos direitos fundamentais de privacidade (Buckley, 2024).

Fora da Europa, experiências no Canadá e nos Estados Unidos ilustram abordagens distintas, mas igualmente estruturadas, para lidar com a coleta e o processamento de dados pessoais. No Canadá, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) combina mecanismos de responsabilização empresarial, transparência na gestão de dados e auditorias periódicas, enquanto nos Estados Unidos, embora não exista uma lei federal unificada, iniciativas estaduais como a Lei de Privacidade do Consumidor da Califórnia (CCPA) introduzem direitos de acesso, exclusão e portabilidade de dados, associando-os a requisitos de divulgação e compliance para grandes plataformas digitais (Martins De Oliveira; Barile Da Silveira; Macena Dias De Oliveira, 2025).

A Suíça, por sua vez, adota políticas de proteção de dados altamente segmentadas, com protocolos técnicos avançados, supervisão regulatória independente e acordos internacionais que reforçam a soberania digital (Baltaian, 2024). Singapura, por outro lado, combina supervisão de provedores de serviços estrangeiros, monitoramento contínuo de riscos cibernéticos e requisitos setoriais para minimização de dados, evidenciando uma abordagem proativa na mitigação de ameaças à segurança digital e à privacidade de seus cidadãos (Chik, 2013).

Apesar do avanço dessas experiências internacionais, o contexto brasileiro apresenta particularidades que revelam lacunas importantes na proteção de dados e no enfrentamento da vigilância digital. Embora a Resolução BCB nº 85 e LGPD estabeleçam obrigações formais de notificação, auditoria e responsabilização, a fiscalização efetiva de serviços digitais

prestados no exterior permanece limitada, especialmente na ausência de convênios de cooperação entre autoridades reguladoras. Além disso, a dependência de tecnologias estrangeiras, combinada à aplicação ainda incipiente de sanções e à vulnerabilidade de populações historicamente marginalizadas, evidencia que os efeitos negativos da coleta e do uso de dados pessoais são sentidos de maneira mais intensa no Brasil do que em contextos regulatoriamente mais avançados.

Esse contraste evidencia um achado importante deste presente estudo: os efeitos adversos do capitalismo de vigilância no Brasil configuram um fenômeno local, situado no Sul Global, e não uma mera reprodução de padrões globais. Enquanto países com regimes regulatórios consolidados conseguem mitigar de maneira sistemática os riscos da exploração comercial de dados pessoais, o Brasil enfrenta desafios estruturais que potencializam vulnerabilidades sociais, econômicas e tecnológicas. Esse achado reforça a necessidade de políticas públicas inovadoras, capazes de articular proteção jurídica, soberania digital e inclusão social, e contribui para o debate acadêmico sobre vigilância digital ao evidenciar como o capitalismo de vigilância se manifesta de maneira diferenciada em contextos de menor capacidade regulatória e maior dependência tecnológica externa.

7. CONSIDERAÇÕES FINAIS

A presente dissertação teve como objetivo geral compreender como as medidas de proteção de dados do Banco Central do Brasil buscam mitigar os riscos de segurança digital no setor do varejo financeiro brasileiro, examinando, simultaneamente, o percurso regulatório histórico da proteção de dados no país e a materialização dessas diretrizes no âmbito das normas emitidas pelo principal órgão supervisor do Sistema Financeiro Nacional. A consecução desse objetivo se desdobrou em três objetivos específicos: (1) caracterizar como as políticas de proteção de dados foram normatizadas pelo Estado brasileiro após a Constituição de 1988; (2) identificar como o Banco Central ajustou suas políticas e regulamentações para atender às diretrizes nacionais de proteção de dados e prevenção de crimes cibernéticos; e (3) compreender os efeitos dessas políticas do Banco Central na proteção de dados e na mitigação de riscos de segurança digital para consumidores do varejo financeiro.

Para iluminar esse percurso analítico, o estudo se apoiou no referencial teórico do capitalismo de vigilância, conforme formulado por Zuboff (2020), que concebe a economia digital contemporânea como estruturada pela extração massiva de dados comportamentais,

pela transformação desses dados em previsões e pela comercialização dessas previsões como forma de induzir comportamentos futuros. Essa matriz teórica se mostrou especialmente relevante para analisar o setor financeiro, no qual a captura e o processamento de dados são estruturantes para decisões de crédito, ofertas personalizadas, gestão de riscos e avaliação comportamental dos consumidores. Assim, a leitura do capitalismo de vigilância funcionou como eixo crítico para compreender tanto as limitações inerentes às normas do Banco Central quanto as tensões entre regulação estatal, autonomia das instituições financeiras e a reprodução de assimetrias informacionais.

Metodologicamente, esta pesquisa adotou uma abordagem de pesquisa documental, fundamentada na análise sistemática das legislações brasileiras sobre proteção de dados — especialmente após a Constituição Federal de 1988 —, incluindo a LGPD e normas complementares. Paralelamente, realizou-se uma busca abrangente no portal do Banco Central para coletar resoluções, circulares, comunicados e instruções normativas relacionadas à proteção de dados, segurança digital, computação em nuvem e gestão de riscos tecnológicos. A análise se deu a partir de um método crítico-analítico, orientado pela identificação de convergências e tensões entre as normas nacionais e as regulamentações emitidas pelo Banco Central, bem como pela avaliação do alcance prático dessas medidas na mitigação de riscos para o consumidor e na proteção da soberania digital brasileira.

A síntese dos argumentos construídos ao longo desta dissertação revela um panorama multifacetado. Em primeiro lugar, demonstrou-se que as legislações brasileiras vêm incorporando gradualmente a proteção de dados e a segurança digital desde a Constituição de 1988. Em segundo lugar, verificou-se que o Banco Central, enquanto órgão regulador, ajustou seu arcabouço normativo de forma alinhada às diretrizes nacionais, expandindo significativamente suas exigências regulatórias entre 2013 e 2025, sobretudo após a promulgação da LGPD. Em terceiro lugar, mostrou-se que as resoluções do Banco Central oferecem um conjunto robusto de salvaguardas para a proteção de dados dos consumidores — incluindo segregação de ambientes, controles de acesso, governança estruturada, auditorias independentes e requisitos para a contratação de serviços em nuvem. Em quarto lugar, evidenciou-se que essas medidas contribuem para fortalecer a segurança digital das instituições e do consumidor final, ainda que sua efetividade dependa de capacidades organizacionais internas e de práticas técnicas que vão além da regulamentação formal. Em quinto lugar, verificou-se que as medidas do Banco Central dialogam de maneira direta com os três princípios fundamentais da segurança da informação — confidencialidade, integridade

e disponibilidade —, sobretudo ao impor requisitos de resiliência operacional, continuidade de negócios e mecanismos de resposta a incidentes.

Além disso, emergiram da análise documental cinco categorias estruturantes das medidas regulatórias do Banco Central — gestão de dados pessoais; segurança digital e resiliência de sistemas; planos de continuidade de negócios; supervisão interna e reporte de incidentes; e gestão de riscos de terceiros —, que serviram como eixos para compreender a profundidade e os limites do aparato regulatório. A partir dessas categorias, foi possível identificar avanços significativos, como a exigência crescente de auditorias, controles de segurança, formalização de governança e diretrizes claras para contratos com provedores de tecnologia. No entanto, também ficaram evidentes lacunas, como a dependência de provedores internacionais de nuvem, a dificuldade de monitoramento contínuo de ambientes externos, a assimetria de capacidades entre grandes bancos e fintechs, e a ausência de mecanismos que limitem o uso de dados para finalidades comportamentais compatíveis com o capitalismo de vigilância.

Por fim, a pesquisa demonstrou que o Brasil avança na construção de elementos de soberania digital — especialmente ao estabelecer salvaguardas regulatórias sobre dados financeiros sensíveis —, mas ainda enfrenta desafios significativos quando comparado a países como Alemanha, França e Singapura, que adotam modelos mais restritivos de governança de dados críticos e exigem maior supervisão estatal de provedores de nuvem e algoritmos financeiros. Em diálogo com esse cenário, demonstrou-se que o capitalismo de vigilância permeia o ecossistema financeiro brasileiro, sobretudo por meio das cinco características descritas por Zuboff (2020): coleta massiva de dados, predição comportamental, economia da atenção, desigualdade algorítmica e invisibilidade dos processos de coleta. Esses elementos aparecem não apenas nas práticas de mercado, mas também nas zonas de silêncio regulatório, nas quais a proteção de dados não se converte automaticamente em limitação da exploração comportamental.

A partir desse percurso analítico, torna-se possível apresentar uma resposta clara para a pergunta de pesquisa: como as medidas de proteção de dados do Banco Central do Brasil buscam mitigar os riscos de segurança digital no setor do varejo financeiro brasileiro? A resposta obtida demonstra que o Banco Central atua por meio de um conjunto articulado de normas que buscam estruturar controles técnicos, procedimentais e organizacionais capazes de reduzir vulnerabilidades no ecossistema financeiro. O BC o faz ao exigir mecanismos de governança de dados, políticas formais de proteção da informação, critérios de segurança para serviços terceirizados, requisitos de resiliência operacional e protocolos de resposta a

incidentes. Dessa forma, as medidas regulatórias buscam mitigar riscos por meio de uma abordagem sistêmica que integra prevenção, detecção, resposta e continuidade. No entanto, conclui-se que essa mitigação é parcial: embora o arcabouço normativo seja sólido e alinhado às legislações brasileiras, sua efetividade depende de capacidades internas das instituições financeiras, do nível de supervisão do Banco Central e de fatores externos, como a dependência tecnológica de provedores de nuvem globais.

As implicações desses achados são significativas para os campos da Administração e da Administração Pública. Em primeiro lugar, o estudo evidencia que a proteção de dados e a segurança digital se tornaram dimensões centrais da governança organizacional no setor financeiro, influenciando modelos de gestão, estratégias tecnológicas e processos de inovação. As normas do Banco Central funcionam como mecanismos de indução regulatória que pressionam as instituições a internalizar práticas avançadas de segurança e compliance digital. Em segundo lugar, a pesquisa contribui ao demonstrar como o Estado brasileiro — por meio de um órgão regulador especializado — exerce papel ativo na mediação entre mercado e sociedade, buscando equilibrar inovação financeira, estabilidade sistêmica e proteção do consumidor. Em terceiro lugar, revela-se que, mesmo em ambientes altamente regulados, persistem tensões entre interesses econômicos, exploração de dados e direitos fundamentais, o que exige novas abordagens administrativas para lidar com riscos digitais complexos e transfronteiriços.

Este estudo buscou contribuir para os campos dos Estudos Organizacionais e da Administração Pública ao articular a proteção de dados, a segurança digital e a regulação financeira a partir do referencial do capitalismo de vigilância. No plano acadêmico, a pesquisa buscou avançar ao aproximar um referencial crítico ainda pouco explorado na literatura administrativa brasileira da análise da atuação regulatória do Estado e da governança organizacional no setor financeiro, evidenciando como normas técnicas e jurídicas operam simultaneamente como instrumentos de mitigação de riscos e como limites parciais à exploração comportamental de dados. Ao propor categorias analíticas para compreender as medidas regulatórias do Banco Central do Brasil, o estudo pretendeu contribuir para a sistematização da segurança digital como dimensão relevante da governança organizacional contemporânea. No plano empírico, a dissertação buscou oferecer um mapeamento analítico do arcabouço normativo do Banco Central relacionado à proteção de dados e à segurança digital no varejo financeiro brasileiro, evidenciando como diretrizes legais se materializam em exigências concretas de governança, controle e supervisão. Para a Administração Pública, a pesquisa procurou evidenciar o papel do Estado como agente mediador entre inovação

tecnológica, estabilidade do sistema financeiro e proteção de direitos fundamentais, ao mesmo tempo em que buscou explicitar as limitações regulatórias associadas às assimetrias tecnológicas globais e à dependência de provedores estrangeiros. Nesse sentido, o estudo pretendeu subsidiar o debate sobre regulação, soberania digital e gestão pública no contexto do Sul Global, sem a pretensão de esgotar o tema, mas de oferecer elementos analíticos para pesquisas futuras e para a reflexão de formuladores de políticas públicas.

Apesar de suas contribuições, o estudo também apresenta algumas importantes fronteiras. A primeira diz respeito ao fato de a análise se concentrar exclusivamente em fontes documentais — leis, regulamentos e normas técnicas —, não incorporando entrevistas, estudos de caso ou avaliações empíricas sobre a implementação prática dessas medidas nas instituições financeiras. A segunda limitação decorre da própria dinâmica acelerada da regulação do setor financeiro e da segurança digital: normas evoluem constantemente, e alguns documentos podem ter sido atualizados após a fase de coleta. A terceira limitação refere-se à dificuldade de analisar com precisão o impacto real das regulamentações sobre a segurança do consumidor, dado que incidentes cibernéticos muitas vezes não são divulgados publicamente ou são reportados de forma incompleta.

Com base nessas fronteiras, algumas direções para pesquisas futuras são recomendadas. Estudos qualitativos com gestores de segurança digital, analistas de risco, supervisores do Banco Central e especialistas em proteção de dados poderiam aprofundar a compreensão sobre desafios práticos de implementação das normas. Pesquisas quantitativas poderiam avaliar se há correlação entre o fortalecimento regulatório do Banco Central e a redução de incidentes cibernéticos no setor financeiro, permitindo mensurar o impacto real das medidas adotadas. Além disso, estudos comparativos com outros países poderiam revelar caminhos alternativos para o avanço da soberania digital brasileira, especialmente no que diz respeito ao controle estatal de provedores estrangeiros de tecnologia e à governança dos fluxos internacionais de dados.

Ao final desse percurso, a reflexão que se impõe é que a proteção de dados e a segurança digital, no contexto financeiro, não podem ser compreendidas como metas definitivamente alcançáveis, mas como processos contínuos de adaptação, vigilância e reconstrução regulatória. O Banco Central desempenha papel estruturante, mas sua atuação só é plenamente efetiva quando articulada a práticas internas maduras das organizações e a políticas estatais integradas de soberania digital. O desafio do Brasil, portanto, não é apenas seguir produzindo normas, mas garantir que a proteção da informação se traduza em

autonomia tecnológica, transparência, equidade e segurança concreta para milhões de consumidores.

A análise comparativa das práticas de proteção de dados e segurança digital evidencia que, enquanto países como Alemanha, França, Canadá, Estados Unidos, Suíça e Singapura desenvolveram estruturas regulatórias robustas, mecanismos de fiscalização efetivos e abordagens tecnológicas proativas, o Brasil apresenta lacunas significativas na operacionalização de suas normas, especialmente em relação à fiscalização de serviços digitais estrangeiros e à mitigação de riscos para populações vulneráveis. Esse contraste aponta para um achado relevante deste estudo: os efeitos negativos da vigilância digital e do uso comercial de dados pessoais no Brasil — neste estudo pensado no setor de varejo financeiro — configuram um fenômeno local, característico do Sul Global, e não uma simples reprodução de padrões globais. A constatação reforça a necessidade de políticas públicas integradas que promovam proteção jurídica e soberania digital.

Em última instância, este estudo reforça que a soberania digital não se esgota na letra da lei, mas se realiza na capacidade de proteger dados, pessoas e instituições em um ambiente cada vez mais mediado por algoritmos e vulnerável a formas sofisticadas de exploração informacional. Numa era marcada por riscos cibernéticos globais e pela lógica do capitalismo de vigilância, garantir a integridade dos sistemas financeiros e a privacidade dos cidadãos não é apenas uma demanda técnica, mas um imperativo democrático. A verdadeira segurança digital, portanto, é aquela que promove autonomia, equidade e liberdade — bases indispensáveis para qualquer projeto de soberania no século XXI.

REFERÊNCIAS

AMER, K; NOUJAIM, J. **Privacidade hackeada.** Direção: Karim Amer; Jehane Noujaim. Estados Unidos: Netflix, 2019. Documentário.

ANDERSON, R. **Security engineering**: a guide to building dependable distributed systems. 3. ed. Indianapolis: Wiley, 2020.

AGÊNCIA BRASIL. Instabilidade do Pix coincide com pane global da AWS. Agência Brasil, 20 out. 2025. Disponível em: https://agenciabrasil.ebc.com.br. Acesso em: nov. 2025.

ARAL, S.; WALKER, D. Creating social contagion through viral product design: a randomized trial of word of mouth and referral program effects. **Marketing Science**, v. 34, n. 5, p. 1215-1234, 2015.

ARNER, D. W.; BARBERIS, J; BUCKLEY, R. P. **FinTech, RegTech and the Reconceptualization of Financial Regulation**. Cambridge: Cambridge University Press, 2020.

ASSAF NETO, A. **Mercado financeiro**. 14. ed. São Paulo: Atlas, 2021.

AYRES, I; BRAITHWAITE, J. **Responsive Regulation:** Transcending the Deregulation Debate. Oxford: Oxford University Press, 1992.

BALTAIAN, M. A New Data Protection Law in Switzerland. Still the Weakest Privacy Law in Western Europe? In: **Journal of International Business and Diplomacy**, Switzerland: International Institute in Geneva, v. 1, n. 1, p. 52-65, 2024.

BANCO CENTRAL DO BRASIL. **Estrutura do Banco Central**. Disponível em: https://www.bcb.gov.br/acessoinformacao/estruturabc.

BANCO CENTRAL DO BRASIL. **História Contada**. Disponível em: https://www.bcb.gov.br/historiacontada/index.html.

BANCO CENTRAL DO BRASIL. **Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.bcb.gov.br/acessoinformacao/lgpd.

BANCO CENTRAL DO BRASIL. **Relatório de Inclusão Financeira.** Brasília, 2023. Disponível em: https://www.bcb.gov.br.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 667, de 22 de setembro de 2025.** Disciplina a dispensa da observância do limite de emissão de Pix de valor superior a R$ 15.000,00 por instituição conectada à Rede do Sistema Financeiro Nacional por meio de Provedor de Serviços de Tecnologia da Informação. Diário Oficial da União, Brasília, DF, 22 set. 2025.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 666, de 22 de setembro de 2025.** Disciplina a dispensa da observância do limite de emissão de Transferência Eletrônica Disponível (TED) de valor igual ou superior a R$ 15.000,00 por instituição conectada à Rede do Sistema Financeiro Nacional por meio de Provedor de Serviços de Tecnologia da Informação. Diário Oficial da União, Brasília, DF, 22 set. 2025.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 664, de 11 de setembro de 2025.** Estabelece prazos para adequação de Provedor de Serviços de Tecnologia da Informação às regras de segurança da informação e gestão de fraudes previstas na Resolução BCB nº 498/2025. Diário Oficial da União, Brasília, DF, 11 set. 2025.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 637, de 13 de junho de 2025.** Divulga a versão 8.0 do Manual de Experiência do Cliente no Open Finance. Diário Oficial da União, Brasília, DF, 13 jun. 2025.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 374, de 26 de abril de 2023.** Divulga procedimentos e prazos relativos aos Sistemas de Mercado Financeiro no âmbito do Sistema de Pagamentos Brasileiro. Diário Oficial da União, Brasília, DF, 26 abr. 2023.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 305, de 15 de setembro de 2022.** Divulga a versão 4.0 do Manual de Segurança do Open Finance. Diário Oficial da União, Brasília, DF, 15 set. 2022.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 498, de 5 de setembro de 2025.** Disciplina os requisitos e procedimentos para credenciamento de Provedor de Serviços de Tecnologia da Informação no âmbito do Sistema Financeiro Nacional. Diário Oficial da União, Brasília, DF, 5 set. 2025.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 454, de 30 de janeiro de 2025.** Dispõe sobre a Estratégia de Uso de Software e de Serviços de Computação em Nuvem do Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 30 jan. 2025.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 447, de 19 de dezembro de 2024.** Altera normas para incluir sociedades corretoras e distribuidoras no escopo regulatório do Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 19 dez. 2024.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 400, de 4 de julho de 2024.** Dispõe sobre as diretrizes para o estabelecimento da Estrutura de Governança do Open Finance. Diário Oficial da União, Brasília, DF, 4 jul. 2024.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 386, de 5 de junho de 2024.** Divulga a Política de Conformidade (Compliance) do Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 5 jun. 2024.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 368, de 25 de janeiro de 2024.** Altera resoluções anteriores para inclusão de sociedades corretoras no escopo regulatório. Diário Oficial da União, Brasília, DF, 25 jan. 2024.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 366, de 17 de janeiro de 2024.** Divulga o Regulamento do Sistema de Informações Banco Central (Sisbacen). Diário Oficial da União, Brasília, DF, 17 jan. 2024.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 304, de 20 de março de 2023.** Aprova o Regulamento do Sistema de Pagamentos Brasileiro e consolida normas sobre liquidação e registro de ativos financeiros. Diário Oficial da União, Brasília, DF, 20 mar. 2023.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 287, de 24 de janeiro de 2023.** Divulga a Política de Segurança da Informação do Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 24 jan. 2023.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 286, de 24 de janeiro de 2023.** Institui o Regulamento de Governança do Portal de Internet do Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 24 jan. 2023.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 265, de 25 de novembro de 2022.** Dispõe sobre a estrutura de gerenciamento de riscos e de capital para conglomerados prudenciais do Tipo 3. Diário Oficial da União, Brasília, DF, 25 nov. 2022.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 250, de 5 de outubro de 2022**. Divulga o Regulamento do Comitê de Governança da Informação. Diário Oficial da União, Brasília, DF, 5 out. 2022.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 249, de 5 de outubro de 2022.** Divulga a Política de Governança da Informação do Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 5 out. 2022.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 204, de 22 de março de 2022.** Dispõe sobre o compartilhamento de dados de operações do Sistema de Operações do Crédito Rural e do Proagro. Diário Oficial da União, Brasília, DF, 22 mar. 2022.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 201, de 11 de março de 2022.** Dispõe sobre metodologia simplificada para apuração do Patrimônio de Referência Simplificado. Diário Oficial da União, Brasília, DF, 11 mar. 2022.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 198, de 11 de março de 2022.** Dispõe sobre o requerimento mínimo de Patrimônio de Referência de Instituições de Pagamento. Diário Oficial da União, Brasília, DF, 11 mar. 2022.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 85, de 8 de abril de 2021**. Dispõe sobre a política de segurança cibernética e requisitos para contratação de serviços de computação em nuvem. Diário Oficial da União, Brasília, DF, 8 abr. 2021.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 1, de 12 de agosto de 2020.** Institui o arranjo de pagamentos Pix e aprova o seu Regulamento. Diário Oficial da União, Brasília, DF, 12 ago. 2020.

BRASIL. Conselho Monetário Nacional. **Resolução CMN nº 5.105, de 28 de setembro de 2023.** Estabelece diretrizes para constituição e funcionamento de sociedades corretoras e distribuidoras de valores mobiliários. Diário Oficial da União, Brasília, DF, 28 set. 2023.

BRASIL. Conselho Monetário Nacional. **Resolução CMN nº 5.076, de 18 de maio de 2023.** Altera as Resoluções nº 4.557/2017 e nº 4.606/2017. Diário Oficial da União, Brasília, DF, 18 maio 2023.

BRASIL. Conselho Monetário Nacional. **Resolução CMN nº 4.893, de 26 de fevereiro de 2021.** Dispõe sobre a política de segurança cibernética das instituições autorizadas a funcionar pelo Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 26 fev. 2021.

BRASIL. Conselho Monetário Nacional. **Resolução CMN nº 4.606, de 19 de outubro de 2017.** Dispõe sobre metodologia simplificada de apuração do Patrimônio de Referência Simplificado. Diário Oficial da União, Brasília, DF, 19 out. 2017.

BRASIL. Conselho Monetário Nacional. **Resolução CMN nº 4.557, de 23 de fevereiro de 2017**. Dispõe sobre a estrutura de gerenciamento de riscos e de capital. Diário Oficial da União, Brasília, DF, 23 fev. 2017.

BRASIL. **Conselho Monetário Nacional. Resolução CMN nº 4.282, de 4 de novembro de 2013.** Estabelece diretrizes para regulamentação e supervisão das instituições de pagamento

integrantes do Sistema de Pagamentos Brasileiro. Diário Oficial da União, Brasília, DF, 4 nov. 2013.

BRASIL. Banco Central do Brasil; BRASIL. **Conselho Monetário Nacional. Resolução Conjunta nº 6, de 23 de maio de 2023.** Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes. Diário Oficial da União, Brasília, DF, 23 maio 2023.

BRASIL. Banco Central do Brasil; BRASIL. **Conselho Monetário Nacional. Resolução Conjunta nº 1, de 4 de maio de 2020.** Dispõe sobre a implementação do Open Finance. Diário Oficial da União, Brasília, DF, 4 maio 2020.

BELLI, L.; RAMOS, B.(Orgs.). **Políticas Digitais no Brasil**: Acesso à Internet, Proteção de Dados e Regulação. 1. ed. Rio de Janeiro: FGV Direito Rio, 2021.

BENTES, A. **Quase um tique:** economia da atenção, vigilância e espetáculo em uma rede social. Rio de Janeiro: Editora UFRJ, 2021.

BHARATI, P.; CHAUDHURY, A. Social media and marketing: a case study of Facebook. **Journal of Business Strategies**, v. 29, n. 2, p. 1-14, 2012.

BORGES, M. A. A. A digitalização e as novas formas de discriminação: um estudo sobre a interseccionalidade no contexto da tecnologia. **Revista Brasileira de Estudos de População**, São Paulo, v. 37, n. 1, p. 1-18, 2020.115-134, 2021.

BRASIL. **Estratégia Nacional de Segurança Cibernética.** Brasília: Presidência da República, 2020.

BRASIL. Lei nº 4.595, de 31 de dezembro de 1964. **Dispõe sobre a política e as instituições monetárias, bancárias e creditícias, cria o Conselho Monetário Nacional e dá outras providências**. Diário Oficial da União: seção 1, Brasília, DF, 31 dez. 1964.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. **Dispõe sobre os direitos autorais e a proteção das obras intelectuais.** Diário Oficial da União, Brasília, DF, 20 fev. 1998.

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

BRASIL. Lei nº 10.695, de 1º de julho de 2003. **Estabelece o Sistema Nacional de Segurança Pública**. Diário Oficial da União, Brasília, DF, 2 jul. 2003.

BRASIL. Lei nº 10.703, de 18 de agosto de 2004. **Institui a Política Nacional de Segurança da Informação.** Diário Oficial da União, Brasília, DF, 19 ago. 2004.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Tipifica crimes cibernéticos.** Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Dispõe sobre a regulamentação da Internet no Brasil.** Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Institui a Lei Geral de Proteção de Dados Pessoais**. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. **Regulamenta a Lei de Acesso à Informação.** Diário Oficial da União, Brasília, DF, 12 mai. 2016.

BRASIL. Lei nº 14.010, de 10 de junho de 2020. **Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19) .** Diário Oficial da União, Brasília, DF, 11 jun. 2020.

BRASIL. Lei nº 14.129, de 29 de março de 2021. **Dispõe sobre a transformação digital dos serviços públicos**. Diário Oficial da União, Brasília, DF, 30 mar. 2021.

BRASIL. Lei nº 14.155, de 27 de julho de 2021. **Altera a Lei nº 12.737, de 30 de novembro de 2012**. Diário Oficial da União, Brasília, DF, 28 jul. 2021.

BUCKLEY, G. GDPR and the indefinable effectiveness of privacy regulators. **Cybersecurity**, v.10, n.1, 2024.

CARVALHO, M. A. **Capitalismo de vigilância:** a privacidade na sociedade da informação. 2019. 102 f. Dissertação (Mestrado em Direito) - Universidade Federal de Sergipe, São Cristóvão, SE, 2019.

CASTELLS, Manuel. **O poder da Comunicação**. 3. ed. São Paulo: Paz e Terra, 2014.

CASTELLS, Manuel. **A sociedade em rede:** a era da informação: economia, sociedade e cultura.. 5. ed. São Paulo: Paz e Terra, 2013.

CHIK, W. B. The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. **Computer Law & Security Review**, v. 29, n. 5, 2013.

CNDL. Pesquisa sobre segurança nas transações online. **Confederação Nacional de Dirigentes Lojistas**, 2022. Disponível em: https://www.cndl.org.br.

COHEN, J E. What privacy is for. **Harvard Law Review**, v. 126, n. 7, p. 1904-1933, 2013.

COULDREY, N; MEJIAS, P, J. Data colonialism: rethinking big data's relation to the contemporary global order. **Television & New Media**, v. 20, n. 4, p. 334-352, 2019.

CRAWFORD, K. **Atlas da IA**: poder, política e os custos planetários da inteligência artificial. São Paulo: Editora Objetiva, 2022.

CRESWELL, J. W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. Porto Alegre: Bookman, 2007.

DENARDIS, L. **The global politics of Internet governance.** New Haven: Yale University Press, 2014.

ESTADO DE MINAS. **Problemas técnicos impactam Pix durante pane global**. Estado de Minas, 20 out. 2025. Disponível em: https://www.em.com.br. Acesso em: nov. 2025.

FAUSTINO, D. Colonialismo de dados: a nova era da extração digital. **Revista de Estudos Interdisciplinares**, v. 4, n. 1, p. 12-30, 2020.

FEBRABAN. Relatório de Segurança: fraudes e golpes no meio digital. São Paulo: **Federação Brasileira de Bancos**, 2021. Disponível em: https://www.febraban.org.br.

FEBRABAN. Estudo sobre fraudes digitais e o uso do Pix. São Paulo: Federaç**ão Brasileira de Bancos**, 2022. Disponível em: https://www.febraban.org.br.

FERREIRA, J. **Segurança da Informação:** Teoria e Prática. Rio de Janeiro: Editora Ciência Moderna, 2019.

FERREIRA, M. de A.; CAMPOS. E. **Governança de Dados e Compliance na Área Financeira**. São Paulo: Atlas, 2020.

FERREIRA, L. V. A. **O papel da auditoria interna na gestão de riscos cibernéticos em instituições financeiras brasileiras:** estudo sob a perspectiva das três linhas. 2024. Dissertação (Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília, 2024.

FERARRI, A.; FARANDA, A. **Security and governance in cloud banking:** The ECB's guide to cloud services outsourcing. 2024.

FISERV. **Dois anos de Pix: confira os avanços do varejo brasileiro**. 2022. Disponível em: https://www.fiserv.com.br/insights/2-anos-de-pix--entenda-quais-foram-os-avancos-no-varejo . Acesso em: 20 out. 2025.

FOUCAULT, M. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. 47. ed. Petrópolis: Vozes, 2014.

FUCHS, C. **Social media:** a critical introduction. London: Sage Publications, 2017.

GOMES, J. R. A coleta de dados e a transparência nas plataformas digitais: um estudo sobre a aceitação das políticas de privacidade. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, v. 13, n. 2, p. 112-124, 2019.

GILLIOM, J; MONAHAN,T. **Supervision**: An Introduction to the Study of Surveillance. Chicago: University of Chicago Press, 2010.

GONÇALVES, T. **Lei Geral de Proteção de Dados**: Impactos e Desafios para o Setor Financeiro. Rio de Janeiro: Lumen Juris, 2023.

GONÇALVES, B. F. C. **A inteligência artificial aplicada à personalização no e-commerce.** 2024. Dissertação (Mestrado em Marketing Digital) — Instituto Superior de Contabilidade e Administração do Porto, Politécnico do Porto, Porto, 2024.

GONZALEZ, R.; ROEDER, M.; MCGILL, T.. Facebook's Like buttons and the tracking of users: An empirical analysis. **Journal of Digital Privacy and Security**, v. 3, n. 2, p. 45-62, 2017.

GROVE, S. The future of the digital economy: the rise of digital security. In: **Digital economy:** the new frontier. New York: Harper Business, 2021.

HANNA, R.; ROHM, A. J.; CRITTENDEN, V. L. We're all connected: the power of the social media ecosystem. **Business Horizons**, v. 54, n. 3, p. 265-273, 2011.

HODDER, Ian. **Entangled**: an archaeology of the relationships between humans and things. Malden: Wiley-Blackwell, 2012.

HUANG, L.; BENYOUCEF, M. User behavior in social commerce: the role of trust and social influence. **Journal of Business Research**, v. 88, p. 308-315, 2018.

HWANG, T. The Attention Economy: A Critical Review. **International Journal of Information Management**, v. 45, p. 53-63, 2019.

IBM. Relatório sobre segurança da informação. **IBM**, 2021. Disponível em: https://www.ibm.com/security.

INFOMONEY. **Usuários relatam instabilidade no Pix em meio a falhas globais na AWS**. InfoMoney, 20 out. 2025. Disponível em: https://www.infomoney.com.br
. Acesso em: nov. 2025.

INTERNATIONAL TECHONOLOGY & INNOVATION FOUNDATION — ITIF. Technical and Legal Criteria for Assessing Cloud Trustworthiness. Washington, DC: **Information Technology & Innovation Foundation** — ITIF, 2024.

KREBS, B. **DDoS on Dyn Impacts Twitter, Spotify, Reddit.** Krebs on Security, october, 2016. Disponível em: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

LIMA, G. P. **Varejo e governo: o pilar varejo no sistema bancário.** 2009. Dissertação (Mestrado em Administração) – Universidade Federal do Ceará, Fortaleza, 2009.

LIPPOLD, W. Dados como recursos: a nova lógica de exploração. In: **Conferência Internacional sobre Tecnologia e Sociedade**, 2020. Anais... São Paulo: Universidade XYZ, 2020. p. 45-60.

LIU, Y.; ARORA, N. The impact of personalized recommendations on online consumer behavior. **Journal of Marketing Research**, v. 50, n. 4, p. 489-503, 2013.

LOPEZ, F. J.; BIANCHINI, L. M.; TAVARES, F. M. Algorithmic Credit Scoring: The Risks of Discrimination in Access to Credit. **Revista Brasileira de Política Internacional**, Brasília, v. 64, n. 2, p. 1-20, 2021.

LOPÉZ, C. et al. The role of social media in marketing: the case of Facebook. **Journal of Business Research**, v. 85, 2018.

LUMI KAMIMURA MURATA, D. A. M.; RITZMANN TORRES, M. P. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?. **Boletim IBCCRIM**, [S. l.], v. 31, n. 368, 2023.

LYON, D. **A cultura da vigilância**: assistindo como um estilo de vida. Rio de Janeiro: Editora FGV, 2019.

MACHADO, D. A modulação de comportamento nas plataformas de mídias sociais. In: SOUZA, J.; AVELINO, R.; SILVEIRA, S. A. da (orgs.). **A sociedade de controle:** manipulação e modulação nas redes digitais. São Paulo: Hedra, 2018. p. 47–69.

MARTINS, R. S.; SOUZA, E. A. A complexidade dos termos de uso: implicações para a privacidade dos usuários. **Estudos em Comunicação**, Porto Alegre, v. 15, n. 2, p. 89-104, 2019.

MARTINS DE OLIVEIRA, M.; BARILE DA SILVEIRA, D.; MACENA DIAS DE OLIVEIRA, M. G. Análise comparada das normas de proteção de dados do Brasil, da União Europeia e do estado da Califórnia – EUA: LGPD x GDPR x CCPA. **Revista de Direito, Governança e Novas Tecnologias**, v. 10, n. 2, 2025.

MEYER, R. A. A evolução dos serviços bancários digitais: implicações para o consumidor e o mercado. **Revista de Finanças e Contabilidade**, v. 12, n. 1, p. 45-60, 2021.

MINAYO, M. C. de S. (Org.). **Pesquisa social:** teoria, método e criatividade. Petrópolis, RJ: Vozes, 1996.

MORAES, M. M. de; WOSZCZYNA, F. D. Algoritmos e desigualdade social: a exclusão no acesso a serviços financeiros. **Revista de Administração Pública**, Rio de Janeiro, v. 53, n. 6, p. 1333-1351, 2019.

MORAES, R. R. de; ALMEIDA, M. C. de. YouTube como plataforma de desinformação: o impacto das recomendações algorítmicas. **Revista de Comunicação e Sociedade**, v. 19, n. 1, p. 85-102, 2020.

MORELLATO, A. C; SANTOS, A. F. P. R. Capitalismo de vigilância e a Lei Geral de Proteção de Dados: perspectivas sobre consentimento, legítimo interesse e anonimização. **Revista Brasileira de Sociologia do Direito**, v. 8, n. 2, maio/ago. 2021.

NARAYANAN, A; SHMATIKOV, V. **Robust de-anonymization of large sparse datasets. In: IEEE Symposium on Security and Privacy**, 2008, Oakland. Proceedings… Oakland: IEEE, 2008. p. 111–125.

NISSENBAUM, H. **Privacy in Context:** Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

NOBLE, S. U. **Algorithms of Oppression:** How Search Engines Reinforce Racism. New York: NYU Press, 2018.

O'NEIL, C. **Weapons of Math Destruction:** How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishing Group, 2016.

PATI, C. **Brasil tem 4,6 mil tentativas de golpes financeiros e digitais por hora**. Revista Veja - Economia, 13 ago 2024. Disponível em: https://veja.abril.com.br/economia/brasil-tem-46-mil-tentativas-de-golpe-financeiro-digital-por-hora

PEREIRA, L. F. de A.; LIMA, R. M. de. A polarização nas redes sociais: o caso do YouTube. **Comunicação & Sociedade**, v. 32, p. 145-160, 2018.

PEREIRA, A. Plataformas digitais: uma nova economia em construção. **Revista de Administração de Empresas**, São Paulo, v. 59, n. 3, p. 238-249, 2019.

PEREIRA, J. R. Educação financeira e segurança digital: a importância da conscientização do consumidor. **Revista Brasileira de Finanças**, v. 13, n. 2, p. 45-60, 2019.

PERROW, C. **Normal Accidents**: Living with High-Risk Technologies. Princeton: Princeton University Press, 1999.

QUIJANO, A. Colonialidade, poder, globalização e democracia. **Revista Novos Rumos**, [S. l.], n. 37, 2022.

ROCHA, L. D.; CANEDO, E. D. Optimizing Compliance: Comparative Study of Data Laws and Privacy Frameworks. **Journal of Internet Services and Applications**, 2025.

SAAL, C.; KRAWCZYK, T.; MOOS, T.; et al. Cloud Outsourcing in the Financial Sector: An Assessment of Internal Governance Strategies on a Cloud Transaction Between a Bank and a Leading Cloud Service Provider. **European Business Organization Law Review**, v. 23, p. 905-936, 2022.

SAMPAIO, J. A. L. Datificação E Vigilância: o judiciário é guardião dos direitos fundamentais na sociedade digital?. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 16, n. 46, p. 155–175, 2022.

SAMPAIO, J. A. L; COSTA, A. C. M. T. Capitalismo de vigilância e modulação do comportamento humano: o ambiente digital como espaço favorável à manipulação do eleitor?. **Opinión Jurídica**, Medellín , v. 24, n. 52, a4542, Dec. 2025 .

SAMPI.NET.BR. **AWS e instabilidade do Pix: impactos e análise**. Sampi.net.br, 20 out. 2025. Disponível em: https://www.sampi.net.br. Acesso em: nov. 2025.

SANTOS, M. **Por uma outra globalização**: do pensamento único à consciência universal. 10. ed. Rio de Janeiro: Record, 2003.

SANTOS, L. L. dos; OLIVEIRA, T. D. de. A economia da atenção e o papel das plataformas digitais na formação da opinião pública. **Revista Brasileira de Política Internacional**, v. 62, n. 1, p. 1-20, 2019.

SCHNEIER, B. **Data and Goliath:** The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton, 2015.

SERASA EXPERIAN. **Fraudes digitais disparam entre jovens: tentativas de golpe crescem 50% entre pessoas de até 25 anos, revela Serasa Experian**. São Paulo, 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/fraudes-digitais-disparam-entre-jovens-tentativas-de-golpe-crescem-50-entre-pessoas-de-ate-25-anos-revela-serasa-experian. Acesso em: out. 2025.

SERASA EXPERIAN. **Fraudômetro: país evita perdas de R$ 39,8 bilhões em golpes no 1º semestre, projeta Serasa Experian**. São Paulo, 2025. Disponivel em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/fraudometro-pais-evita-perdas-de-rdollar-398-bilhoes-em-golpes-no-1-semestre-projeta-serasa-experian/?utm_source=chatgpt.com. Acesso em: Julho 2025.

SILVA, J. A criação do Sistema Financeiro Nacional: contexto histórico e objetivos da Lei nº 4.595/1964. **Revista Brasileira de Economia**, Rio de Janeiro, v. 58, n. 2, p. 123-145, abr./jun. 2004.

SILVA, T. **Algoritmos e desigualdade:** como as tecnologias digitais perpetuam a exclusão social. Edições Sesc SP. 2022.

SILVA, F. C. da; LIMA, R. P. de. O papel da economia da atenção nas estratégias de comunicação digital. **Revista Brasileira de Gestão de Negócios**, v. 21, n. 4, p. 720-733, 2019.

SILVA, A. P.; MORAES, T. F. Cibersegurança em instituições financeiras: desafios e oportunidades. **Journal of Financial Technology**, v. 5, n. 1, p. 25-40, 2020.

SILVEIRA, S. A. Governo dos algoritmos. Revista de Políticas Públicas, v. 21, n. 1, p. 267–282, 2017.

SILVEIRA, S. A. A noção de modulação e os sistemas algorítmicos. In: SOUZA, J.; AVELINO, R.; SILVEIRA, S. A. da (orgs.). **A sociedade de controle:** manipulação e modulação nas redes digitais. São Paulo: Hedra, 2018. p. 31–46.

SILVEIRA, S. A. da. **Democracia e os códigos invisíveis:** como os algoritmos estão modulando comportamentos e escolhas políticas. São Paulo: Edições Sesc, 2019.

SILVEIRA, A. L. F. da; SANTOS, R. M. dos. A tecnologia como instrumento de discriminação: a vulnerabilidade dos grupos sociais em relação aos algoritmos. **Revista Brasileira de Política Internacional**, Brasília, v. 62, n. 1, p. 1-20, 2019.

SILVEIRA, S. A. da. Inteligência artificial baseada em dados e as operações do capital. PAULUS: **Revista de Comunicação da FAPCOM**, [S. l.], v. 5, n. 10, 2021.

SILVEIRA, D. B; OLIVEIRA, M. G. M. D. de; MOZANER, V. C. Os impactos da regulação sobre privacidade e proteção de dados na segurança da informação: um estudo à luz da GDPR e da LGPD. **Revista de Direito Administrativo, Infraestrutura, Regulação e Compliance**, n. 30, p. 49-65, jul./set. 2024.

SINGH, S; LYON, D. **Surveilling consumers:** the social consequences of data processing on Amazon.com. In: KOSKELA, H.; PELTONEN, J. (orgs.). The Routledge Companion to Digital Consumption. 1. ed. Abingdon: Routledge, 2012. p. 14.

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2011.

STALLINGS, W; KATZ, L. **Computer Security:** Principles and Practice. 4. ed. Boston: Pearson, 2018.

SOUZA, C. E. R.; EUGÊNIO, L. M. S.; ARAÚJO, N. V. DE S. Da Europa ao Brasil: um estudo comparativo entre o GDPR e a LGPD. Anais da ERSIMT, 2025. Disponível em: https://sol.sbc.org.br/index.php/ersimt/article/view/35789. Acesso em: dez. 2025.

SULLIVAN, D. Colonial Pipeline ransomware attack: What we know about the cyberattack and its aftermath. **CNN Business**, 2021.

TOURINHO, Vanessa Pereira. **Cibersegurança bancária no Brasil:** avaliação da aderência às orientações do Banco de Compensações Internacionais (BIS). 2025. Dissertação (Mestrado) — Fundação Getúlio Vargas, 2025.

UNION EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Diário Oficial da União Europeia**, Bruxelas, 4 maio 2016.

VIANNA, F. Se os Dados são o Novo Petróleo, Onde Estão os Royalties? O Neoliberalismo na Era do Capitalismo de Vigilância. **Revista Gestão & Conexões**, [S. l.], v. 10, n. 3, p. 123–143, 2021.

VILELA, M. E. M.; GIOLO JÚNIOR, C. Lei Geral de Proteção de Dados (LGPD) e General Data Protection Regulation (GDPR): Uma análise entre os principais elementos das legislações. **Revista Direito França**, 2023.

WOODS, D. D.; SIMPSON, A. **Resilience Engineering**: Concepts and Precepts. Farnham: Ashgate, 2017.

ZARSKY, J. WannaCry Ransomware Attack: An Overview of the Impact. **Journal of Cybersecurity**, v. 3, n. 4, p. 45-60, 2018.

ZHANG, J.; ZHAO, S. J. Personalization in e-commerce: the role of customer reviews and recommendations. **International Journal of Information Management**, v. 35, n. 2, p. 174-183, 2015.

ZUBOFF, S. **Big Other:** surveillance capitalism and the prospects of an information civilization", Journal of Information Technology, v. 30, 2015, p. 75-89. In: BRUNO, F, et al. Tecnopolíticas da vigilância : perspectivas da margem- 1. ed. São Paulo :Boitempo, 2018.

ZUBOFF, S. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

ANEXO 1 - Resultados da pesquisa nas legislações brasileiras entre 1998 e 2025

Legislações brasileiras onde foram realizadas as buscas:

- 1988 - Constituição Federal
- 1998 - Lei nº 9.610 (Lei dos direitos autorais)
- 2002 - Lei nº 10.406 (Código Civil)
- 2003 - Lei nº 10.695 (Lei da Pirataria)
- 2004 - Lei nº 10.703
- 2012 - Lei nº 12.737 (Lei Carolina Dieckmann)
- 2014 - Lei nº 12.965 (Marco Civil da Internet)
- 2016 - Decreto nº 8.771
- 2018 - Lei nº 13.709 (Lei Geral de Proteção de Dados - LGPD)
- 2020 - Estratégia Nacional de Segurança Cibernética (ENSC)
- 2020 - Lei nº 14.010 (Lei da Pandemia)
- 2021 - Lei nº 14.129 (Lei de Governo Digital)2021 - Lei nº 14.155
- 2023 - Decreto Nº 11.491 (Promulgação da Convenção sobre o Crime Cibernético)
- 2025 - Decreto Nº 12.573, de 4 de agosto de 2025 (E-Ciber - Estratégia Nacional de Cibersegurança 2025)

Termos de busca utilizados:

- Banco Central - Banco.
- Crime Cibernético - Crimes Cibernéticos - Crimes Informáticos - Cibercrime - Crime Digital - Infração Cibernética - Delitos Informáticos - Crimes de Violação de Dispositivo Informático.
- Proteção de dados - Proteção dos dados, Proteção a dados, Proteção de seus dados, Dados.
- Segurança Digital - Digital, Digitais.
- Soberania digital

1988 - CONSTITUIÇÃO DE FEDERAL

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BANCO CENTRAL - BANCO

O termo **"Banco Central"** aparece **8 vezes**. Além disso, o termo **"Banco"**, de forma isolada, aparece em mais **9 ocasiões**, totalizando de **17 resultados**

TERMO "BANCO CENTRAL"

1) Art. 52. Compete privativamente ao Senado Federal:

III - aprovar previamente, por voto secreto, após argüição pública, a escolha de:

d) Presidente e diretores do **banco central**;

2) Art. 84. Compete privativamente ao Presidente da República:

XIV - nomear, após aprovação pelo Senado Federal, os Ministros do Supremo Tribunal Federal e dos Tribunais Superiores, os Governadores de Territórios, o Procurador-Geral da República, o presidente e os diretores do **banco central** e outros servidores, quando determinado em lei;

3) Art. 164. A competência da União para emitir moeda será exercida exclusivamente pelo **banco central**.

4) § 1º É vedado ao **banco central** conceder, direta ou indiretamente, empréstimos ao Tesouro Nacional e a qualquer órgão ou entidade que não seja instituição financeira.

5) § 2º O **banco central** poderá comprar e vender títulos de emissão do Tesouro Nacional, com o objetivo de regular a oferta de moeda ou a taxa de juros.

6) § 3º As disponibilidades de caixa da União serão depositadas no **banco central**; as dos Estados, do Distrito Federal, dos Municípios e dos órgãos ou entidades do Poder Público e das empresas por ele controladas, em instituições financeiras oficiais, ressalvados os casos previstos em lei.

7) Art. 47. Na liquidação dos débitos, inclusive suas renegociações e composições posteriores, ainda que ajuizados, decorrentes de quaisquer empréstimos concedidos por bancos e por instituições financeiras, não existirá correção monetária desde que o empréstimo tenha sido concedido:

V - se o beneficiário não for proprietário de mais de cinco módulos rurais.

§ 6º A concessão do presente benefício por bancos comerciais privados em nenhuma hipótese acarretará ônus para o Poder Público, ainda que através de refinanciamento e repasse de recursos pelo **banco central**.

8) Art. 97. Até que seja editada a lei complementar de que trata o § 15 do art. 100 da Constituição Federal, os Estados, o Distrito Federal e os Municípios que, na data de publicação desta Emenda Constitucional, estejam em mora na quitação de precatórios vencidos, relativos às suas administrações direta e indireta, inclusive os emitidos durante o período de vigência do regime especial instituído por este artigo, farão esses pagamentos de acordo com as normas a seguir estabelecidas, sendo inaplicável o disposto no art. 100 desta Constituição Federal, exceto em seus §§ 2º, 3º, 9º, 10, 11, 12, 13 e 14, e sem prejuízo dos acordos de juízos conciliatórios já formalizados na data de promulgação desta Emenda Constitucional. (Incluído pela Emenda Constitucional nº 62, de 2009) (Vide Emenda Constitucional nº 62, de 2009)

§ 9º Os leilões de que trata o inciso I do § 8º deste artigo: (Incluído pela Emenda Constitucional nº 62, de 2009)

I - serão realizados por meio de sistema eletrônico administrado por entidade autorizada pela Comissão de Valores Mobiliários ou pelo **Banco Central** do Brasil; (Incluído pela Emenda Constitucional nº 62, de 2009).

TERMO "BANCO"

1) Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

   LXXII - conceder-se-á "habeas-data":

   a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou **bancos** de dados de entidades governamentais ou de caráter público;

2) Art. 239. A arrecadação decorrente das contribuições para o Programa de Integração Social, criado pela Lei Complementar nº 7, de 7 de setembro de 1970, e para o Programa de Formação do Patrimônio do Servidor Público, criado pela Lei Complementar nº 8, de 3 de dezembro de 1970, passa, a partir da promulgação desta Constituição, a financiar, nos termos que a lei dispuser, o programa do seguro-desemprego, outras ações da previdência social e o abono de que trata o § 3º deste artigo.(Redação dada pela Emenda Constitucional nº 103, de 2019)

   § 1º Dos recursos mencionados no caput, no mínimo 28% (vinte e oito por cento) serão destinados para o financiamento de programas de desenvolvimento econômico, por meio do **Banco** Nacional de Desenvolvimento Econômico e Social, com critérios de remuneração que preservem o seu valor. (Redação dada pela Emenda Constitucional nº 103, de 2019).

3) Art. 34. O sistema tributário nacional entrará em vigor a partir do primeiro dia do quinto mês seguinte ao da promulgação da Constituição, mantido, até então, o da Constituição de 1967, com a redação dada pela Emenda nº 1, de 1969, e pelas posteriores.

   § 10. Enquanto não entrar em vigor a lei prevista no art. 159, I, "c", cuja promulgação se fará até 31 de dezembro de 1989, é assegurada a aplicação dos recursos previstos naquele dispositivo da seguinte maneira:

   III - o percentual relativo ao Fundo de Participação dos Municípios, a partir de 1989, inclusive, será elevado à razão de meio ponto percentual por exercício financeiro, até atingir o estabelecido no art. 159, I, "b".

   I - seis décimos por cento na Região Norte, através do **Banco** da Amazônia S.A.;

4) II - um inteiro e oito décimos por cento na Região Nordeste, através do **Banco** do Nordeste do Brasil S.A.;
5) III - seis décimos por cento na Região Centro-Oeste, através do **Banco** do Brasil S.A.
6) § 11. Fica criado, nos termos da lei, o **Banco** de Desenvolvimento do Centro-Oeste, para dar cumprimento, na referida região, ao que determinam os arts. 159, I, "c", e 192, § 2º, da Constituição.
7) Art. 47. Na liquidação dos débitos, inclusive suas renegociações e composições posteriores, ainda que ajuizados, decorrentes de quaisquer empréstimos concedidos por **bancos** e por instituições financeiras, não existirá correção monetária desde que o empréstimo tenha sido concedido:
8) V - se o beneficiário não for proprietário de mais de cinco módulos rurais.

   § 5º No caso de operações com prazos de vencimento posteriores à data- limite de liquidação da dívida, havendo interesse do mutuário, os **bancos** e as instituições financeiras promoverão, por instrumento próprio, alteração nas condições contratuais originais de forma a ajustá-las ao presente benefício.

9) § 6º A concessão do presente benefício por **bancos** comerciais privados em nenhuma hipótese acarretará ônus para o Poder Público, ainda que através de refinanciamento e repasse de recursos pelo banco central.

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo“**Proteção dos dados**” aparece **1 vez**. Além disso, o termo "**Dados**", de forma isolada, aparece em mais **9 ocasiões**, totalizando **10 resultados**.

TERMO “PROTEÇÃO DOS DADOS”

1. TÍTULO II

   Dos Direitos e Garantias Fundamentais

   CAPÍTULO I

   DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS

   LXXIX - é assegurado, nos termos da lei, o direito à **proteção dos dados** pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)

TERMO “DADOS”

1) Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

   XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de **dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)

1. LXXII - conceder-se-á "habeas-data":

   a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de **dados** de entidades governamentais ou de caráter público;

2. b) para a retificação de **dados**, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
3. Art. 21. Compete à União:

   XXVI - organizar e fiscalizar a proteção e o tratamento de **dados** pessoais, nos termos da lei. (Incluído pela Emenda Constitucional nº 115, de 2022)

4. Art. 22. Compete privativamente à União legislar sobre:

   XXX - proteção e tratamento de **dados** pessoais. (Incluído pela Emenda Constitucional nº 115, de 2022)

5. Art. 162. A União, os Estados, o Distrito Federal e os Municípios divulgarão, até o último dia do mês subseqüente ao da arrecadação, os montantes de cada um dos tributos arrecadados, os recursos recebidos, os valores de origem tributária entregues e a entregar e a expressão numérica dos critérios de rateio.

   Parágrafo único. Os **dados** divulgados pela União serão discriminados por Estado e por Município; os dos Estados, por Município.

6. (7 e 8) Art. 163-A. A União, os Estados, o Distrito Federal e os Municípios disponibilizarão suas informações e **dados** contábeis, orçamentários e fiscais, conforme periodicidade, formato e sistema estabelecidos pelo órgão central de contabilidade da União, de forma a garantir a rastreabilidade, a comparabilidade e a publicidade dos **dados** coletados, os quais deverão ser divulgados em meio eletrônico de amplo acesso público. (Incluído pela Emenda Constitucional nº 108, de 2020).
7. (7 e 8) Art. 163-A. A União, os Estados, o Distrito Federal e os Municípios disponibilizarão suas informações e **dados** contábeis, orçamentários e fiscais, conforme periodicidade, formato e sistema estabelecidos pelo órgão central de contabilidade da União, de forma a garantir a rastreabilidade, a

comparabilidade e a publicidade dos **dados** coletados, os quais deverão ser divulgados em meio eletrônico de amplo acesso público. (Incluído pela Emenda Constitucional nº 108, de 2020).

8. Art. 130. Resolução do Senado Federal fixará, para todas as esferas federativas, as alíquotas de referência dos tributos previstos nos arts. 156-A e 195, V, da Constituição Federal, observados a forma de cálculo e os limites previstos em lei complementar, de forma a assegurar: (Incluído pela Emenda Constitucional nº 132, de 2023)

   § 10. O cálculo das alíquotas a que se refere este artigo será realizado com base em propostas encaminhadas pelo Poder Executivo da União e pelo Comitê Gestor do Imposto sobre Bens e Serviços, que deverão fornecer ao Tribunal de Contas da União todos os subsídios necessários, mediante o compartilhamento de **dados** e informações, nos termos de lei complementar. (Incluído pela Emenda Constitucional nº 132, de 2023)

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

O termo "**Digitais**" aparece **2 vezes**, totalizando **2 resultados**.

TERMO "DIGITAIS"

1. Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

   LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios **digitais**. (Incluído pela Emenda Constitucional nº 115, de 2022)

2. Art. 150. Sem prejuízo de outras garantias asseguradas ao contribuinte, é vedado à União, aos Estados, ao Distrito Federal e aos Municípios:

   VI - instituir impostos sobre: (Vide Emenda Constitucional nº 3, de 1993)

   e) fonogramas e videofonogramas musicais produzidos no Brasil contendo obras musicais ou literomusicais de autores brasileiros e/ou obras em geral interpretadas por artistas brasileiros bem como os suportes materiais ou arquivos **digitais** que os contenham, salvo na etapa de replicação industrial de mídias ópticas de leitura a laser. (Incluída pela Emenda Constitucional nº 75, de 15.10.2013)

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

1998 - LEI Nº 9.610 (Lei dos direitos autorais)

https://www.planalto.gov.br/ccivil_03/leis/l9610.htm#:~:text=L9610&text=LEI%20N%C2%BA%209.610%2C%20DE%2019%20DE%20FEVEREIRO%20DE%201998.&text=Altera%2C%20atualiza%20e%20consolida%20a,autorais%20e%20d%C3%A1%20outras%20provid%C3%AAncias.&text=Art.%201%C2%BA%20Esta%20Lei%20regula,os%20que%20lhes%20s%C3%A3o%20conexos.

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação.

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **"Dados"** aparece **8 vezes**, totalizando **8 resultados**.

TERMO "DADOS"

1. Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como:

   XIII - as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de **dados** e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual.

2. (2 e 3) § 2º A proteção concedida no inciso XIII não abarca os **dados** ou materiais em si mesmos e se entende sem prejuízo de quaisquer direitos autorais que subsistam a respeito dos **dados** ou materiais contidos nas obras.
3. (2 e 3) § 2º A proteção concedida no inciso XIII não abarca os **dados** ou materiais em si mesmos e se entende sem prejuízo de quaisquer direitos autorais que subsistam a respeito dos **dados** ou materiais contidos nas obras.
4. Art. 29. Depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades, tais como:

   IX - a inclusão em base de **dados**, o armazenamento em computador, a microfilmagem e as demais formas de arquivamento do gênero;

5. Capítulo VII Da Utilização de Bases de **Dados**
6. Art. 87. O titular do direito patrimonial sobre uma base de **dados** terá o direito exclusivo, a respeito da forma de expressão da estrutura da referida base, de autorizar ou proibir:
7. III - a distribuição do original ou cópias da base de **dados** ou a sua comunicação ao público;
8. Art. 98. Com o ato de filiação, as associações de que trata o art. 97 tornam-se mandatárias de seus associados para a prática de todos os atos necessários à defesa judicial ou extrajudicial de seus direitos autorais, bem como para o exercício da atividade de cobrança desses direitos. (Redação dada pela Lei nº 12.853, de 2013)

   § 6º As associações deverão manter um cadastro centralizado de todos os contratos, declarações ou documentos de qualquer natureza que comprovem a autoria e a titularidade das obras e dos fonogramas, bem como as participações individuais em cada obra e em cada fonograma, prevenindo o falseamento de **dados** e fraudes e promovendo a desambiguação de títulos similares de obras. (Incluído pela Lei nº 12.853, de 2013)

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

Os termos referidos não são mencionados nesta legislação.

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

2002 - LEI Nº 10.406 (Código Civil)

https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm

BANCO CENTRAL - BANCO

O termo **"Banco central"** aparece **1 vez**, assim como o termo **"Banco"**, sendo o mesmo trecho do texto, totalizando **1 resultado**

TERMO "BANCO CENTRAL"

1) Art. 406. Quando não forem convencionados, ou quando o forem sem taxa estipulada, ou quando provierem de determinação da lei, os juros serão fixados de acordo com a taxa legal. (Redação dada pela Lei nº 14.905, de 2024) Produção de efeitos

   § 2º A metodologia de cálculo da taxa legal e sua forma de aplicação serão definidas pelo Conselho Monetário Nacional e divulgadas pelo **Banco Central** do Brasil. (Incluído pela Lei nº 14.905, de 2024)

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **"Dados"** aparece **8 vezes**, totalizando **8 resultados**

TERMO "DADOS"

1. Art. 364. A novação extingue os acessórios e garantias da dívida, sempre que não houver estipulação em contrário. Não aproveitará, contudo, ao credor ressalvar o penhor, a hipoteca ou a anticrese, se os bens **dados** em garantia pertencerem a terceiro que não foi parte na novação
2. Art. 615. Concluída a obra de acordo com o ajuste, ou o costume do lugar, o dono é obrigado a recebê-la. Poderá, porém, rejeitá-la, se o empreiteiro se afastou das instruções recebidas e dos planos **dados**, ou das regras técnicas em trabalhos de tal natureza.
3. Seção III - Do Transporte de Coisas

   Art. 744. Ao receber a coisa, o transportador emitirá conhecimento com a menção dos **dados** que a identifiquem, obedecido o disposto em lei especial.

4. CAPÍTULO XVI - Da Constituição de Renda

   Art. 809. Os bens **dados** em compensação da renda caem, desde a tradição, no domínio da pessoa que por aquela se obrigou.

5. TÍTULO X Do Penhor, da Hipoteca e da Anticrese

   CAPÍTULO I - Disposições Gerais

   Art. 1.420. Só aquele que pode alienar poderá empenhar, hipotecar ou dar em anticrese; só os bens que se podem alienar poderão ser **dados** em penhor, anticrese ou hipoteca.

6. CAPÍTULO IV Da Anticrese

   Art. 1.507. O credor anticrético pode administrar os bens **dados** em anticrese e fruir seus frutos e utilidades, mas deverá apresentar anualmente balanço, exato e fiel, de sua administração.

7. § 2 o O credor anticrético pode, salvo pacto em sentido contrário, arrendar os bens **dados** em anticrese a terceiro, mantendo, até ser pago, direito de retenção do imóvel, embora o aluguel desse arrendamento não seja vinculativo para o devedor.
8. Art. 1.510. O adquirente dos bens **dados** em anticrese poderá remi-los, antes do vencimento da dívida, pagando a sua totalidade à data do pedido de remição e imitir-se-á, se for o caso, na sua posse.

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

O termo "**Digital**" aparece **2 vezes**, totalizando **2 resultados**

TERMO "DIGITAL

1. Art. 968. A inscrição do empresário far-se-á mediante requerimento que contenha:

   II - a firma, com a respectiva assinatura autógrafa que poderá ser substituída pela assinatura autenticada com certificação **digital** ou meio equivalente que comprove a sua autenticidade, ressalvado o disposto no inciso I do § 1º do art. 4º da Lei Complementar nº 123, de 14 de dezembro de 2006 ; (Redação dada pela Lei Complementar nº 147, de 2014)

2. Parágrafo único. A reunião ou a assembleia poderá ser realizada de forma **digital**, respeitados os direitos legalmente previstos de participação e de manifestação dos sócios e os demais requisitos regulamentares. (Incluído pela Lei nº 14.030, de 2020)

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

2003 - LEI N. 10.695 (Pirataria)

https://www.planalto.gov.br/ccivil_03/leis/2003/l10.695.htm

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

Os termos referidos não são mencionados nesta legislação

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

Os termos referidos não são mencionados nesta legislação

SOBERANIA DIGITAL
O termo referido não é mencionado nesta legislação

2001 - Assinatura da Convenção de Budapeste: O Brasil se torna signatário da Convenção sobre Cibercrime, que estabelece diretrizes para a cooperação internacional no combate a crimes cibernéticos. A convenção visa padronizar legislações e práticas entre os países signatários, facilitando a troca de informações e a assistência mútua em investigações relacionadas a crimes digitais. Apesar de o Brasil ter assinado a Convenção de Budapeste sobre o Crime Cibernético em 23 de novembro de 2001, só a promulgou e ratificou internamente anos depois, em 2021 e **2023**. (tabela feita no ano de 2023)

2004 - LEI Nº 10.703 (Cadastramento de usuários de telefones celulares pré-pagos)
https://www.planalto.gov.br/ccivil_03/leis/2003/l10.703.htm
BANCO CENTRAL - BANCO Os termos referidos não são mencionados nesta legislação
CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO Os termos referidos não são mencionados nesta legislação
PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS O termo **"Dados"** aparece **3 vezes**, totalizando **3 resultados**
TERMO 'DADOS" 1. Art. 1o Incumbe aos prestadores de serviços de telecomunicações na modalidade pré-paga, em operação no território nacional, manter cadastro atualizado de usuários. § 2o Os atuais usuários deverão ser convocados para fornecimento dos **dados** necessários ao atendimento do disposto neste artigo, no prazo de noventa dias, a partir da data da promulgação desta Lei, prorrogável por igual período, a critério do Poder Executivo. (Vide Decreto nº 4.860, de 18.10.2003) 2. § 3o Os **dados** constantes do cadastro, salvo motivo justificado, deverão ser imediatamente disponibilizados pelos prestadores de serviços para atender solicitação da autoridade judicial, sob pena de multa de até R$ 10.000,00 (dez mil reais) por infração cometida. 3. Art. 2o Os estabelecimentos que comercializam aparelhos de telefonia celular, na modalidade pré-paga, ficam obrigados a informar aos prestadores de serviços, no prazo de vinte e quatro horas após executada a venda, os **dados** referidos no art. 1o, sob pena de multa de até R$ 500,00 (quinhentos reais) por infração.
SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

Os termos referidos não são mencionados nesta legislação

SOBERANIA DIGITAL

Os termos referidos não são mencionados nesta legislação

2012 - LEI Nº 12.737 (Lei Carolina Dieckmann)

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

O termo **"Delitos Informáticos"** aparece **2 vezes**, totalizando **2 resultados**

TERMO "DELITOS INFORMÁTICOS"

1. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. - Dispõe sobre a tipificação criminal de **delitos informáticos**; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
2. Art. 1º Esta Lei dispõe sobre a tipificação criminal de **delitos informáticos** e dá outras providências.

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **"Dados"** aparece **2 vezes**, totalizando **2 resultados**

TERMO "DADOS"

1. Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

   "Invasão de dispositivo informático

   Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir **dados** ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

   Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

2. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput .

   § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos **dados** ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

Os termos referidos não são mencionados nesta legislação

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

2014 -LEI Nº 12.965 (Marco Civil da Internet)

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **“Proteção de dados”** é mencionado **3 vezes**, o termo **“Proteção dos Dados” 2 vezes** e **“Proteção de seus Dados” 1 vez**. Além disso, o termo "**Dados**", de forma isolada, aparece em mais **16 ocasiões**, totalizando **22 resultados**.

TERMO “PROTEÇÃO DE DADOS”

1. Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

   X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a **proteção de dados** pessoais; (Redação dada pela Lei nº 13.709, de 2018) (Vigência)

2. Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

3. II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a **proteção de dados** pessoais. (Redação dada pela Lei nº 13.709, de 2018) (Vigência)

TERMO “PROTEÇÃO DOS DADOS”

1. Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

   I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

   II - proteção da privacidade;

   III - **proteção dos dados** pessoais, na forma da lei;

   IV - preservação e garantia da neutralidade de rede;

   V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

   VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

   VII - preservação da natureza participativa da rede;

   VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

   Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

2. Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à **proteção dos dados** pessoais e ao sigilo das comunicações privadas e dos registros.

TERMO “PROTEÇÃO DE SEUS DADOS

1. Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

   VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e **proteção de seus dados** pessoais, que somente poderão ser utilizados para finalidades que:

   a) justifiquem sua coleta;

   b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

TERMO “DADOS”

1. Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

   I - do direito de acesso à internet a todos;

   II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

   III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

   IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de **dados**.

2. Art. 5º Para os efeitos desta Lei, considera-se:

   I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de **dados** entre terminais por meio de diferentes redes;

3. V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de **dados** pela internet, mediante a atribuição ou autenticação de um endereço IP;
4. VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de **dados**;
5. CAPÍTULO III

   DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

   Seção I

   Da Neutralidade de Rede

   Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de **dados**, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

6. § 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de **dados**, respeitado o disposto neste artigo.
7. Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de **dados** pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
8. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a **dados** pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
9. § 3º O disposto no caput não impede o acesso aos **dados** cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
10. Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de **dados** pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
11. § 1º O disposto no caput aplica-se aos **dados** coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
12. § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação

brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de **dados**,bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

13. Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

    I - dos registros de acesso a outras aplicações de internet sem que o titular dos **dados** tenha consentido previamente, respeitado o disposto no art. 7º ; ou

14. II - de **dados** pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais. (Redação dada pela Lei nº 13.709, de 2018) (Vigência)
15. CAPÍTULO IV

    DA ATUAÇÃO DO PODER PÚBLICO

    Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

    VI - publicidade e disseminação de **dados** e informações públicos, de forma aberta e estruturada;

16. VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de **dados** no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

O termo **“Digital”** aparece **3 vezes** e o termo“**Digitais” 1 vez**, totalizando **4 resultados**

TERMO “DIGITAL”

1. Art. 27. As iniciativas públicas de fomento à cultura **digital** e de promoção da internet como ferramenta social devem:
2. I - promover a inclusão **digital**;
3. Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

   Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão **digital** de crianças e adolescentes.

TERMO “DIGITAIS”

1. Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

   II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios **digitais**;

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

2016 - DECRETO Nº 8.771 - Regulamenta o Marco Civil da Internet

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **"Proteção de dados"** aparece **1 vez**, enquanto o termo **"Dados"**, de forma isolada, aparece **19 vezes**. Totalizando **20 resultados**

TERMO "PROTEÇÃO DE DADOS"

1. Art. 1º Este Decreto trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indica procedimentos para guarda e **proteção de dados** por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações contidas na Lei nº 12.965, de 23 de abril de 2014 .

TERMO "DADOS"

1. Art. 1º Este Decreto trata das hipóteses admitidas de discriminação de pacotes de **dados** na internet e de degradação de tráfego, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de **dados** cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações contidas na Lei nº 12.965, de 23 de abril de 2014 .
2. Art. 8º A degradação ou a discriminação decorrente da priorização de serviços de emergência somente poderá decorrer de:

   Parágrafo único. A transmissão de **dados** nos casos elencados neste artigo será gratuita.

3. Art. 9º Ficam vedadas condutas unilaterais ou acordos entre o responsável pela transmissão, pela comutação ou pelo roteamento e os provedores de aplicação que:

   I - comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País;

   II - priorizem pacotes de **dados** em razão de arranjos comerciais; ou

   III - privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico.

4. CAPÍTULO III

   DA PROTEÇÃO AOS REGISTROS, AOS **DADOS** PESSOAIS E ÀS COMUNICAÇÕES PRIVADAS

5. Seção I - Da requisição de **dados** cadastrais
6. Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos **dados** cadastrais.
7. § 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais **dados**.

8. § 2º São considerados **dados** cadastrais:

   I - a filiação;

   II - o endereço; e

   III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

9. § 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos **dados** estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.
10. Art. 12. A autoridade máxima de cada órgão da administração pública federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de **dados** cadastrais, contendo:
11. I - o número de pedidos realizados;

    II - a listagem dos provedores de conexão ou de acesso a aplicações aos quais os **dados** foram requeridos;

    III - o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e

    IV - o número de usuários afetados por tais solicitações.

12. Seção II

    Padrões de segurança e sigilo dos registros, **dados** pessoais e comunicações privadas

13. Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de **dados** pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
14. I - o estabelecimento de controle estrito sobre o acesso aos **dados** mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

    II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

    III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e

15. IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos **dados**, como encriptação ou medidas de proteção equivalentes.
16. § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014 , os provedores de conexão e aplicações devem reter a menor quantidade possível de **dados** pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
17. Art. 14. Para os fins do disposto neste Decreto, considera-se:

    I - **dado pessoal** - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e

18. II - tratamento de **dados** pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
19. Art. 15. Os **dados** de que trata o art. 11 da Lei nº 12.965, de 2014 , deverão ser mantidos em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto.

O termo referido não é mencionado nesta legislação

2018 - LEI Nº 13.709 (Lei Geral de Proteção de Dados Pessoais (LGPD)

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

O termo **"Banco"**, de forma isolada, aparece em **7 ocasiões**, totalizando **7 resultados**

TERMO "BANCO"

1. Art. 4º IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.Esta Lei não se aplica ao tratamento de dados pessoais:

   § 4º Em nenhum caso a totalidade dos dados pessoais de **banco** de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência

2. Art. 5º Para os fins desta Lei, considera-se:

   IV - **banco** de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

3. XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do **banco** de dados;
4. XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em **banco** de dados, independentemente do procedimento empregado;
5. XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de **banco**s de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
6. 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: (Vigência)

   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)

7. Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de **bancos** de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **“Proteção de dados”** aparece **47 vezes**, enquanto os termos **“Proteção dos Dados” 4 vezes**, e “Proteção a Dados” 1 vez. Além disso, o termo **“Dado”** ou **“Dados”**, de forma isolada, aparecem **203 vezes**. Totalizando **255 resultados**.

TERMO “PROTEÇÃO DE DADOS”

1) Lei Geral de **Proteção de Dados** Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) Vigência
2) 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.

3) IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de **proteção de dados** pessoais adequado ao previsto nesta Lei.
4) § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à **proteção de dados** pessoais.
5) VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de **Proteção de Dados** – ANPD; (Redação dada pela Medida Provisória nº 1.317, de 2025)
6) XVII - relatório de impacto à **proteção de dados** pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
7) 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.
8) § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à **proteção de dados** pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
9) § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de **Proteção de Dados** Pessoais.
10) Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de **proteção de dados** pessoais elencados no art. 6º desta Lei.
11) Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à **proteção de dados** pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.
12) Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

    I - para países ou organismos internacionais que proporcionem grau de **proteção de dados** pessoais adequado ao previsto nesta Lei;

13) II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de **proteção de dados** previstos nesta Lei, na forma de:

    a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

14) Art. 34. O nível de **proteção de dados** do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
15) III - a observância dos princípios gerais de **proteção de dados** pessoais e direitos dos titulares previstos nesta Lei;
16) V - a existência de garantias judiciais e institucionais para o respeito aos direitos de **proteção de dados** pessoais; e
17) Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à **proteção de dados** pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
18) Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 2º As atividades do encarregado consistem em:

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à **proteção de dados** pessoais; e

19) Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de **proteção de dados** pessoais, é obrigado a repará-lo.
20) § 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de **proteção de dados** ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

21) Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de **proteção de dados**; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

22) § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à **proteção de dados** pessoais;

23) CAPÍTULO IX

(Redação dada pela Medida Provisória nº 1.317, de 2025)

DA AGÊNCIA NACIONAL DE **PROTEÇÃO DE DADOS** E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

24) Seção I

Da Agência Nacional de **Proteção de Dados**

25) Art. 55-A. Fica criada a Agência Nacional de **Proteção de Dados** – ANPD, autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia funcional,

técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal, nos termos do disposto na Lei nº 13.848, de 25 de junho de 2019. (Redação dada pela Medida Provisória nº 1.317, de 2025)

26) Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de **Proteção de Dados** Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

27) 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)

28) III - elaborar diretrizes para a Política Nacional de **Proteção de Dados** Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)
29) VI - promover na população o conhecimento das normas e das políticas públicas sobre **proteção de dado**s pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)
30) 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)
31) 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)
32) XIII - editar regulamentos e procedimentos sobre **proteção de dados** pessoais e privacidade, 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; (Incluído pela Lei nº 13.853, de 2019)
33) XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, 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; (Incluído pela Lei nº 13.853, de 2019)
34) XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, 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; (Incluído pela Lei nº 13.853, de 2019)
35) Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à **proteção de dados** pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)
36) Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de **proteção de dados** pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)
37) Seção II

Do Conselho Nacional de **Proteção de Dados** Pessoais e da Privacidade

38) Art. 58-A. O Conselho Nacional de **Proteção de Dados** Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)
39) I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a **proteção de dados** pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

40) § 4º A participação no Conselho Nacional de **Proteção de Dados** Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)
41) Art. 58-B. Compete ao Conselho Nacional de **Proteção de Dados** Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)
42) 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; (Incluído pela Lei nº 13.853, de 2019)
43) II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de **Proteção de Dados** Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

44) IV - elaborar estudos e realizar debates e audiências públicas sobre a **proteção de dados** pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)
45) V - disseminar o conhecimento sobre a **proteção de dados** pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)
46) Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) , passa a vigorar com as seguintes alterações: Vigência

"Art. 7º .....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

47) "Art. 16. .....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a **proteção de dados** pessoais." (NR)

TERMO "PROTEÇÃO DOS DADOS"

1. Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

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

2. Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a **proteção dos dados** pessoais.

3. Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

   III - a indicação das medidas técnicas e de segurança utilizadas para a **proteção dos dados**, observados os segredos comercial e industrial;

4. 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)

   TERMO "PROTEÇÃO A DADOS"

1. Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de **proteção a dados** pessoais conferido por país ou organismo internacional.

   TERMOS "DADO" E "DADOS"

1. Art. 1º Esta Lei dispõe sobre o tratamento de **dados** pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
2. Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os **dados**, desde que:
3. I - a operação de tratamento seja realizada no território nacional;

   II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de **dados** de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

4. III - os **dados** pessoais objeto do tratamento tenham sido coletados no território nacional.
5. § 1º Consideram-se coletados no território nacional os **dados** pessoais cujo titular nele se encontre no momento da coleta.
6. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.
7. Art. 4º Esta Lei não se aplica ao tratamento de **dados** pessoais:

   I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

   II - realizado para fins exclusivamente:

   a) jornalístico e artísticos; ou

   b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

   III - realizado para fins exclusivos de:

   a) segurança pública;

   b) defesa nacional;

   c) segurança do Estado; ou

   d) atividades de investigação e repressão de infrações penais; ou

8. IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de **dados** com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
9. IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência

internacional de **dados** com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

10. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
11. § 2º É vedado o tratamento dos **dados** a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
12. § 4º Em nenhum caso a totalidade dos **dados** pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência
13. Art. 5º Para os fins desta Lei, considera-se:

    I - **dado** pessoal: informação relacionada a pessoa natural identificada ou identificável;

14. II - **dado** pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
15. II - dado pessoal sensível: **dado** pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
16. II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, **dado** referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
17. II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, **dado** genético ou biométrico, quando vinculado a uma pessoa natural;
18. III - **dado** anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
19. III - dado anonimizado: **dado** relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
20. IV - banco de **dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
21. IV - banco de dados: conjunto estruturado de **dados** pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
22. V - titular: pessoa natural a quem se referem os **dados** pessoais que são objeto de tratamento;
23. VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de **dados** pessoais;
24. VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de **dados** pessoais em nome do controlador;
25. VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos **dados** e a Agência Nacional de Proteção de Dados – ANPD; (Redação dada pela Medida Provisória nº 1.317, de 2025)

    IX - agentes de tratamento: o controlador e o operador;

26. X - tratamento: toda operação realizada com **dados** pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
27. XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um **dado** perde a possibilidade de associação, direta ou indireta, a um indivíduo;
28. XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus **dados** pessoais para uma finalidade determinada;

29. XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do **dado** pessoal ou do banco de dados;
30. XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de **dados**;
31. XIV - eliminação: exclusão de **dado** ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
32. XIV - eliminação: exclusão de dado ou de conjunto de **dados** armazenados em banco de dados, independentemente do procedimento empregado;
33. XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de **dados**, independentemente do procedimento empregado;
34. XV - transferência internacional de **dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
35. XV - transferência internacional de dados: transferência de **dados** pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
36. XVI - uso compartilhado de **dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
37. XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de **dados** pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
38. XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de **dados** pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
39. XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de **dados** pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
40. 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;

41. 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;
42. 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**;
43. 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;
44. 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;
45. 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;

46. 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;
47. 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;

48. CAPÍTULO II

    DO TRATAMENTO DE **DADOS** PESSOAIS

49. Seção I

    Dos Requisitos para o Tratamento de **Dados** Pessoais

50. 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;

51. 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;
52. IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos **dados** pessoais;
53. 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; (Redação dada pela Lei nº 13.853, de 2019) Vigência

    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.

54. § 3º O tratamento de **dados** pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
55. § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os **dados** tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
56. § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar **dados** pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

    § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

57. § 7º O tratamento posterior dos **dados** pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

58. Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

    § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

    § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

    § 3º É vedado o tratamento de **dados** pessoais mediante vício de consentimento.

59. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de **dados** pessoais serão nulas.
60. Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus **dados**, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

    I - finalidade específica do tratamento;

    II - forma e duração do tratamento, observados os segredos comercial e industrial;

    III - identificação do controlador;

    IV - informações de contato do controlador;

61. V - informações acerca do uso compartilhado de **dados** pelo controlador e a finalidade;

    VI - responsabilidades dos agentes que realizarão o tratamento; e

    VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

62. § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de **dados** pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.
63. § 3º Quando o tratamento de **dados** pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.
64. Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de **dados** pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

    I - apoio e promoção de atividades do controlador; e

    II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

65. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os **dados** pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
66. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de **dados** baseado em seu legítimo interesse.
67. Seção II

    Do Tratamento de **Dados** Pessoais Sensíveis

68. Art. 11. O tratamento de **dados** pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

    I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

    II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

    a) cumprimento de obrigação legal ou regulatória pelo controlador;

69. b) tratamento compartilhado de **dados** necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
70. c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos **dados** pessoais sensíveis;

    d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

    e) proteção da vida ou da incolumidade física do titular ou de terceiro;

    f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

    g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

71. § 1º Aplica-se o disposto neste artigo a qualquer tratamento de **dados** pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
72. § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele **dados** pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
73. § 3º A comunicação ou o uso compartilhado de **dados** pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
74. § 4º É vedada a comunicação ou o uso compartilhado entre controladores de **dados** pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência
75. § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de **dados**, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência
76. I - a portabilidade de **dados** quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

    II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência

77. § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de **dados** de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) Vigência
78. Art. 12. Os **dados** anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
79. Art. 12. Os dados anonimizados não serão considerados **dados** pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
80. § 2º Poderão ser igualmente considerados como **dados** pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
81. Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de **dados** pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

82. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar **dados** pessoais.
83. § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos **dados** a terceiro.
84. § 3º O acesso aos **dados** de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
85. § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um **dado** perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
86. Seção III

    Do Tratamento de **Dados** Pessoais de Crianças e de Adolescentes

87. Art. 14. O tratamento de **dados** pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
88. § 1º O tratamento de **dados** pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
89. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque **dado** por pelo menos um dos pais ou pelo responsável legal.
90. § 2º No tratamento de **dados** de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
91. § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de **dados** coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
92. § 3º Poderão ser coletados **dados** pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

    § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

93. § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi **dado** pelo responsável pela criança, consideradas as tecnologias disponíveis.
94. § 6º As informações sobre o tratamento de **dados** referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.
95. Seção IV

    Do Término do Tratamento de Dados

96. Art. 15. O término do tratamento de **dados** pessoais ocorrerá nas seguintes hipóteses:
97. I - verificação de que a finalidade foi alcançada ou de que os **dados** deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

    II - fim do período de tratamento;

    III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

    IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

98. Art. 16. Os **dados** pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

    I - cumprimento de obrigação legal ou regulatória pelo controlador;

99. II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos **dados** pessoais;
100. III - transferência a terceiro, desde que respeitados os requisitos de tratamento de **dados** dispostos nesta Lei; ou
101. IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os **dados**.
102. Art. 17. 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.
103. 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:
104. 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:
105. I - confirmação da existência de tratamento;

    II - acesso aos **dados**;

106. III - correção de **dados** incompletos, inexatos ou desatualizados;
107. V - anonimização, bloqueio ou eliminação de **dados** desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
108. 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; (Redação dada pela Lei nº 13.853, de 2019) Vigência
109. VI - eliminação dos **dados** pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
110. 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.

111. § 1º O titular dos **dados** pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
112. § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus **dados** contra o controlador perante a autoridade nacional.
113. § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

    I - comunicar que não é agente de tratamento dos **dados** e indicar, sempre que possível, o agente; ou

    II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

114. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de **dados** a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência
115. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos **dados**, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência
116. § 7º A portabilidade dos **dados** pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
117. § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui **dados** que já tenham sido anonimizados pelo controlador.
118. Art. 19. A confirmação de existência ou o acesso a **dados** pessoais serão providenciados, mediante requisição do titular:

    I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos **dados**, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os **dados** pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os **dados** poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus **dados** pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

Art. 20. O titular dos **dados** tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de **dados** pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de **dados** pessoais.

Art. 21. Os **dados** pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de **dados** poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV

DO TRATAMENTO DE **DADOS** PESSOAIS PELO PODER PÚBLICO

Seção I

Das Regras

Art. 23. O tratamento de **dados** pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de **dados** pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de **dados** pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO).(Incluído pela Lei nº 13.853, de 2019) Vigência

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos **dados** por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

133. Art. 25. Os **dados** deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.
134. Art. 26. O uso compartilhado de **dados** pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
135. § 1º É vedado ao Poder Público transferir a entidades privadas **dados** pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;

II - (VETADO);

136. III - nos casos em que os **dados** forem acessíveis publicamente, observadas as disposições desta Lei.

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

137. V - na hipótese de a transferência dos **dados** objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência
138. V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos **dados**, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência
139. Art. 27. A comunicação ou o uso compartilhado de **dados** pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:
140. I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de **dados**, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019) Vigência

141. Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de **dados** pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019) Vigência
142. Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de **dados** pessoais.
143. Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de **dados** pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.
144. CAPÍTULO V

DA TRANSFERÊNCIA INTERNACIONAL DE **DADOS**

145. Art. 33. A transferência internacional de **dados** pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

146. Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos **dados**;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

147. CAPÍTULO VI

DOS AGENTES DE TRATAMENTO DE **DADOS** PESSOAIS

148. Seção I

Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de **dados** pessoais que realizarem, especialmente quando baseado no legítimo interesse.

149. Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de **dados** sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
150. Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de **dados**, nos termos de regulamento, observados os segredos comercial e industrial.
151. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de **dados** coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
152. Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos **dados** e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.
153. Seção II

Do Encarregado pelo Tratamento de **Dados** Pessoais

154. Art. 41. O controlador deverá indicar encarregado pelo tratamento de **dados** pessoais.
155. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de **dados**.
156. Seção III

Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de **dados** pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

157. § 1º A fim de assegurar a efetiva indenização ao titular dos **dados**:
158. I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos **dados** respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

159. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos **dados** quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
160. Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de **dados** pessoais que lhes é atribuído;

161. II - que, embora tenham realizado o tratamento de **dados** pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
162. III - que o dano é decorrente de culpa exclusiva do titular dos **dados** ou de terceiro.
163. Art. 44. O tratamento de **dados** pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

164. III - as técnicas de tratamento de **dados** pessoais disponíveis à época em que foi realizado.
165. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos **dados** o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.
166. Seção I

Da Segurança e do Sigilo de **Dados**

167. Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
168. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de **dados** pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
169. Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos **dados** pessoais, mesmo após o seu término.
170. Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos **dados** pessoais afetados;

171. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os **dados** pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
172. Art. 49. Os sistemas utilizados para o tratamento de **dados** pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.
173. Seção II

Das Boas Práticas e da Governança

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.

174. 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.
175. § 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.
176. § 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.
177. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos **dados** tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
178. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos **dados**, poderá:
179. I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de **dados** pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

180. c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos **dados** tratados;
181. Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus **dados** pessoais.
182. 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: (Vigência)
183. 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;

184. VI - eliminação dos **dados** pessoais a que se refere a infração;
185. 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)
186. 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)
187. XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de **dados**. (Incluído pela Lei nº 13.853, de 2019)

188. § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de **dados**, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

189. Art. 55-J. Compete à ANPD: (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)

190. 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)
191. XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de **dados** pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)
192. XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos **dados** e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)
193. XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de **dados** pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)
194. XIX - garantir que o tratamento de **dados** de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)
195. XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de **dados** pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)
196. § 1º Ao impor condicionantes administrativas ao tratamento de **dados** pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)
197. § 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de **dados** pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)
198. Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, **dados** e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

199. Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de **dados** pessoais; e (Incluído pela Lei nº 13.853, de 2019)

200. Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) , passa a vigorar com as seguintes alterações: Vigência

"Art. 7º .....

X - exclusão definitiva dos **dados** pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

201. "Art. 16. .....

II - de **dados** pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

202. II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi **dado** consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

203. Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de **dados** constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

204. Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos **dados**.

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

O termo **"Digitais"** aparece **1 vez**, totalizando **1 resultado**

TERMO "DIGITAIS

1. CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios **digitais,** por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 - Estratégia Nacional de Segurança Cibernética (ENSC)

Revogado pelo Decreto nº 12.573, de 2025

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm

2020 - LEI Nº 14.010 - Lei da Pandemia

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14010.htm#:~:text=Art.,Par%C3%A1grafo%20%C3%BAnico.

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

Os termos referidos não são mencionados nesta legislação

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

Os termos referidos não são mencionados nesta legislação

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

2021 - LEI nº 14.129 (Lei do Governo Digital)

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

Os termos referidos não são mencionados nesta legislação

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **“Proteção de dados”** é mencionado **20 vezes**, enquanto o termo **“Dados”**, de forma isolada, aparece **84 vezes**, totalizando **104 resultados**

“TERMO PROTEÇÃO DE DADOS”

1. Art. 1º Esta Lei dispõe sobre princípios, regras e instrumentos para o aumento da eficiência da administração pública, especialmente por meio da desburocratização, da inovação, da transformação digital e da participação do cidadão.

   Parágrafo único. Na aplicação desta Lei deverá ser observado o disposto nas Leis nºs 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), 13.460, de 26 de junho de 2017, 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais), e 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e na Lei Complementar nº 105, de 10 de janeiro de 2001.

2. Art. 3º São princípios e diretrizes do Governo Digital e da eficiência pública:

   IX - a atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos, com o compartilhamento de dados pessoais em ambiente seguro quando for indispensável para a prestação do serviço, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais), e, quando couber, com a transferência de sigilo, nos termos do art. 198 da Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e da Lei Complementar nº 105, de 10 de janeiro de 2001;

3. XVII - a **proteção de dados** pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
4. XVII - a proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais);
5. XXIII - a implantação do governo como plataforma e a promoção do uso de dados, preferencialmente anonimizados, por pessoas físicas e jurídicas de diferentes setores da sociedade, resguardado o disposto nos arts. 7º e 11 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais), com vistas, especialmente, à formulação de políticas públicas, de pesquisas científicas, de geração de negócios e de controle social;
6. Parágrafo único. Aplicam-se a esta Lei os conceitos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais).
7. Art. 21. A ferramenta digital de atendimento e de acompanhamento da entrega dos serviços públicos de que trata o inciso I do caput do art. 20 desta Lei deve apresentar, no mínimo, as seguintes características e funcionalidades:

   X - funcionalidade para solicitar acesso a informações acerca do tratamento de dados pessoais, nos termos das Leis nºs 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais); e

8. Art. 25. As Plataformas de Governo Digital devem dispor de ferramentas de transparência e de controle do tratamento de dados pessoais que sejam claras e facilmente acessíveis e que permitam ao cidadão o exercício dos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais).
9. § 1º As ferramentas previstas no caput deste artigo devem:

   I - disponibilizar, entre outras, as fontes dos dados pessoais, a finalidade específica do seu tratamento pelo respectivo órgão ou ente e a indicação de outros órgãos ou entes com os quais é realizado o uso compartilhado de dados pessoais, incluído o histórico de acesso ou uso compartilhado, ressalvados os casos previstos no inciso III do caput do art. 4º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais);

10. II - permitir que o cidadão efetue requisições ao órgão ou à entidade controladora dos seus dados, especialmente aquelas previstas no art. 18 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais).
11. § 2º A Autoridade Nacional de **Proteção de Dados** (ANPD) poderá editar normas complementares para regulamentar o disposto neste artigo.
12. Art. 27. São garantidos os seguintes direitos aos usuários da prestação digital de serviços públicos, além daqueles constantes das Leis nºs 13.460, de 26 de junho de 2017, e 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais):
13. Art. 29. Os dados disponibilizados pelos prestadores de serviços públicos, bem como qualquer informação de transparência ativa, são de livre utilização pela sociedade, observados os princípios dispostos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais).
14. § 1º Na promoção da transparência ativa de dados, o poder público deverá observar os seguintes requisitos:

    II - garantia de acesso irrestrito aos dados, os quais devem ser legíveis por máquina e estar disponíveis em formato aberto, respeitadas as Leis nºs 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais);

15. VIII - respeito à privacidade dos dados pessoais e dos dados sensíveis, sem prejuízo dos demais requisitos elencados, conforme a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais);
16. IX - intercâmbio de dados entre órgãos e entidades dos diferentes Poderes e esferas da Federação, respeitado o disposto no art. 26 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais); e
17. Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais), deverão gerir suas ferramentas digitais, considerando:
18. III - a **proteção de dados** pessoais, observada a legislação vigente, especialmente a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
19. III - a proteção de dados pessoais, observada a legislação vigente, especialmente a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais).
20. Parágrafo único. Aplicam-se aos dados pessoais tratados por meio de mecanismos de interoperabilidade as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de **Proteção de Dados** Pessoais).

TERMO "DADOS"

1. Art. 3º São princípios e diretrizes do Governo Digital e da eficiência pública:

   IX - a atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos, com o compartilhamento de **dados** pessoais em ambiente seguro quando for indispensável para a prestação do serviço, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e, quando couber, com a transferência de sigilo, nos termos do art. 198 da Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e da Lei Complementar nº 105, de 10 de janeiro de 2001;

2. XIV - a interoperabilidade de sistemas e a promoção de **dados** abertos;
3. XXIII - a implantação do governo como plataforma e a promoção do uso de **dados**, preferencialmente anonimizados, por pessoas físicas e jurídicas de diferentes setores da sociedade, resguardado o disposto nos arts. 7º e 11 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), com vistas, especialmente, à formulação de políticas públicas, de pesquisas científicas, de geração de negócios e de controle social;
4. Art. 4º Para os fins desta Lei, considera-se:

   III - base nacional de serviços públicos: base de **dados** que contém as informações necessárias sobre a oferta de serviços públicos de todos os prestadores desses serviços;

5. IV - **dados** abertos: dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou tratamento por qualquer pessoa, física ou jurídica;
6. IV - dados abertos: **dados** acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou tratamento por qualquer pessoa, física ou jurídica;
7. VII - governo como plataforma: infraestrutura tecnológica que facilite o uso de **dados** de acesso público e promova a interação entre diversos agentes, de forma segura, eficiente e responsável, para estímulo à inovação, à exploração de atividade econômica e à prestação de serviços à população;
8. X - registros de referência: informação íntegra e precisa oriunda de uma ou mais fontes de **dados**, centralizadas ou descentralizadas, sobre elementos fundamentais para a prestação de serviços e para a gestão de políticas públicas; e
9. XI - transparência ativa: disponibilização de **dados** pela administração pública independentemente de solicitações.
10. Art. 20. As Plataformas de Governo Digital, instrumentos necessários para a oferta e a prestação digital dos serviços públicos de cada ente federativo, deverão ter pelo menos as seguintes funcionalidades:

    II - painel de monitoramento do desempenho dos serviços públicos.

§ 2º As funcionalidades de que trata o caput deste artigo deverão observar padrões de interoperabilidade e a necessidade de integração de **dados** como formas de simplificação e de eficiência nos processos e no atendimento aos usuários.

11. IX - nível de segurança compatível com o grau de exigência, a natureza e a criticidade dos serviços públicos e dos **dados** utilizados;
12. X - funcionalidade para solicitar acesso a informações acerca do tratamento de **dados** pessoais, nos termos das Leis nºs 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais); e
13. Art. 24. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos deverão, no âmbito de suas competências:

    IV - eliminar, inclusive por meio da interoperabilidade de **dados**, as exigências desnecessárias ao usuário quanto à apresentação de informações e de documentos comprobatórios prescindíveis;

14. V - eliminar a replicação de registros de **dados**, exceto por razões de desempenho ou de segurança;
15. VI - tornar os **dados** da prestação dos serviços públicos sob sua responsabilidade interoperáveis para composição dos indicadores do painel de monitoramento do desempenho dos serviços públicos;
16. VII - realizar a gestão das suas políticas públicas com base em **dados** e em evidências por meio da aplicação de inteligência de dados em plataforma digital; e
17. VII - realizar a gestão das suas políticas públicas com base em dados e em evidências por meio da aplicação de inteligência de **dados** em plataforma digital; e
18. Art. 25. As Plataformas de Governo Digital devem dispor de ferramentas de transparência e de controle do tratamento de **dados** pessoais que sejam claras e facilmente acessíveis e que permitam ao cidadão o exercício dos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
19. § 1º As ferramentas previstas no caput deste artigo devem:

    I - disponibilizar, entre outras, as fontes dos **dados** pessoais, a finalidade específica do seu tratamento pelo respectivo órgão ou ente e a indicação de outros órgãos ou entes com os quais é realizado o uso compartilhado de dados pessoais, incluído o histórico de acesso ou uso compartilhado, ressalvados os casos previstos no inciso III do caput do art. 4º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

20. § 1º As ferramentas previstas no caput deste artigo devem:

    I - disponibilizar, entre outras, as fontes dos dados pessoais, a finalidade específica do seu tratamento pelo respectivo órgão ou ente e a indicação de outros órgãos ou entes com os quais é realizado o uso compartilhado de **dados** pessoais, incluído o histórico de acesso ou uso compartilhado, ressalvados os casos previstos no inciso III do caput do art. 4º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

21. II - permitir que o cidadão efetue requisições ao órgão ou à entidade controladora dos seus **dados**, especialmente aquelas previstas no art. 18 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
22. Art. 28. Fica estabelecido o número de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ) como número suficiente para identificação do cidadão ou da pessoa jurídica, conforme o caso, nos bancos de **dados** de serviços públicos, garantida a gratuidade da inscrição e das alterações nesses cadastros.
23. § 1º O número de inscrição no CPF deverá constar dos cadastros e dos documentos de órgãos públicos, do registro civil de pessoas naturais, dos documentos de identificação de conselhos profissionais e, especialmente, dos seguintes cadastros e documentos:

    XV - outros certificados de registro e números de inscrição existentes em bases de **dados** públicas federais, estaduais, distritais e municipais.

24. § 2º A inclusão do número de inscrição no CPF nos cadastros e nos documentos de que trata o § 1º deste artigo ocorrerá sempre que a instituição responsável pelos cadastros e pelos documentos tiver acesso a documento comprobatório ou à base de **dados** administrada pela Secretaria Especial da Receita Federal do Brasil do Ministério da Economia.

25. § 3º A incorporação do número de inscrição no CPF à carteira de identidade será precedida de consulta à base de **dados** administrada pela Secretaria Especial da Receita Federal do Brasil do Ministério da Economia e de validação de acordo com essa base de dados.
26. § 4º Na hipótese de o requerente da carteira de identidade não estar inscrito no CPF, o órgão de identificação realizará a sua inscrição, caso tenha integração com a base de **dados** da Secretaria Especial da Receita Federal do Brasil do Ministério Economia.
27. Seção I

    Da Abertura dos **Dados**

28. Art. 29. Os **dados** disponibilizados pelos prestadores de serviços públicos, bem como qualquer informação de transparência ativa, são de livre utilização pela sociedade, observados os princípios dispostos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
29. § 1º Na promoção da transparência ativa de **dados**, o poder público deverá observar os seguintes requisitos:
30. I - observância da publicidade das bases de **dados** não pessoais como preceito geral e do sigilo como exceção;
31. II - garantia de acesso irrestrito aos **dados**, os quais devem ser legíveis por máquina e estar disponíveis em formato aberto, respeitadas as Leis nºs 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
32. III - descrição das bases de **dados** com informação suficiente sobre estrutura e semântica dos dados, inclusive quanto à sua qualidade e à sua integridade;
33. III - descrição das bases de dados com informação suficiente sobre estrutura e semântica dos **dados**, inclusive quanto à sua qualidade e à sua integridade;
34. IV - permissão irrestrita de uso de bases de **dados** publicadas em formato aberto;
35. V - completude de bases de **dados,** as quais devem ser disponibilizadas em sua forma primária, com o maior grau de granularidade possível, ou referenciar bases primárias, quando disponibilizadas de forma agregada;
36. VI - atualização periódica, mantido o histórico, de forma a garantir a perenidade de **dados**, a padronização de estruturas de informação e o valor dos dados à sociedade e a atender às necessidades de seus usuários;
37. VI - atualização periódica, mantido o histórico, de forma a garantir a perenidade de dados, a padronização de estruturas de informação e o valor dos **dados** à sociedade e a atender às necessidades de seus usuários;
38. VIII - respeito à privacidade dos **dados** pessoais e dos dados sensíveis, sem prejuízo dos demais requisitos elencados, conforme a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
39. VIII - respeito à privacidade dos dados pessoais e dos **dados** sensíveis, sem prejuízo dos demais requisitos elencados, conforme a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
40. IX - intercâmbio de **dados** entre órgãos e entidades dos diferentes Poderes e esferas da Federação, respeitado o disposto no art. 26 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais); e
41. XI - o inventário de bases de **dados** produzidos ou geridos no âmbito do órgão ou instituição, bem como catálogo de dados abertos disponíveis;
42. XI - o inventário de bases de dados produzidos ou geridos no âmbito do órgão ou instituição, bem como catálogo de **dados** abertos disponíveis;
43. XII - as concessões de recursos financeiros ou as renúncias de receitas para pessoas físicas ou jurídicas, com vistas ao desenvolvimento político, econômico, social e cultural, incluída a divulgação dos valores recebidos, da contrapartida e dos objetivos a serem alcançados por meio da utilização desses recursos e, no caso das renúncias individualizadas, dos **dados** dos beneficiários.
44. Art. 30. Qualquer interessado poderá apresentar pedido de abertura de bases de **dados** da administração pública, que deverá conter os dados de contato do requerente e a especificação da base de dados requerida.
45. Art. 30. Qualquer interessado poderá apresentar pedido de abertura de bases de dados da administração pública, que deverá conter os **dados** de contato do requerente e a especificação da base de dados requerida.

46. Art. 30. Qualquer interessado poderá apresentar pedido de abertura de bases de dados da administração pública, que deverá conter os dados de contato do requerente e a especificação da base de **dados** requerida.
47. § 1º O requerente poderá solicitar a preservação de sua identidade quando entender que sua identificação prejudicará o princípio da impessoalidade, caso em que o canal responsável deverá resguardar os **dados** sem repassá-los ao setor, ao órgão ou à entidade responsável pela resposta.
48. § 2º Os procedimentos e os prazos previstos para o processamento de pedidos de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), aplicam-se às solicitações de abertura de bases de **dados** da administração pública.
49. § 3º Para a abertura de base de **dados** de interesse público, as informações para identificação do requerente não podem conter exigências que inviabilizem o exercício de seu direito.
50. § 4º São vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de abertura de base de **dados** públicos.
51. § 5º Os pedidos de abertura de base de **dados** públicos, bem como as respectivas respostas, deverão compor base de dados aberta de livre consulta.
52. § 5º Os pedidos de abertura de base de dados públicos, bem como as respectivas respostas, deverão compor base de **dados** aberta de livre consulta.
53. § 6º Consideram-se automaticamente passíveis de abertura as bases de **dados** que não contenham informações protegidas por lei.
54. Art. 32. A existência de inconsistências na base de **dados** não poderá obstar o atendimento da solicitação de abertura. (Promulgação partes vetadas)
55. Art. 33. A solicitação de abertura da base de **dados** será considerada atendida a partir da notificação ao requerente sobre a disponibilização e a catalogação da base de dados para acesso público no site oficial do órgão ou da entidade na internet.
56. Art. 33. A solicitação de abertura da base de dados será considerada atendida a partir da notificação ao requerente sobre a disponibilização e a catalogação da base de **dados** para acesso público no site oficial do órgão ou da entidade na internet.
57. Art. 34. É direito do requerente obter o inteiro teor da decisão negativa de abertura de base de **dados**.
58. Parágrafo único. Eventual decisão negativa à solicitação de abertura de base de **dados** ou decisão de prorrogação de prazo, em razão de custos desproporcionais ou não previstos pelo órgão ou pela entidade da administração pública, deverá ser acompanhada da devida análise técnica que conclua pela inviabilidade orçamentária da solicitação.
59. Art. 35. No caso de indeferimento de abertura de base de **dados**, poderá o interessado interpor recurso contra a decisão no prazo de 10 (dez) dias, contado de sua ciência. (Promulgação partes vetadas)
60. Art. 36. Os órgãos gestores de **dados** poderão disponibilizar em transparência ativa dados de pessoas físicas e jurídicas para fins de pesquisa acadêmica e de monitoramento e de avaliação de políticas públicas, desde que anonimizados antes de sua disponibilização os dados protegidos por sigilo ou com restrição de acesso prevista, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).
61. Art. 36. Os órgãos gestores de dados poderão disponibilizar em transparência ativa **dados** de pessoas físicas e jurídicas para fins de pesquisa acadêmica e de monitoramento e de avaliação de políticas públicas, desde que anonimizados antes de sua disponibilização os dados protegidos por sigilo ou com restrição de acesso prevista, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).
62. Art. 36. Os órgãos gestores de dados poderão disponibilizar em transparência ativa dados de pessoas físicas e jurídicas para fins de pesquisa acadêmica e de monitoramento e de avaliação de políticas públicas, desde que anonimizados antes de sua disponibilização os **dados** protegidos por sigilo ou com restrição de acesso prevista, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).
63. Seção II

    Da Interoperabilidade de Dados entre Órgãos Públicos

64. Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de **dados**, inclusive os controladores de dados pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas digitais, considerando:

65. Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de **dados** pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas digitais, considerando:
66. I - a interoperabilidade de informações e de **dados** sob gestão dos órgãos e das entidades referidos no art. 2º desta Lei, respeitados as restrições legais, os requisitos de segurança da informação e das comunicações, as limitações tecnológicas e a relação custo-benefício da interoperabilidade;
67. II - a otimização dos custos de acesso a **dados** e o reaproveitamento, sempre que possível, de recursos de infraestrutura de acesso a dados por múltiplos órgãos e entidades;
68. II - a otimização dos custos de acesso a dados e o reaproveitamento, sempre que possível, de recursos de infraestrutura de acesso a **dados** por múltiplos órgãos e entidades;
69. III - a proteção de **dados** pessoais, observada a legislação vigente, especialmente a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
70. II - aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública, por meio de mecanismos de manutenção da integridade e da segurança da informação no tratamento das bases de **dados**, tornando-as devidamente qualificadas e consistentes;
71. IV - facilitar a interoperabilidade de **dados** entre os órgãos de governo;
72. V - realizar o tratamento de informações das bases de **dados** a partir do número de inscrição do cidadão no CPF, conforme previsto no art. 11 da Lei nº 13.444, de 11 de maio de 2017.
73. Parágrafo único. Aplicam-se aos **dados** pessoais tratados por meio de mecanismos de interoperabilidade as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
74. Art. 40. Os órgãos abrangidos por esta Lei serão responsáveis pela publicidade de seus registros de referência e pelos mecanismos de interoperabilidade de que trata esta Seção.

    § 1º As pessoas físicas e jurídicas poderão verificar a exatidão, a correção e a completude de qualquer um dos seus **dados** contidos nos registros de referência, bem como monitorar o acesso a esses dados.

75. § 1º As pessoas físicas e jurídicas poderão verificar a exatidão, a correção e a completude de qualquer um dos seus dados contidos nos registros de referência, bem como monitorar o acesso a esses **dados**.
76. § 2º Nova base de **dados** somente poderá ser criada quando forem esgotadas as possibilidades de utilização dos registros de referência existentes.
77. Art. 41. É de responsabilidade dos órgãos e das entidades referidos no art. 2º desta Lei os custos de adaptação de seus sistemas e de suas bases de **dados** para a implementação da interoperabilidade.
78. Art. 42. Os órgãos e as entidades referidos no art. 2º desta Lei, mediante opção do usuário, poderão realizar todas as comunicações, as notificações e as intimações por meio eletrônico.

    Art. 43. As ferramentas usadas para os atos de que trata o art. 42 desta Lei:

    V - conservarão os **dados** de envio e de recebimento por, pelo menos, 5 (cinco) anos.

79. Art. 44. Os entes públicos poderão instituir laboratórios de inovação, abertos à participação e à colaboração da sociedade para o desenvolvimento e a experimentação de conceitos, de ferramentas e de métodos inovadores para a gestão pública, a prestação de serviços públicos, o tratamento de **dados** produzidos pelo poder público e a participação do cidadão no controle da administração pública.
80. Art. 45. Os laboratórios de inovação terão como diretrizes:

    VIII - apoio a políticas públicas orientadas por **dados** e com base em evidências, a fim de subsidiar a tomada de decisão e de melhorar a gestão pública;

81. Art. 51. O art. 3º da Lei nº 7.116, de 29 de agosto de 1983, passa a vigorar com a seguinte redação:

    "Art. 3º .
    .....

    g) assinatura do dirigente do órgão expedidor;

    h) número de inscrição no Cadastro de Pessoas Físicas (CPF).

§ 1º A inclusão do número de inscrição no CPF na Carteira de Identidade, conforme disposto na alínea “h” do caput deste artigo, ocorrerá sempre que o órgão de identificação tiver acesso a documento comprobatório ou à base de **dados** administrada pela Secretaria Especial da Receita Federal do Brasil.

82. § 2º A incorporação do número de inscrição no CPF à Carteira de Identidade será precedida de consulta e de validação com a base de **dados** administrada pela Secretaria Especial da Receita Federal do Brasil.
83. O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu promulgo, nos termos do parágrafo 5o do art. 66 da Constituição Federal, as seguintes partes vetadas da Lei no 14.129, de 29 de março de 2021:

    “Art. 32. A existência de inconsistências na base de **dados** não poderá obstar o atendimento da solicitação de abertura.”

84. “Art. 35. No caso de indeferimento de abertura de base de **dados**, poderá o interessado interpor recurso contra a decisão no prazo de 10 (dez) dias, contado de sua ciência.

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

O termo **“Digital”** e mencionado **48 veze**s, e o termo **“Digitais” 11 vezes**, totalizando **59 resultados**

TERMO “DIGITAL”

1. LEI Nº 14.129, DE 29 DE MARÇO DE 2021 - Dispõe sobre princípios, regras e instrumentos para o Governo **Digital** e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017.
2. Art. 1º Esta Lei dispõe sobre princípios, regras e instrumentos para o aumento da eficiência da administração pública, especialmente por meio da desburocratização, da inovação, da transformação **digital** e da participação do cidadão.
3. Art. 3º São princípios e diretrizes do Governo Digital e da eficiência pública:
4. III - a possibilidade aos cidadãos, às pessoas jurídicas e aos outros entes públicos de demandar e de acessar serviços públicos por meio **digital**, sem necessidade de solicitação presencial;
5. XX - o estímulo a ações educativas para qualificação dos servidores públicos para o uso das tecnologias digitais e para a inclusão **digital** da população;
6. XXI - o apoio técnico aos entes federados para implantação e adoção de estratégias que visem à transformação **digital** da administração pública;
7. Art. 4º Para os fins desta Lei, considera-se:

    II - autosserviço: acesso pelo cidadão a serviço público prestado por meio **digital**, sem necessidade de mediação humana;

8. IV - dados abertos: dados acessíveis ao público, representados em meio **digital**, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou tratamento por qualquer pessoa, física ou jurídica;
9. IX - plataformas de governo **digital**: ferramentas digitais e serviços comuns aos órgãos, normalmente ofertados de forma centralizada e compartilhada, necessárias para a oferta digital de serviços e de políticas públicas;
10. IX - plataformas de governo digital: ferramentas digitais e serviços comuns aos órgãos, normalmente ofertados de forma centralizada e compartilhada, necessárias para a oferta **digital** de serviços e de políticas públicas;
11. CAPÍTULO II

    DA DIGITALIZAÇÃO DA ADMINISTRAÇÃO PÚBLICA E DA PRESTAÇÃO **DIGITAL** DE SERVIÇOS PÚBLICOS - GOVERNO DIGITAL

12. DA DIGITALIZAÇÃO DA ADMINISTRAÇÃO PÚBLICA E DA PRESTAÇÃO DIGITAL DE SERVIÇOS PÚBLICOS - GOVERNO **DIGITAL**

13. Art. 5º A administração pública utilizará soluções digitais para a gestão de suas políticas finalísticas e administrativas e para o trâmite de processos administrativos eletrônicos.

    Parágrafo único. Entes públicos que emitem atestados, certidões, diplomas ou outros documentos comprobatórios com validade legal poderão fazê-lo em meio **digital**, assinados eletronicamente na forma do art. 7º desta Lei e da Lei nº 14.063, de 23 de setembro de 2020.

14. Art. 7º Os documentos e os atos processuais serão válidos em meio **digital** mediante o uso de assinatura eletrônica, desde que respeitados parâmetros de autenticidade, de integridade e de segurança adequados para os níveis de risco em relação à criticidade da decisão, da informação ou do serviço específico, nos termos da lei.
15. Seção II

    Do Governo **Digital**

16. Art. 14. A prestação **digital** dos serviços públicos deverá ocorrer por meio de tecnologias de amplo acesso pela população, inclusive pela de baixa renda ou residente em áreas rurais e isoladas, sem prejuízo do direito do cidadão a atendimento presencial.
17. Parágrafo único. O acesso à prestação **digital** dos serviços públicos será realizado, preferencialmente, por meio do autosserviço.
18. Art. 15. A administração pública participará, de maneira integrada e cooperativa, da consolidação da Estratégia Nacional de Governo **Digital,** editada pelo Poder Executivo federal, que observará os princípios e as diretrizes de que trata o art. 3º desta Lei.
19. Art. 16. A administração pública de cada ente federado poderá editar estratégia de governo **digital**, no âmbito de sua competência, buscando a sua compatibilização com a estratégia federal e a de outros entes.
20. Art. 17. O Poder Executivo federal poderá criar redes de conhecimento, com o objetivo de:

    III - discutir sobre os desafios enfrentados e as possibilidades de ação quanto ao Governo **Digital** e à eficiência pública;

21. IV - prospectar novas tecnologias para facilitar a prestação de serviços públicos disponibilizados em meio **digital**, o fornecimento de informações e a participação social por meios digitais.
22. Seção IV

    Dos Componentes do Governo **Digital**

23. Art. 18. São componentes essenciais para a prestação **digital** dos serviços públicos na administração pública:
24. I - a Base Nacional de Serviços Públicos;

    II - as Cartas de Serviços ao Usuário, de que trata a Lei nº 13.460, de 26 de junho de 2017; e

    III - as Plataformas de Governo **Digital**.

25. Subseção III

    Das Plataformas de Governo **Digital**

26. Art. 20. As Plataformas de Governo **Digital,** instrumentos necessários para a oferta e a prestação digital dos serviços públicos de cada ente federativo, deverão ter pelo menos as seguintes funcionalidades:
27. Art. 20. As Plataformas de Governo Digital, instrumentos necessários para a oferta e a prestação **digital** dos serviços públicos de cada ente federativo, deverão ter pelo menos as seguintes funcionalidades:
28. I - ferramenta **digital** de solicitação de atendimento e de acompanhamento da entrega dos serviços públicos; e

    II - painel de monitoramento do desempenho dos serviços públicos.

29. § 1º As Plataformas de Governo **Digital** deverão ser acessadas por meio de portal, de aplicativo ou de outro canal digital único e oficial, para a disponibilização de informações institucionais, notícias e prestação de serviços públicos.

30. § 1º As Plataformas de Governo Digital deverão ser acessadas por meio de portal, de aplicativo ou de outro canal **digital** único e oficial, para a disponibilização de informações institucionais, notícias e prestação de serviços públicos.
31. Art. 21. A ferramenta **digital** de atendimento e de acompanhamento da entrega dos serviços públicos de que trata o inciso I do caput do art. 20 desta Lei deve apresentar, no mínimo, as seguintes características e funcionalidades:
32. II - solicitação **digital** do serviço;
33. III - agendamento **digital,** quando couber;
34. VIII - possibilidade de pagamento **digital** de serviços públicos e de outras cobranças, quando necessário;
35. Seção V

    Da Prestação **Digital** dos Serviços Públicos

36. Art. 24. Os órgãos e as entidades responsáveis pela prestação **digital** de serviços públicos deverão, no âmbito de suas competências:
37. I - manter atualizadas:

    a) as Cartas de Serviços ao Usuário, a Base Nacional de Serviços Públicos e as Plataformas de Governo **Digital**;

38. VII - realizar a gestão das suas políticas públicas com base em dados e em evidências por meio da aplicação de inteligência de dados em plataforma **digital**; e
39. Art. 25. As Plataformas de Governo **Digital** devem dispor de ferramentas de transparência e de controle do tratamento de dados pessoais que sejam claras e facilmente acessíveis e que permitam ao cidadão o exercício dos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
40. Seção VI

    Dos Direitos dos Usuários da Prestação **Digital** de Serviços Públicos

41. Art. 27. São garantidos os seguintes direitos aos usuários da prestação **digital** de serviços públicos, além daqueles constantes das Leis nºs 13.460, de 26 de junho de 2017, e 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais):
42. I - gratuidade no acesso às Plataformas de Governo **Digital**;
43. III - padronização de procedimentos referentes à utilização de formulários, de guias e de outros documentos congêneres, incluídos os de formato **digital**;
44. IV - recebimento de protocolo, fisico ou **digital**, das solicitações apresentadas; e
45. Art. 38. Os órgãos e as entidades responsáveis pela prestação **digital** de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas digitais, considerando:
46. Art. 48. Os órgãos e as entidades a que se refere o art. 2º desta Lei deverão estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e de controle interno com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos da prestação **digital** de serviços públicos que possam impactar a consecução dos objetivos da organização no cumprimento de sua missão institucional e na proteção dos usuários, observados os seguintes princípios:
47. Art. 50. O acesso e a conexão para o uso de serviços públicos poderão ser garantidos total ou parcialmente pelo governo, com o objetivo de promover o acesso universal à prestação **digital** dos serviços públicos e a redução de custos aos usuários, nos termos da lei.
48. Art. 53. O caput do art. 3º da Lei nº 12.682, de 9 de julho de 2012, passa a vigorar com a seguinte redação:

    "Art. 3º O processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento **digital**, com o emprego de assinatura eletrônica.

TERMO "DIGITAIS"

1. Art. 3º São princípios e diretrizes do Governo Digital e da eficiência pública:

I - a desburocratização, a modernização, o fortalecimento e a simplificação da relação do poder público com a sociedade, mediante serviços **digitais**, acessíveis inclusive por dispositivos móveis;

2. XX - o estímulo a ações educativas para qualificação dos servidores públicos para o uso das tecnologias digitais e para a inclusão **digital** da população;
3. Art. 4º Para os fins desta Lei, considera-se:

   IX - plataformas de governo digital: ferramentas **digitais** e serviços comuns aos órgãos, normalmente ofertados de forma centralizada e compartilhada, necessárias para a oferta digital de serviços e de políticas públicas;

4. Art. 5º A administração pública utilizará soluções **digitais** para a gestão de suas políticas finalísticas e administrativas e para o trâmite de processos administrativos eletrônicos.
5. Art. 11. Os documentos nato-**digitais** assinados eletronicamente na forma do art. 7º desta Lei são considerados originais para todos os efeitos legais.
6. Art. 12. O formato e o armazenamento dos documentos **digitais** deverão garantir o acesso e a preservação das informações, nos termos da legislação arquivística nacional.
7. Art. 13. A guarda dos documentos **digitais** e dos processos administrativos eletrônicos considerados de valor permanente deverá estar de acordo com as normas previstas pela instituição arquivística pública responsável por sua custódia.
8. Art. 17. O Poder Executivo federal poderá criar redes de conhecimento, com o objetivo de:

   IV - prospectar novas tecnologias para facilitar a prestação de serviços públicos disponibilizados em meio digital, o fornecimento de informações e a participação social por meios **digitais**.

9. Art. 24. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos deverão, no âmbito de suas competências:

   III - integrar os serviços públicos às ferramentas de notificação aos usuários, de assinatura eletrônica e de meios de pagamento **digitais,** quando aplicáveis;

10. Art. 26. Presume-se a autenticidade de documentos apresentados por usuários dos serviços públicos ofertados por meios **digitais**, desde que o envio seja assinado eletronicamente.
11. Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas **digitais**, considerando:

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

2021 - LEI Nº 14.155 (Altera o Código Penal e o Código de Processo Penal)

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm#:~:text=Altera%20o%20Decreto%2DLei%20n%C2%BA,Penal)%2C%20para%20definir%20a%20compet%C3%AAncia

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

O termo **"Crimes de Violação de Dispositivo Informático"** é mencionado **1 vez**, totalizando **1 resultado**

“TERMO CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO”

1. LEI Nº 14.155, DE 27 DE MAIO DE 2021 - Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os **crimes de violação de dispositivo informático**, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo “dados” é mencionado **1 vez**, totalizando **1 resultado**.

TERMO “DADOS”

1. Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:

   “Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir **dados** ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

   Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.....

   § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico

   § 3º .....

   Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
   .....” (NR)

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

Os termos referidos não são mencionados nesta legislação

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

2023 - DECRETO Nº 11.491 (Promulgação da Convenção sobre o Crime Cibernético)

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

O termo **"Crime Cibernético"** é mencionado **6 vezes, "Crimes cibernéticos" 2 vezes**, **"Crimes Informáticos" 3 vezes**, totalizando **11 resultados**

TERMO "CRIME CIBERNÉTICO"

1. Promulga a Convenção sobre o **Crime Cibernético**, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.
2. Considerando que a República Federativa do Brasil firmou a Convenção sobre o **Crime Cibernético**, em Budapeste, em 23 de novembro de 2001;
3. Art. 1º Fica promulgada a Convenção sobre o **Crime Cibernético**, firmada em Budapeste, em 23 de novembro de 2001, anexa a este Decreto.
4. Convenção sobre o **Crime Cibernético**

Preâmbulo

5. Convencidos da necessidade de buscar prioritariamente uma política criminal comum destinada à proteção da sociedade contra o **crime cibernético**, nomeadamente pela adoção de legislação apropriada e pela promoção da cooperação internacional, entre outras medidas;
6. Atentando para a Resolução n. 1, adotada durante a 21ª Conferência dos Ministros da Justiça europeus (Praga, de 10 a 11 de junho de 1997), que recomendou ao Conselho de Ministros apoiar o trabalho desenvolvido pelo Comitê Europeu para os Problemas Criminais (CDPC) sobre criminalidade cibernética, a fim de aprovar leis penais domésticas compatíveis e possibilitar meios eficazes de investigação de tais infrações, bem como para a Resolução n. 3, aprovada pela 23ª Conferência de Ministros da Justiça Europeus (Londres, 8 e 9 de junho de 2000), que encorajou as partes negociantes a continuar seus esforços para encontrar soluções adequadas para permitir que o maior número possível de Estados se tornem partes da Convenção e reconheceu a necessidade de um sistema de cooperação internacional imediato e eficiente, que considere devidamente as necessidades específicas da luta contra o **crime cibernético**;

TERMO "CRIMES CIBERNÉTICO"

1. Acreditando que um combate eficiente aos **crimes cibernéticos** exige uma cooperação internacional em assuntos penais mais intensa, rápida e eficaz;
2. Artigo 46 - Consultas entre as Partes

1. As Partes, quando conveniente, consultar-se-ão periodicamente para facilitar:

a. a utilização e a implementação eficientes desta Convenção, inclusive a identificação de quaisquer problemas a ela relativos, bem como dos efeitos de qualquer declaração ou reserva apresentada de acordo com esta Convenção;

b. a troca de informações sobre importantes inovações jurídicas, políticas ou tecnológicas relativas a **crimes cibernéticos** e à coleta de provas em forma eletrônica;

TERMO "CRIMES INFORMÁTICOS "

1. Levando em conta as atuais convenções do Conselho da Europa sobre cooperação em matéria criminal, bem como os tratados similares existentes entre membros do Conselho da Europa e outros Estados, e enfatizando que a presente Convenção visa a complementar esses pactos de modo a tornar as investigações criminais e os procedimentos relacionados a **crimes informáticos** mais eficientes e de modo a possibilitar a obtenção de provas digitais de uma infração penal;
2. Evocando a Recomendação n. R (85) 10 do Comitê de Ministros relativa à aplicação prática da Convenção Europeia para Assistência Mútua em Assuntos Penais a respeito de cartas rogatórias para a interceptação de telecomunicações; a Recomendação n. R (88) 2 sobre violação de direitos autorais e direitos correlatos; a Recomendação n. R (87) 15, que regula o uso policial de dados pessoais; a Recomendação n. R (95) 4 sobre a proteção de dados pessoais nos serviços de telecomunicações, com referência especial aos serviços de telefonia; bem como a Recomendação n. R (89) 9, que estabelece diretrizes para os legislativos nacionais na definição de certos **crimes informáticos** e a Recomendação n. R (95) 13, que diz respeito a problemas de direito processual penal relacionados à tecnologia da informação;
3. Título 2 - **Crimes informáticos**

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **"Proteção de Dados"** é mencionado **3 vezes**, enquanto o termo **"Dados"**, de forma isolada, é mencionado **88 vezes**, totalizando **91 resultados**

TERMO "PROTEÇÃO DE DADOS"

1. Também preocupados com o direito à **proteção de dados** pessoais, como previsto, por exemplo, na Convenção Europeia para a Proteção de Dados Pessoais sujeitos a Processamento Eletrônico, de 1981;
2. Também preocupados com o direito à proteção de dados pessoais, como previsto, por exemplo, na Convenção Europeia para a **Proteção de Dados** Pessoais sujeitos a Processamento Eletrônico, de 1981;
3. vocando a Recomendação n. R (85) 10 do Comitê de Ministros relativa à aplicação prática da Convenção Europeia para Assistência Mútua em Assuntos Penais a respeito de cartas rogatórias para a interceptação de telecomunicações; a Recomendação n. R (88) 2 sobre violação de direitos autorais e direitos correlatos; a Recomendação n. R (87) 15, que regula o uso policial de dados pessoais; a Recomendação n. R (95) 4 sobre a **proteção de dados** pessoais nos serviços de telecomunicações, com referência especial aos serviços de telefonia; bem como a Recomendação n. R (89) 9, que estabelece diretrizes para os legislativos nacionais na definição de certos crimes informáticos e a Recomendação n. R (95) 13, que diz respeito a problemas de direito processual penal relacionados à tecnologia da informação;

TERMO " DADOS" e "DADO"

1. Convencidos de que a presente Convenção é necessária para impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e **dados** de computador, bem como para impedir o abuso de tais sistemas, redes e dados, ao prever a criminalização de tais condutas, tal como se encontram descritas nesta Convenção, e ao prever a criação de competências suficientes para combater efetivamente tais crimes, facilitando a descoberta, a investigação e o julgamento dessas infrações penais em instâncias domésticas e internacionais, e ao estabelecer mecanismos para uma cooperação internacional rápida e confiável;
2. Convencidos de que a presente Convenção é necessária para impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados de computador, bem como para impedir o abuso de tais sistemas, redes e **dados**, ao prever a criminalização de tais condutas, tal como se encontram descritas nesta Convenção, e ao prever a criação de competências suficientes para combater efetivamente tais crimes, facilitando a descoberta, a investigação e o julgamento dessas infrações penais em instâncias domésticas e internacionais, e ao estabelecer mecanismos para uma cooperação internacional rápida e confiável;
3. Evocando a Recomendação n. R (85) 10 do Comitê de Ministros relativa à aplicação prática da Convenção Europeia para Assistência Mútua em Assuntos Penais a respeito de cartas rogatórias para a interceptação de telecomunicações; a Recomendação n. R (88) 2 sobre violação de direitos autorais e direitos correlatos; a Recomendação n. R (87) 15, que regula o uso policial de **dados** pessoais; a Recomendação n. R (95) 4 sobre a proteção de dados pessoais nos serviços de telecomunicações, com referência especial aos serviços de telefonia; bem como a Recomendação n. R (89) 9, que estabelece diretrizes para os legislativos nacionais na definição de certos crimes informáticos e a Recomendação n. R (95) 13, que diz respeito a problemas de direito processual penal relacionados à tecnologia da informação;
4. Artigo 1 - Definições

   Para os fins desta Convenção:

   a. "sistema de computador" designa qualquer aparelho ou um conjunto de aparelhos interconectados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o processamento eletrônico de **dados**;

5. b. "**dado** de computador" é qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa;

6. c. “provedor de serviços” significa:

   (i) qualquer entidade pública ou privada que permite aos seus usuários se comunicarem por meio de um sistema de computador, e

   (ii) qualquer outra entidade que realiza o processamento ou armazenamento de **dados** de computador em nome desses serviços de comunicação ou de seus usuários.

7. d. “**dados** de tráfego” designa quaisquer dados de computador referentes a uma comunicação por meio de um sistema informatizado, gerados por um computador que seja parte na cadeia de comunicação, e que indicam sua origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado.
8. d. “dados de tráfego” designa quaisquer **dados** de computador referentes a uma comunicação por meio de um sistema informatizado, gerados por um computador que seja parte na cadeia de comunicação, e que indicam sua origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado.
9. Capítulo II - Medidas a serem adotadas nas jurisdições nacionais

   Seção 1 - Direito Penal

   Título 1 - Crimes contra a confidencialidade, integridade e disponibilidade de **dados** e sistemas de computador

10. Artigo 2 - Acesso ilegal

    Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter **dados** de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador.

11. Artigo 3 - Interceptação ilícita

    Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime em sua legislação interna a interceptação ilegal e intencional, realizada por meios técnicos, de transmissões não-públicas de **dados** de computador para um sistema informatizado, a partir dele ou dentro dele, inclusive das emissões eletromagnéticas oriundas de um sistema informatizado que contenham esses dados de computador. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento com objetivo fraudulento ou que seja praticado contra um sistema de computador que esteja conectado a outro sistema de computador.

12. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime em sua legislação interna a interceptação ilegal e intencional, realizada por meios técnicos, de transmissões não-públicas de dados de computador para um sistema informatizado, a partir dele ou dentro dele, inclusive das emissões eletromagnéticas oriundas de um sistema informatizado que contenham esses **dados** de computador. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento com objetivo fraudulento ou que seja praticado contra um sistema de computador que esteja conectado a outro sistema de computador.

13. Artigo 4 - Violação de **dados**

14. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a danificação, a eliminação, a deterioração, a alteração ou a supressão dolosas e não autorizadas de **dados** de computador.

    2. Qualquer Parte pode reservar-se o direito de exigir que da conduta descrita no parágrafo 1 resulte sério dano para a vítima.

15. Artigo 5 - Interferência em sistema

    Cada Parte adotará medidas legislativas semelhantes e outras providências necessárias para tipificar como crime, em sua legislação interna, qualquer grave obstrução ou impedimento, dolosos e não

autorizados, do funcionamento de um sistema de computador por meio da inserção, transmissão, danificação, apagamento, deterioração, alteração ou supressão de **dados** de computador.

16. Artigo 6 - Uso indevido de aparelhagem

    1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando dolosas e não autorizadas:

    a. a produção, venda, aquisição para uso, importação, distribuição ou a disponibilização por qualquer meio de:

    i. aparelho, incluindo um programa de computador, desenvolvido ou adaptado principalmente para o cometimento de quaisquer dos crimes estabelecidos de acordo com os artigos de 2 a 5;

    ii. uma senha de computador, código de acesso, ou **dados** similares por meio dos quais se possa acessar um sistema de computador ou qualquer parte dele, com a intenção de usá-lo para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5; e

    b. a posse de qualquer dos instrumentos referidos nos parágrafos a.i ou ii, com a intenção de usá-los para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5. Qualquer Parte pode exigir, por lei, a posse de um número mínimo de tais instrumentos, para que a responsabilidade criminal se materialize.

17. Título 2 - Crimes informáticos

    Artigo 7 - Falsificação informática

    Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de **dados** de computador, de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento.

18. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador, de que resultem **dados** inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento.
19. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador, de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os **dados** serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento.
20. Artigo 8 - Fraude informática

    Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de:

    a. qualquer inserção, alteração, apagamento ou supressão de **dados** de computador;

    b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita.

21. Título 3 - Crimes relacionados ao conteúdo da informação

    Artigo 9 - Pornografia infantil

    1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando cometidas dolosamente e de forma não autorizadas:

e. possuir pornografia infantil num sistema de computador ou num dispositivo de armazenamento de **dados** de computador.

22. Título 2 - Preservação expedita de **dados** armazenados em computador
23. Artigo 16 - Preservação expedita de **dados** de computador
24. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para permitir que a autoridade competente ordene ou obtenha a expedita preservação de **dados** de computador especificados, incluindo dados de tráfego, que tenham sido armazenados por meio de um sistema de computador, especialmente quando haja razões para admitir que os dados de computador estão particularmente sujeitos a perda ou modificação.
25. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para permitir que a autoridade competente ordene ou obtenha a expedita preservação de dados de computador especificados, incluindo **dados de** tráfego, que tenham sido armazenados por meio de um sistema de computador, especialmente quando haja razões para admitir que os dados de computador estão particularmente sujeitos a perda ou modificação.
26. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para permitir que a autoridade competente ordene ou obtenha a expedita preservação de dados de computador especificados, incluindo dados de tráfego, que tenham sido armazenados por meio de um sistema de computador, especialmente quando haja razões para admitir que os **dados** de computador estão particularmente sujeitos a perda ou modificação.
27. 2. Se a Parte der efeito ao parágrafo 1 acima por meio de uma ordem a uma pessoa para preservar **dados** de computador determinados que estejam sob sua posse, detenção ou controle, o Estado adotará medidas legislativas e outras providências necessárias para obrigar essa pessoa a preservar e manter a integridade desses dados de computador pelo período de tempo necessário, até o máximo de 90 (noventa) dias, a fim de permitir à autoridade competente buscar sua revelação. Qualquer Parte pode estipular que tal ordem possa ser renovada subsequentemente.
28. 2. Se a Parte der efeito ao parágrafo 1 acima por meio de uma ordem a uma pessoa para preservar dados de computador determinados que estejam sob sua posse, detenção ou controle, o Estado adotará medidas legislativas e outras providências necessárias para obrigar essa pessoa a preservar e manter a integridade desses **dados** de computador pelo período de tempo necessário, até o máximo de 90 (noventa) dias, a fim de permitir à autoridade competente buscar sua revelação. Qualquer Parte pode estipular que tal ordem possa ser renovada subsequentemente.
29. 3. Cada Parte adotará medidas legislativas e outras providências necessárias para obrigar o detentor dos **dados** ou terceiro encarregado da sua preservação, a manter em sigilo o início do procedimento investigativo por um período de tempo estabelecido na sua legislação interna.
30. Artigo 17 - Preservação expedita e revelação parcial de **dados** de tráfego
31. 1. Cada Parte adotará, a respeito dos **dados** de tráfego que devem ser preservados de acordo com o Artigo 16, medidas legislativas e outras providências pertinentes para:
32. a. assegurar que essa expedita preservação de **dados** de tráfego seja possível independentemente do número de provedores de serviço envolvidos na transmissão dessa comunicação; e
33. b. assegurar expedita revelação à autoridade competente da Parte, ou a uma pessoa indicada por essa autoridade, de um conjunto suficiente de **dados** de tráfego que permitam à Parte identificar os provedores de serviço e o caminho por meio do qual a comunicação se realizou.
34. Título 3 - Ordem de exibição

    Artigo 18 - Ordem de exibição

    1. Cada Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a autoridades competentes para ordenar:

    a. a qualquer pessoa residente em seu território a entregar **dados** de computador especificados, por ela controlados ou detidos, que estejam armazenados num sistema de computador ou em qualquer meio de armazenamento de dados de computador;

35. 3. Paras os fins deste Artigo, o termo “informações cadastrais do assinante” indica qualquer informação mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinantes de seus serviços, com exceção dos **dados** de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:
36. Título 4 - Busca e apreensão de **dados** de computador

37. Artigo 19 - Busca e apreensão de **dados** de computador
38. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para busca ou investigação, em seu território:

    a. de qualquer sistema de computador ou de parte dele e dos **dados** nele armazenados; e

39. b. de qualquer meio de armazenamento de **dados** de computador no qual possam estar armazenados os dados procurados em seu território.
40. b. de qualquer meio de armazenamento de dados de computador no qual possam estar armazenados os **dados** procurados em seu território.
41. 2. Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que, quando a autoridade competente proceder a busca em um determinado sistema de computador ou em parte dele, de acordo com o parágrafo 1.a, e tiver fundadas razões para supor que os **dados** procurados estão armazenados em outro sistema de computador ou em parte dele, situado em seu território, e que tais dados são legalmente acessíveis a partir do sistema inicial, ou disponíveis a esse sistema, tal autoridade poderá estender prontamente a busca ou o acesso ao outro sistema.
42. 2. Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que, quando a autoridade competente proceder a busca em um determinado sistema de computador ou em parte dele, de acordo com o parágrafo 1.a, e tiver fundadas razões para supor que os dados procurados estão armazenados em outro sistema de computador ou em parte dele, situado em seu território, e que tais **dados** são legalmente acessíveis a partir do sistema inicial, ou disponíveis a esse sistema, tal autoridade poderá estender prontamente a busca ou o acesso ao outro sistema.
43. 3. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para apreender ou proteger **dados** de computador acessados de acordo com os parágrafos 1 ou 2. Estas medidas incluirão o poder de:
44. a. apreender ou proteger um sistema de computador ou parte dele ou um meio de armazenamento de **dados**;
45. b. fazer e guardar uma cópia desses **dados** de computador;
46. c. manter a integridade dos **dados** de computador relevantes;
47. d. tornar inacessíveis esses **dados** no sistema de computador acessado ou dele removê-los.
48. 4. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a sua autoridade competente para determinar que qualquer pessoa que conheça o funcionamento do sistema de computador ou as medidas empregadas para proteger os **dados** nele armazenados que forneça, tanto quanto seja razoável, as informações necessárias para permitir as providências referidas nos parágrafos 1 e 2.
49. Título 5 - Obtenção de **dados** de computador em tempo real
50. Artigo 20 - Obtenção de **dados** de tráfego em tempo real
51. 1. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes, no que seja pertinente a **dados** de tráfego, em tempo real, vinculados a comunicações específicas, ocorridas em seu território, por meio de um sistema de computador, para:
52. a. coletar tais **dados** ou gravá-los por meios técnicos, no território da Parte, e
53. b. obrigar um provedor de serviço, nos limites de sua capacidade técnica:

    i. a reunir tais **dados** ou gravá-los por meios técnicos, no território da Parte; ou

54. ii. a cooperar com as autoridades competentes ou auxiliá-las na obtenção ou gravação de tais **dados**.
55. 2. Quando uma Parte, em razão dos princípios legais de seu sistema jurídico, não puder adotar as medidas referidas no parágrafo 1.a., a Parte poderá substituí-las por medidas legislativas e outras providências necessárias para assegurar a obtenção ou a gravação em tempo real, por meios técnicos aplicados em seu próprio território, dos **dados** de tráfego vinculados a uma comunicação específica, transmitida nesse território.
56. Artigo 21 - Interceptação de **dados** de conteúdo
57. Artigo 28 - Confidencialidade e limitações de uso

    2. A Parte requerida pode condicionar o fornecimento de informação ou de **dados** em atendimento a um pedido:

    a. à sua manutenção em sigilo, quando o pedido de assistência jurídica mútua não puder ser cumprido sem tal condição, ou

    b. à sua não utilização para investigações ou procedimentos diversos daqueles indicados no pedido.

58. 4. Qualquer Parte que forneça informações ou **dados** sob uma condição referida no parágrafo 2 pode exigir que a outra Parte esclareça, em relação àquela condição, o uso feito de tais informações ou dados.
59. 4. Qualquer Parte que forneça informações ou dados sob uma condição referida no parágrafo 2 pode exigir que a outra Parte esclareça, em relação àquela condição, o uso feito de tais informações ou **dados**.
60. Seção 2 - Disposições específicas

    Título 1 - Assistência mútua em relação a medidas cautelares

    Artigo 29 - Conservação expedita de **dados** armazenados em computador

61. 1. Qualquer Parte pode pedir a outra Parte que determine a obtenção ou de qualquer modo obtenha a expedita conservação de **dados** armazenados por meio de um sistema de computador, localizado no território daquela outra Parte, em relação aos quais a Parte requerente pretende apresentar um pedido de assistência mútua para busca ou acesso, apreensão ou guarda, ou revelação dos dados.
62. 1. Qualquer Parte pode pedir a outra Parte que determine a obtenção ou de qualquer modo obtenha a expedita conservação de dados armazenados por meio de um sistema de computador, localizado no território daquela outra Parte, em relação aos quais a Parte requerente pretende apresentar um pedido de assistência mútua para busca ou acesso, apreensão ou guarda, ou revelação dos **dados**.
63. 2. Qualquer pedido de conservação feito de acordo com o parágrafo 1 deve especificar:

    c. os **dados** de computador armazenados a serem conservados e sua relação com o crime;

64. d. qualquer informação disponível que identifique o detentor dos **dados** de computador armazenados ou a localização do sistema de computador;
65. f. que a Parte pretende apresentar um pedido de assistência mútua para a busca ou acesso, apreensão ou guarda, ou revelação dos **dados** armazenados em computador.
66. 3. Ao receber o pedido de outra Parte, a Parte requerida adotará todas as medidas apropriadas para conservar, com presteza, os **dados** especificados, de acordo com sua legislação doméstica. Para resposta a um pedido de assistência, o princípio da dupla tipicidade não será exigido como condição para autorizar a conservação de dados.
67. 3. Ao receber o pedido de outra Parte, a Parte requerida adotará todas as medidas apropriadas para conservar, com presteza, os dados especificados, de acordo com sua legislação doméstica. Para resposta a um pedido de assistência, o princípio da dupla tipicidade não será exigido como condição para autorizar a conservação de **dados**.
68. 4. Qualquer Parte que exija a dupla tipicidade como condição para atender a um pedido de assistência mútua para a busca ou acesso, apreensão ou guarda, ou revelação de **dados** armazenados pode, em relação a outros crimes que não os tipificados de acordo com os artigos 2 a 11 desta Convenção, reservar-se o direito de recusar o pedido de conservação em conformidade com este Artigo, quando a Parte requerida tenha motivos para crer que ao tempo da revelação a condição de dupla tipicidade não terá sido atendida.
69. 6. Quando a Parte requerida verificar que a conservação não assegurará a futura disponibilidade dos **dados** ou que irá ameaçar a confidencialidade ou de outro modo prejudicar a investigação da Parte requerente, deve informar imediatamente à Parte requerente, que então decidirá se ainda assim o pedido deve ser executado.
70. 7. Qualquer conservação efetivada em resposta ao pedido referido no parágrafo 1 perdurará por prazo não inferior a 60 (sessenta) dias, a fim de permitir que a Parte requerente apresente um pedido de busca ou acesso, apreensão ou guarda, ou revelação dos **dados**. Depois da recepção de tal pedido, os dados continuarão protegidos até a decisão final.
71. 7. Qualquer conservação efetivada em resposta ao pedido referido no parágrafo 1 perdurará por prazo não inferior a 60 (sessenta) dias, a fim de permitir que a Parte requerente apresente um pedido de busca ou acesso, apreensão ou guarda, ou revelação dos dados. Depois da recepção de tal pedido, os **dados** continuarão protegidos até a decisão final.
72. Artigo 30 - Revelação expedita de **dados** de tráfego conservados
73. 1. Quando, no curso da execução de um pedido feito de acordo com o Artigo 29 para a conservação de **dados** de tráfego de uma comunicação específica, a Parte requerida descobrir que um provedor de serviços em outro Estado está envolvido na transmissão da comunicação, a Parte requerida deverá entregar rapidamente à Parte requerente dados de tráfego suficientes para identificar aquele provedor e o caminho por meio do qual se deu a comunicação.

74. 1. Quando, no curso da execução de um pedido feito de acordo com o Artigo 29 para a conservação de dados de tráfego de uma comunicação específica, a Parte requerida descobrir que um provedor de serviços em outro Estado está envolvido na transmissão da comunicação, a Parte requerida deverá entregar rapidamente à Parte requerente **dados** de tráfego suficientes para identificar aquele provedor e o caminho por meio do qual se deu a comunicação.
75. Título 2 - Assistência mútua em relação a poderes investigativos

    Artigo 31 - Assistência mútua em relação ao acesso a **dados** de computador armazenados

76. 1. Qualquer Parte pode pedir a outra Parte que realize busca, acesso, apreensão, guarda ou a revelação de **dados** armazenados por meio de um sistema de computador localizado no território da Parte requerida, inclusive dos dados que tenham sido conservados de acordo com o Artigo 29.
77. 1. Qualquer Parte pode pedir a outra Parte que realize busca, acesso, apreensão, guarda ou a revelação de dados armazenados por meio de um sistema de computador localizado no território da Parte requerida, inclusive dos **dados** que tenham sido conservados de acordo com o Artigo 29.
78. 3. O pedido receberá resposta rápida se:

    a. houver motivos para supor que importantes **dados** estão especialmente vulneráveis a perda ou modificação; ou

    b. os instrumentos, acordos e leis referidos no parágrafo 2 dispuserem de forma diferente no tocante à cooperação expedita.

79. Artigo 32 - Acesso transfronteiriço a **dados** armazenados num computador, mediante consentimento, ou a sistema de acesso público
80. Uma Parte poderá, sem a autorização de outra Parte:

    a. acessar **dados** de computador disponíveis ao público (fonte aberta), independentemente de onde os dados estejam geograficamente localizados; ou

81. a. acessar dados de computador disponíveis ao público (fonte aberta), independentemente de onde os **dados** estejam geograficamente localizados; ou
82. b. acessar ou receber, por meio de um sistema de computador em seu território, **dados** de computador armazenados no território de outra Parte, se a Parte obtiver o legítimo e voluntário consentimento de uma pessoa que tenha autoridade legal para revelar os dados à Parte interessada, por meio de um sistema de computador.
83. b. acessar ou receber, por meio de um sistema de computador em seu território, dados de computador armazenados no território de outra Parte, se a Parte obtiver o legítimo e voluntário consentimento de uma pessoa que tenha autoridade legal para revelar os **dados** à Parte interessada, por meio de um sistema de computador.
84. Artigo 33 - Assistência mútua na interceptação de **dados** de tráfego em tempo real
85. 1. As Partes conceder-se-ão assistência mútua na interceptação, em tempo real, de **dados** de tráfego vinculados a uma comunicação específica transmitida no seu território por meio de um sistema de computador. Sem prejuízo das disposições do parágrafo 2, esta assistência será regida pelas condições e procedimentos estabelecidos pela legislação interna.
86. 2. Cada Parte disponibilizará tal assistência pelo menos em relação aos crimes para os quais a interceptação de **dados** em tempo real seria possível, quando se tratasse de fatos similares de jurisdição nacional.
87. Artigo 35 - Sistema de plantão 24 por 7

    1. Cada Parte indicará um órgão de contato disponível 24 horas por dia, 7 dias por semana, de modo a assegurar a assistência imediata para investigações ou procedimentos relacionados a crimes de computador e de **dados**, ou para a obtenção de provas eletrônicas de uma infração penal. Tal assistência incluirá a facilitação, ou, se permitido pelas leis e costumes jurídicos locais, a adoção direta das seguintes medidas:

88. a. o fornecimento de suporte técnico;

    b. a conservação de **dados** de acordo com os artigos 29 e 30;

    c. a coleta de provas, o fornecimento de informação jurídica e a localização de suspeitos.

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

O termo **“Digitais”** é mencionado **1 vez**, totalizando **1 resultado**

“TERMO DIGITAIS”

1. Levando em conta as atuais convenções do Conselho da Europa sobre cooperação em matéria criminal, bem como os tratados similares existentes entre membros do Conselho da Europa e outros Estados, e enfatizando que a presente Convenção visa a complementar esses pactos de modo a tornar as investigações criminais e os procedimentos relacionados a crimes informáticos mais eficientes e de modo a possibilitar a obtenção de provas **digitais** de uma infração penal;

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

DECRETO Nº 12.573, DE 4 DE AGOSTO DE 2025 (Nova Estratégia Nacional de Cibersegurança - E-Ciber)

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm

BANCO CENTRAL - BANCO

Os termos referidos não são mencionados nesta legislação

CRIME CIBERNÉTICO - CRIMES CIBERNÉTICOS - CRIMES INFORMÁTICOS - CIBERCRIME - CRIME DIGITAL - INFRAÇÃO CIBERNÉTICA - DELITOS INFORMÁTICOS - CRIMES DE VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

O termo **“Crime Cibernético**” é mencionado **1 vez**, enquanto o termo **“Cibercrime”** é mencionado **7 vezes**, totalizando **8 resultados**

TERMO “CRIME CIBERNÉTICO”

1. Art. 4º A proteção e a conscientização do cidadão e da sociedade abrangem, no mínimo, as seguintes ações:

   XI - divulgação da Convenção sobre o **Crime Cibernético**, promulgada pelo Decreto nº 11.491, de 12 de abril de 2023, e de instrumentos congêneres, nacionais e internacionais, relacionados a cibercrimes vigentes no País;

TERMO “CIBERCRIME”

1. Definições

   Art. 2º Para fins do disposto neste Decreto, consideram-se:

   III - **cibercrime** - crime praticado contra ou por meio de ciberativos;

2. Art. 4º A proteção e a conscientização do cidadão e da sociedade abrangem, no mínimo, as seguintes ações:

   X - promoção da prevenção e do combate aos **cibercrimes**, às fraudes digitais e a outras ações maliciosas no ciberespaço por meio de atuação multissetorial;

3. XI - divulgação da Convenção sobre o Crime Cibernético, promulgada pelo Decreto nº 11.491, de 12 de abril de 2023, e de instrumentos congêneres, nacionais e internacionais, relacionados a **cibercrimes** vigentes no País;
4. XII - promoção de ações que aumentem a efetividade das operações contra o **cibercrime**;
5. XIII - estímulo ao aprimoramento normativo e estrutural dos canais para notificação de **cibercrimes**; e
6. XIV - incentivo à capacitação e ao aprimoramento dos órgãos de persecução penal na repressão aos **cibercrimes**.
7. Art. 8º A cooperação e a integração entre órgãos e entidades, públicas e privadas, abrangem, no mínimo, as seguintes ações:

   d) combater **cibercrimes** e outros ilícitos cometidos no ciberespaço;

PROTEÇÃO DE DADOS - PROTEÇÃO DOS DADOS - PROTEÇÃO DE SEUS DADOS - PROTEÇÃO A DADOS - DADOS

O termo **"Dados"** é mencionado **4 vezes**, totalizando **4 resultados**

TERMO "DADOS"

1. Definições

   Art. 2º Para fins do disposto neste Decreto, consideram-se:

   I - ciberativos - hardwares, softwares, redes, dispositivos, aplicações, serviços, sistemas e **dados** utilizados para processar, armazenar ou transmitir informações por meio eletrônico ou digital;

2. X - tecnologia da informação - conjunto de ciberativos destinados ao processamento de sistemas e de **dados**; e
3. Art. 6º A segurança e a resiliência dos serviços essenciais e das infraestruturas críticas abrangem, no mínimo, as seguintes ações:

   V - estímulo à adoção de padrões mínimos de segurança para categorias de **dados** relevantes e sensíveis;

4. X - estímulo ao aperfeiçoamento da segurança na interoperabilidade de **dados** e de canais digitais; e

SEGURANÇA DIGITAL - DIGITAL - DIGITAIS

O termo **"Digital"** é mencionado **1 vez**, enquanto o termo **"Digitais"** é mencionado **4 vezes**, totalizando **5 resultados**

TERMO "DIGITAL"

1. Definições

   Art. 2º Para fins do disposto neste Decreto, consideram-se:

   I - ciberativos - hardwares, softwares, redes, dispositivos, aplicações, serviços, sistemas e dados utilizados para processar, armazenar ou transmitir informações por meio eletrônico ou **digital**;

TERMO "DIGITAIS"

1. Proteção e conscientização do cidadão e da sociedade

   Art. 3º No âmbito da E-Ciber, a proteção e a conscientização do cidadão e da sociedade têm por objetivo criar condições seguras para o uso dos serviços **digitais**, especialmente por pessoas em situação de vulnerabilidade, tais como:

   I - crianças e adolescentes;

II - pessoas idosas; e

III - pessoas neurodivergentes.

2. Art. 4º A proteção e a conscientização do cidadão e da sociedade abrangem, no mínimo, as seguintes ações:

X - promoção da prevenção e do combate aos cibercrimes, às fraudes **digitais** e a outras ações maliciosas no ciberespaço por meio de atuação multissetorial;

3. Art. 6º A segurança e a resiliência dos serviços essenciais e das infraestruturas críticas abrangem, no mínimo, as seguintes ações:

III - adoção de mecanismos de alerta de risco na prestação de serviços **digitais**;

4. X - estímulo ao aperfeiçoamento da segurança na interoperabilidade de dados e de canais **digitais**; e

SOBERANIA DIGITAL

O termo referido não é mencionado nesta legislação

ANEXO 2 - Resultados das buscas no site do Banco Central do Brasil

Resultados da busca pelo termo "Proteção de dados" no site do BC com os seguintes filtros:

Tipo de documento: Todos
Conteúdo: Proteção de dados
Período: 01/01/1988 - 01/10/2025
Situação: Em vigor

Total de resultados encontrados na busca no site do BC: 118 resultados

- Após leitura de cada um dos resultados encontrados, foram destacados em azul os que apresentam trechos relacionados com a temática

Total de resultados compatíveis com a temática trabalhada: 33 resultados

- Todos que possuem relação com a temática foram baixados em arquivo PDF e organizados em uma pasta para posterior análise

1. **Título:** Instrução Normativa BCB n° 667, 22/9/2025
   Data/Hora Documento: 22/9/2025 20:44
   Assunto: Disciplina a dispensa da observância do limite de emissão de Pix de valor superior a R$15.000,00 (quinze mil reais) por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.
   Responsável: DEGEF
   https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=667

2. **Título:** Instrução Normativa BCB n° 666, 22/9/2025
   Data/Hora Documento: 22/9/2025 20:30
   Assunto: Disciplina a dispensa da observância do limite de emissão de Transferência Eletrônica Disponível – TED de valor igual ou superior a R$15.000,00 (quinze mil reais) por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.
   Responsável: DEGEF
   https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=666

3. **Título:** Instrução Normativa BCB n° 664, 11/9/2025
   Data/Hora Documento: 11/9/2025 21:15
   Assunto: Estabelece prazos para o Provedor de Serviços de Tecnologia da Informação – PSTI, em funcionamento na data da entrada em vigor da Resolução BCB nº 498, de 5 de setembro de 2025, promover as adaptações necessárias com vistas a sua adequação às regras sobre política de segurança da informação e sobre política de gestão de fraudes estabelecidas na referida Resolução.
   Responsável: DEINF
   https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=664

4. **Título:** Resolução BCB n° 498, 5/9/2025
   Data/Hora Documento: 5/9/2025 18:05
   Assunto: Disciplina, no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI e dá outras providências.
   Responsável: DINOR, DIRAD, DIFIS, DIORF
   https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=498

5. **Título:** Resolução CMN n° 5.228, 1/7/2025

Data/Hora Documento: 1/7/2025 12:29
Assunto: Ajusta normas do Capítulo 11 (Programas de Investimento Agropecuário – InvestAgro) do Manual de Crédito Rural – MCR.
Responsável: MF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5228

6. **Título:** Instrução Normativa BCB n° 637, 13/6/2025
Data/Hora Documento: 13/6/2025 14:53
Assunto: Divulga a versão 8.0 do Manual de Experiência do Cliente no Open Finance.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=637

7. **Título:** Instrução Normativa BCB n° 636, 10/6/2025
Data/Hora Documento: 10/6/2025 11:36
Assunto: Altera o leiaute das informações de que trata a Circular n° 3.290, de 5 de setembro de 2005.
Responsável: DEATI
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=636

8. **Título:** Resolução BCB n° 478, 30/5/2025
Data/Hora Documento: 30/5/2025 09:04
Assunto: Dispõe sobre o escopo e a metodologia de apuração da Razão de Alavancagem – RA, introduz requerimento mínimo de RA para instituição do Tipo 3 e implementa condições para a exclusão de exposições entre integrantes de um mesmo sistema cooperativo.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=478

9. **Título:** Instrução Normativa BCB n° 627, 29/5/2025
Data/Hora Documento: 29/5/2025 12:38
Assunto: Altera o Leiaute, as Instruções de Preenchimento, e as Instruções complementares relativas a informações de operações de crédito voltadas a programas governamentais relativos ao documento 3040 - Dados de Risco de Crédito, do Sistema de Informações de Créditos (SCR), de que tratam a Circular nº 3.870, de 19 de dezembro de 2017, e a Carta Circular nº 3.869, de 19 de março de 2018.
Responsável: DESIG
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=627

10. **Título:** Instrução Normativa BCB n° 588, 31/1/2025
Data/Hora Documento: 31/1/2025 16:57
Assunto: Divulga a versão 4.0 do Manual de Serviços Prestados pela Estrutura de Governança do Open Finance.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=588

11. **Título:** Instrução Normativa BCB n° 587, 31/1/2025
Data/Hora Documento: 31/1/2025 16:32
Assunto: Divulga a versão 6.0 do Manual de Escopo de Dados e Serviços do Open Finance.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=587

12. **Título:** Resolução BCB n° 454, 30/1/2025
Data/Hora Documento: 30/1/2025 18:01
Assunto: Dispõe sobre a Estratégia de Uso de Software e de Serviços de Computação em Nuvem do

Banco Central do Brasil.
Responsável: DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=454

13. **Título:** Instrução Normativa BCB n° 575, 20/12/2024
Data/Hora Documento: 20/12/2024 16:41
Assunto: Divulga a versão 2.0 do Manual de Monitoramento do Open Finance.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=575

14. **Título:** Resolução BCB n° 447, 19/12/2024
Data/Hora Documento: 19/12/2024 18:05
Assunto: Altera as Circulares ns. 3.634, 3.635, 3.636, 3.637, 3.638, 3.639 e 3.641, de 4 de março de 2013, 3.809, de 25 de agosto de 2016, 3.846, de 13 de setembro de 2017, 3.861 e 3.863, de 7 de dezembro de 2017, 3.876, de 31 de janeiro de 2018, e 3.979, de 30 de janeiro de 2020, e as Resoluções BCB ns. 54, de 16 de dezembro de 2020, 111, de 6 de julho de 2021, 139, de 15 de setembro de 2021, 199, 200, 201 e 202, de 11 de março de 2022, 229, de 12 de maio de 2022, 265, de 25 de novembro de 2022, 291, de 8 de fevereiro de 2023, 303, de 16 de março de 2023, 307, de 23 de março de 2023, 313, de 26 de abril de 2023, 319, de 18 de maio de 2023, 331, de 27 de junho de 2023, e 356, de 28 de novembro de 2023, para incluir em seus escopos de aplicação as sociedades corretoras de títulos e valores mobiliários, as sociedades distribuidoras de títulos e valores mobiliários e as sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=447

15. **Título:** Resolução CMN n° 5.193, 19/12/2024
Data/Hora Documento: 19/12/2024 18:02
Assunto: Altera normas da Seção 9 (Impedimentos Sociais, Ambientais e Climáticos) do Capítulo 2 (Condições Básicas) do Manual de Crédito Rural – MCR.
Responsável: MF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5193

16. **Título:** Instrução Normativa BCB n° 531, 18/10/2024
Data/Hora Documento: 18/10/2024 13:34
Assunto: Altera o Leiaute e as Instruções de Preenchimento do documento 3040 – Dados de Risco de Crédito, do Sistema de Informações de Créditos – SCR, de que tratam a Circular nº 3.870, de 19 de dezembro de 2017, e a Carta Circular nº 3.869, de 19 de março de 2018.
Responsável: DESIG
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=531

17. **Título:** Resolução BCB n° 427, 16/10/2024
Data/Hora Documento: 16/10/2024 18:02
Assunto: Divulga o Regimento Interno do Conselho de Controle de Atividades Financeiras – Coaf.
Responsável: PRESI, DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=427

18. **Título:** Resolução CMN n° 5.166, 22/8/2024
Data/Hora Documento: 22/8/2024 18:03
Assunto: Dispõe sobre as condições de emissão de Certificado de Operações Estruturadas – COE pelas instituições financeiras que especifica.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%2

0CMN&numero=5166

19. **Título:** Instrução Normativa BCB n° 495, 26/7/2024
Data/Hora Documento: 26/7/2024 19:53
Assunto: Altera a Instrução Normativa BCB nº 428, de 1º de dezembro de 2023, que define as rubricas contábeis do grupo Compensação Ativa do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=495

20. **Título:** Instrução Normativa BCB n° 494, 26/7/2024
Data/Hora Documento: 26/7/2024 19:45
Assunto: Altera a Instrução Normativa BCB nº 427, de 1º de dezembro de 2023, que define as rubricas contábeis do grupo Ativo Permanente do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=494

21. **Título:** Instrução Normativa BCB n° 493, 26/7/2024
Data/Hora Documento: 26/7/2024 19:37
Assunto: Altera a Instrução Normativa BCB nº 426, de 1º de dezembro de 2023, que define as rubricas contábeis do grupo Ativo Realizável do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=493

22. **Título:** Instrução Normativa BCB n° 491, 23/7/2024
Data/Hora Documento: 23/7/2024 10:13
Assunto: Estabelece as diretrizes para cadastramento de dispositivo de acesso para a iniciação de transações Pix e para o gerenciamento de chaves Pix e define o valor máximo permitido para iniciar transações Pix em dispositivo de acesso não cadastrado.
Responsável: DECEM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=491

23. **Título:** Resolução BCB n° 400, 4/7/2024
Data/Hora Documento: 4/7/2024 10:32
Assunto: Dispõe sobre as diretrizes para o estabelecimento da Estrutura de Governança do Open Finance.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=400

24. **Título:** Resolução CMN n° 5.152, 3/7/2024
Data/Hora Documento: 3/7/2024 09:03
Assunto: Ajusta normas na Seção 2 (Créditos de Custeio) do Capítulo 3 (Operações) do Manual de Crédito Rural – MCR.
Responsável: MF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5152

25. **Título:** Resolução BCB n° 396, 27/6/2024
Data/Hora Documento: 27/6/2024 18:01

Assunto: Divulga alterações no Regimento Interno do Banco Central do Brasil.
Responsável: PRESI, DIRAD, DIFIS, DIORF, DIPEC, DIPOM, DINOR, DIREC
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=396

26. **Título:** Resolução BCB n° 395, 26/6/2024
Data/Hora Documento: 26/6/2024 18:36
Assunto: Altera as Resoluções BCB ns. 319, de 18 de maio de 2023, 313, de 26 de abril de 2023, e 229, de 12 de maio de 2022, para manter a harmonia com a apuração da parcela dos ativos ponderados pelo risco - RWA relativa às exposições ao risco de crédito dos instrumentos financeiros classificados na carteira de negociação - RWADRC.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=395

27. **Título:** Instrução Normativa BCB n° 480, 13/6/2024
Data/Hora Documento: 13/6/2024 19:40
Assunto: Estabelece procedimentos referentes ao Programa de Gestão e Desempenho - PGD do Banco Central do Brasil.
Responsável: DEPES
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=480

28. **Título:** Resolução BCB n° 386, 5/6/2024
Data/Hora Documento: 5/6/2024 18:03
Assunto: Divulga a Política de Conformidade (Compliance) do Banco Central do Brasil – PCO-BCB.
Responsável: DIREX
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=386

29. **Título:** Instrução Normativa BCB n° 471, 22/5/2024
Data/Hora Documento: 22/5/2024 11:50
Assunto: Estabelece os procedimentos para inscrição e os critérios a serem observados na classificação dos interessados inscritos no Cadastro de Responsáveis por Regimes de Resolução (Caresp) para formação de lista a ser encaminhada à autoridade competente.
Responsável: DERAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=471

30. **Título:** Resolução CMN n° 5.130, 25/4/2024
Data/Hora Documento: 25/4/2024 18:01
Assunto: Dispõe sobre os financiamentos ao amparo da Linha de Mobilização de Capital Privado Externo e Proteção Cambial – Linha Eco Invest Brasil –, no âmbito do Fundo Nacional sobre Mudança do Clima (FNMC).
Responsável: MF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5130

31. **Título:** Resolução BCB n° 368, 25/1/2024
Data/Hora Documento: 25/1/2024 18:02
Assunto: Altera as Resoluções BCB ns. 28, de 23 de outubro de 2020; 65, de 26 de janeiro de 2021; 85, de 8 de abril de 2021; 93, de 6 de maio de 2021; 155, de 14 de outubro de 2021; e 260, de 22 de novembro de 2022, para incluir em seus escopos de aplicação as sociedades corretoras de títulos e valores mobiliários, as sociedades distribuidoras de títulos e valores mobiliários e as sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=368

32. **Título:** Resolução BCB n° 366, 17/1/2024
Data/Hora Documento: 17/1/2024 18:00
Assunto: Divulga o Regulamento do Sistema de Informações Banco Central (Sisbacen).
Responsável: DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=366

33. **Título:** Instrução Normativa BCB n° 438, 14/12/2023
Data/Hora Documento: 14/12/2023 16:06
Assunto: Altera a Instrução Normativa BCB nº 236, de 17 de fevereiro de 2022, que altera e consolida os procedimentos para a remessa de demonstrações financeiras individuais e consolidadas, anuais, semestrais e intermediárias, para fins de divulgação na Central de Demonstrações Financeiras do Sistema Financeiro Nacional (CDSFN), de que trata a Resolução BCB nº 2, de 12 de agosto de 2020.
Responsável: DESIG
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=438

34. **Título:** Instrução Normativa BCB n° 433, 1/12/2023
Data/Hora Documento: 1/12/2023 21:22
Assunto: Define as rubricas contábeis do grupo Compensação Passiva do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=433

35. **Título:** Instrução Normativa BCB n° 432, 1/12/2023
Data/Hora Documento: 1/12/2023 21:06
Assunto: Define as rubricas contábeis do grupo Resultado Devedor do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=432

36. **Título:** Instrução Normativa BCB n° 431, 1/12/2023
Data/Hora Documento: 1/12/2023 20:43
Assunto: Define as rubricas contábeis do grupo Resultado Credor do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=431

37. **Título:** Instrução Normativa BCB n° 430, 1/12/2023
Data/Hora Documento: 1/12/2023 20:35
Assunto: Define as rubricas contábeis do grupo Patrimônio Líquido do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=430

38. **Título:** Instrução Normativa BCB n° 429, 1/12/2023
Data/Hora Documento: 1/12/2023 20:28
Assunto: Define as rubricas contábeis do grupo Passivo Exigível do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=429

39. **Título:** Instrução Normativa BCB n° 428, 1/12/2023
Data/Hora Documento: 1/12/2023 20:13
Assunto: Define as rubricas contábeis do grupo Compensação Ativa do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=428

40. **Título:** Instrução Normativa BCB n° 427, 1/12/2023
Data/Hora Documento: 1/12/2023 19:59
Assunto: Define as rubricas contábeis do grupo Ativo Permanente do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=427

41. **Título:** Instrução Normativa BCB n° 426, 1/12/2023
Data/Hora Documento: 1/12/2023 19:06
Assunto: Define as rubricas contábeis do grupo Ativo Realizável do elenco de contas do Padrão Contábil das Instituições Reguladas pelo Banco Central do Brasil (Cosif) para utilização pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=426

42. **Título:** Resolução BCB n° 352, 23/11/2023
Data/Hora Documento: 23/11/2023 18:00
Assunto: Dispõe sobre os conceitos e os critérios contábeis aplicáveis a instrumentos financeiros, bem como para a designação e o reconhecimento das relações de proteção (contabilidade de hedge) pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários, pelas sociedades corretoras de câmbio, pelas administradoras de consórcio e pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil e sobre os procedimentos contábeis para a definição de fluxos de caixas de ativo financeiro como somente pagamento de principal e juros, a aplicação da metodologia para apuração da taxa de juros efetiva de instrumentos financeiros, a constituição de provisão para perdas associadas ao risco de crédito e a evidenciação de informações relativas a instrumentos financeiros em notas explicativas a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=352

43. **Título:** Resolução BCB n° 347, 17/10/2023
Data/Hora Documento: 17/10/2023 18:00
Assunto: Divulga a Política de Auditoria Interna do Banco Central do Brasil.
Responsável: PRESI
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=347

44. **Título:** Instrução Normativa BCB n° 414, 16/10/2023
Data/Hora Documento: 16/10/2023 09:56
Assunto: Altera o Leiaute e as Instruções de Preenchimento do documento 3040 - Dados de Risco de Crédito, do Sistema de Informações de Créditos (SCR), de que tratam a Circular nº 3.870, de 19 de

dezembro de 2017, e a Carta Circular nº 3.869, de 19 de março de 2018.
Responsável: DESIG
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=414

45. **Título:** Resolução CMN n° 5.105, 28/9/2023
Data/Hora Documento: 28/9/2023 18:01
Assunto: Estabelece diretrizes mínimas para a disciplina das condições de constituição e de funcionamento, para a autorização para constituição e funcionamento e para a supervisão das atividades das sociedades corretoras de títulos e valores mobiliários, das sociedades corretoras de câmbio e das sociedades distribuidoras de títulos e valores mobiliários.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5105

46. **Título:** Resolução BCB n° 340, 21/9/2023
Data/Hora Documento: 21/9/2023 18:00
Assunto: Divulga o novo Regimento Interno do Banco Central do Brasil.
Responsável: DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=340

47. **Título:** Resolução BCB n° 331, 27/6/2023
Data/Hora Documento: 27/6/2023 18:01
Assunto: Dispõe sobre a Política de Responsabilidade Social, Ambiental e Climática (PRSAC) a ser estabelecida por conglomerado prudencial classificado como Tipo 3 e sobre as ações com vistas à sua efetividade.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=331

48. **Título:** Resolução Conjunta n° 6, 23/5/2023
Data/Hora Documento: 23/5/2023 09:30
Assunto: Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=6

49. **Título:** Resolução BCB n° 319, 18/5/2023
Data/Hora Documento: 18/5/2023 18:05
Assunto: Estabelece limites máximos de exposição por cliente e limite máximo de exposições concentradas, e altera as Resoluções BCB ns. 201, de 11 de março de 2022, e 265, de 25 de novembro de 2022.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=319

50. **Título:** Resolução CMN n° 5.077, 18/5/2023
Data/Hora Documento: 18/5/2023 18:04
Assunto: Altera as Resoluções ns. 4.557, de 23 de fevereiro de 2017, 4.606, de 19 de outubro de 2017, e 4.677, de 31 de julho de 2018.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5077

51. **Título:** Resolução CMN n° 5.076, 18/5/2023
Data/Hora Documento: 18/5/2023 18:03

Assunto: Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, e a Resolução nº 4.606, de 19 de outubro de 2017.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5076

52. **Título:** Resolução BCB n° 315, 27/4/2023
Data/Hora Documento: 27/4/2023 09:00
Assunto: Institui o Comitê Executivo de Gestão (CEG) do Projeto-Piloto da Plataforma do Real Digital (Piloto RD) e aprova o Regulamento do Piloto RD.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=315

53. **Título:** Resolução BCB n° 313, 26/4/2023
Data/Hora Documento: 26/4/2023 18:21
Assunto: Estabelece os procedimentos para o cálculo diário, mediante abordagem padronizada, da parcela dos ativos ponderados pelo risco (RWA) relativa ao cálculo do capital requerido para as exposições ao risco de crédito dos instrumentos financeiros classificados na carteira de negociação (RWADRC), de que tratam a Resolução CMN nº 4.958, de 21 de outubro de 2021, e a Resolução BCB nº 200, de 11 de março de 2022.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=313

54. **Título:** Resolução CMN n° 5.071, 26/4/2023
Data/Hora Documento: 26/4/2023 18:19
Assunto: Dispõe sobre o cheque, as consequências de seu uso indevido e as condições para seu fornecimento ao cliente pelas instituições financeiras.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5071

55. **Título:** Instrução Normativa BCB n° 374, 26/4/2023
Data/Hora Documento: 26/4/2023 10:14
Assunto: Divulga procedimentos, prazos, documentos e informações necessários para a instrução de pedidos de autorização relacionados ao funcionamento dos Sistemas de Mercado Financeiro (SMF) no âmbito do Sistema de Pagamentos Brasileiro (SPB), e os tipos de alterações nos SMF e em seus regulamentos que representam risco relevante à sua segurança, à sua eficiência ou à solidez e ao normal funcionamento do SPB ou do Sistema Financeiro Nacional (SFN).
Responsável: DEORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=374

56. **Título:** Resolução CMN n° 5.070, 20/4/2023
Data/Hora Documento: 20/4/2023 18:02
Assunto: Dispõe sobre a realização de operações de derivativos de crédito no País por instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5070

57. **Título:** Resolução BCB n° 306, 23/3/2023
Data/Hora Documento: 23/3/2023 18:00
Assunto: Altera circulares e resoluções BCB que dispõem sobre o Processo Interno de Avaliação da Adequação de Capital (Icaap) e o Processo Interno Simplificado de Avaliação da Adequação de Capital (IcaapSimp), sobre a base de dados de risco operacional, sobre a divulgação do Relatório de Pilar 3, sobre o Relatório de Riscos e Oportunidades Sociais, Ambientais e Climáticas (Relatório GRSAC), sobre critérios para a classificação de instrumentos na carteira de negociação ou na carteira

bancária, sobre os requisitos de governança relativos às mesas de operações em que são gerenciados os instrumentos sujeitos ao risco de mercado, sobre as exigências para o reconhecimento de transferências internas de risco e sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de conglomerado prudencial classificado como Tipo 3.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=306

58. **Título:** Resolução BCB n° 304, 20/3/2023
Data/Hora Documento: 20/3/2023 14:01
Assunto: Aprova o Regulamento que disciplina, no âmbito do Sistema de Pagamentos Brasileiro, o funcionamento dos sistemas de liquidação, o exercício das atividades de registro e de depósito centralizado de ativos financeiros e a constituição de ônus e gravames sobre ativos financeiros registrados ou depositados, e consolida normas sobre a matéria.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=304

59. **Título:** Resolução BCB n° 287, 24/1/2023
Data/Hora Documento: 24/1/2023 18:01
Assunto: Divulga a Política de Segurança da Informação do Banco Central do Brasil (PSIBC).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=287

60. **Título:** Resolução BCB n° 286, 24/1/2023
Data/Hora Documento: 24/1/2023 18:00
Assunto: Institui o Regulamento de Governança do Portal de Internet do Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=286

61. **Título:** Resolução BCB n° 265, 25/11/2022
Data/Hora Documento: 25/11/2022 14:14
Assunto: Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de conglomerado prudencial classificado como Tipo 3 enquadrado no Segmento 2 (S2), Segmento 3 (S3) ou Segmento 4 (S4).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=265

62. **Título:** Resolução BCB n° 250, 5/10/2022
Data/Hora Documento: 5/10/2022 18:11
Assunto: Divulga o novo Regulamento do Comitê de Governança da Informação (CGI).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=250

63. **Título:** Resolução BCB n° 249, 5/10/2022
Data/Hora Documento: 5/10/2022 18:10
Assunto: Divulga a Política de Governança da Informação do Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=249

64. **Título:** Instrução Normativa BCB n° 305, 15/9/2022
Data/Hora Documento: 15/9/2022 19:08
Assunto: Divulga a versão 4.0 do Manual de Segurança do Open Finance.

Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=305

65. **Título:** Resolução CMN n° 5.021, 29/6/2022
Data/Hora Documento: 29/6/2022 18:00
Assunto: Ajusta normas gerais do crédito rural e de financiamentos ao amparo do Fundo de Defesa da Economia Cafeeira (Funcafé) a serem aplicadas a partir de 1º de julho de 2022.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5021

66. **Título:** Resolução BCB n° 229, 12/5/2022
Data/Hora Documento: 12/5/2022 18:00
Assunto: Estabelece os procedimentos para o cálculo da parcela dos ativos ponderados pelo risco (RWA) referente às exposições ao risco de crédito sujeitas ao cálculo do requerimento de capital mediante abordagem padronizada (RWACPAD), de que tratam a Resolução CMN nº 4.958, de 21 de outubro de 2021, e a Resolução BCB nº 200, de 11 de março de 2022
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=229

67. **Título:** Resolução CMN n° 5.001, 24/3/2022
Data/Hora Documento: 24/3/2022 18:20
Assunto: Dispõe sobre a emissão de Letras Imobiliárias Garantidas pelas instituições financeiras que específica.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5001https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5001

68. **Título:** Resolução BCB n° 204, 22/3/2022
Data/Hora Documento: 22/3/2022 10:30
Assunto: Dispõe sobre o compartilhamento de dados de operações registradas no Sistema de Operações do Crédito Rural e do Proagro (Sicor).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=204

69. **Título:** Resolução BCB n° 201, 11/3/2022
Data/Hora Documento: 11/3/2022 07:33
Assunto: Dispõe sobre a metodologia facultativa simplificada para apuração do requerimento mínimo de Patrimônio de Referência Simplificado (PRS5) para os conglomerados prudenciais classificados como do Tipo 3, sobre os requisitos para opção por essa metodologia e sobre a estrutura simplificada de gerenciamento contínuo de riscos.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=201

70. **Título:** Resolução BCB n° 198, 11/3/2022
Data/Hora Documento: 11/3/2022 07:31
Assunto: Dispõe sobre o requerimento mínimo de Patrimônio de Referência de Instituição de Pagamento (PRIP) de conglomerado do Tipo 2, nos termos da Resolução BCB nº 197, de 11 de março de 2022, e de instituição de pagamento não integrante de conglomerado prudencial, e sobre a metodologia de apuração desses requerimentos e a respectiva estrutura de gerenciamento contínuo de riscos.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=198

71. **Título:** Resolução CMN n° 4.966, 25/11/2021
Data/Hora Documento: 25/11/2021 18:32
Assunto: Dispõe sobre os conceitos e os critérios contábeis aplicáveis a instrumentos financeiros, bem como para a designação e o reconhecimento das relações de proteção (contabilidade de hedge) pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4966

72. **Título:** Resolução BCB n° 150, 6/10/2021
Data/Hora Documento: 6/10/2021 18:17
Assunto: Consolida normas sobre os arranjos de pagamento, aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=150

73. **Título:** Resolução BCB n° 139, 15/9/2021
Data/Hora Documento: 15/9/2021 09:31
Assunto: Dispõe sobre a divulgação do Relatório de Riscos e Oportunidades Sociais, Ambientais e Climáticas (Relatório GRSAC).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=139

74. **Título:** Resolução BCB n° 130, 20/8/2021
Data/Hora Documento: 20/8/2021 08:00
Assunto: Dispõe sobre a prestação de serviços de auditoria independente para as administradoras de consórcio e as instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil e estabelece os procedimentos específicos para elaboração dos relatórios resultantes do trabalho de auditoria independente realizado nas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=130

75. **Título:** Resolução CMN n° 4.935, 29/7/2021
Data/Hora Documento: 29/7/2021 18:05
Assunto: Dispõe sobre a contratação de correspondentes no País pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4935

76. **Título:** Resolução CMN n° 4.933, 29/7/2021
Data/Hora Documento: 29/7/2021 18:04
Assunto: Aprova o Estatuto e o Regulamento do Fundo Garantidor do Cooperativismo de Crédito (FGCoop) e estabelece a forma de contribuição.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4933

77. **Título:** Resolução BCB n° 111, 6/7/2021
Data/Hora Documento: 6/7/2021 18:01
Assunto: Dispõe sobre os critérios para a classificação de instrumentos na carteira de negociação ou na carteira bancária, sobre os requisitos de governança relativos às mesas de operações em que são

gerenciados os instrumentos sujeitos ao risco de mercado, sobre as exigências para o reconhecimento de transferências internas de risco na apuração dos requerimentos mínimos de que trata a Resolução nº 4.193, de 1º de março de 2013, e revoga a Circular nº 3.354, de 27 de junho de 2007.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=111

78. **Título:** Resolução CMN n° 4.910, 27/5/2021
Data/Hora Documento: 27/5/2021 18:01
Assunto: Dispõe sobre a prestação de serviços de auditoria independente para as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4910

79. **Título:** Resolução BCB n° 96, 19/5/2021
Data/Hora Documento: 19/5/2021 18:00
Assunto: Dispõe sobre a abertura, a manutenção e o encerramento de contas de pagamento.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=96

80. **Título:** Resolução BCB n° 85, 8/4/2021
Data/Hora Documento: 8/4/2021 18:00
Assunto: 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 de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85

81. **Título:** Resolução CMN n° 4.902, 25/3/2021
Data/Hora Documento: 25/3/2021 18:04
Assunto: Dispõe sobre a consolidação dos dispositivos atualmente inseridos no Capítulo 16 do Manual de Crédito Rural (MCR), acerca do Programa de Garantia da Atividade Agropecuária (Proagro).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4902https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4902

82. **Título:** Resolução CMN n° 4.900, 25/3/2021
Data/Hora Documento: 25/3/2021 18:02
Assunto: Dispõe sobre a consolidação dos dispositivos atualmente inseridos nos Capítulos 4, 5, 7 e 12 do Manual de Crédito Rural (MCR), acerca de finalidades e instrumentos especiais da política agrícola.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4900

83. **Título:** Resolução BCB n° 77, 3/3/2021
Data/Hora Documento: 3/3/2021 18:00
Assunto: Institui o Comitê Estratégico de Gestão do Sandbox Regulatório (CESB) e divulga seu Regulamento.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=77

84. **Título:** Resolução CMN n° 4.893, 26/2/2021
Data/Hora Documento: 26/2/2021 14:06
Assunto: 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 autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893

85. **Título:** Resolução CMN n° 4.889, 26/2/2021
Data/Hora Documento: 26/2/2021 14:03
Assunto: Dispõe sobre a consolidação do Capítulo 8 (Programa Nacional de Apoio ao Médio Produtor Rural - Pronamp), do Capítulo 9 (Fundo de Defesa da Economia Cafeeira - Funcafé), do Capítulo 10 (Programa Nacional de Fortalecimento da Agricultura Familiar - Pronaf) e do Capítulo 11 (Programas com Recursos do BNDES) do Manual de Crédito Rural (MCR), em conformidade com o disposto no art. 5º do Decreto nº 10.139, de 28 de novembro de 2019.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4889

86. **Título:** Resolução BCB n° 70, 11/2/2021
Data/Hora Documento: 11/2/2021 17:09
Assunto: Institui a Política de Gestão Integrada de Riscos do Banco Central do Brasil (PGR-BCB).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=70

87. **Título:** Resolução CMN n° 4.883, 23/12/2020
Data/Hora Documento: 23/12/2020 17:17
Assunto: Dispõe sobre a consolidação dos dispositivos inseridos nos Capítulos 1, 2 e 3 do Manual de Crédito Rural (MCR), acerca de princípios, conceitos básicos e operação aplicáveis ao crédito rural.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4883

88. **Título:** Resolução BCB n° 47, 24/11/2020
Data/Hora Documento: 24/11/2020 21:06
Assunto: Dispõe sobre a concessão da jornada de trabalho remoto instituída de maneira excepcional e temporária por meio da Portaria nº 107.218, de 17 de março de 2020, e disciplina o retorno gradual das atividades presenciais para os servidores das carreiras do Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=47

89. **Título:** Resolução BCB n° 29, 26/10/2020
Data/Hora Documento: 26/10/2020 14:01
Assunto: Estabelece as diretrizes para funcionamento do Ambiente Controlado de Testes para Inovações Financeiras e de Pagamento (Sandbox Regulatório) e as condições para o fornecimento de produtos e serviços no contexto desse ambiente no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=29

90. **Título:** Resolução CMN n° 4.865, 26/10/2020
Data/Hora Documento: 26/10/2020 14:00
Assunto: Estabelece as diretrizes para funcionamento do Ambiente Controlado de Testes para Inovações Financeiras e de Pagamento (Sandbox Regulatório) e as condições para o fornecimento de produtos e serviços no contexto desse ambiente no âmbito do Sistema Financeiro Nacional.

Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4865

91. **Título:** Instrução Normativa BCB n° 6, 20/8/2020
Data/Hora Documento: 20/8/2020 15:03
Assunto: Altera a Carta Circular nº 4.056, de 25 de maio de 2020, que estabelece os procedimentos necessários para a adesão ao PIX, desde o seu lançamento.
Responsável: DECEM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=6

92. **Título:** Carta Circular n° 4.070, 16/7/2020
Data/Hora Documento: 16/7/2020 15:40
Assunto: Altera a Carta Circular nº 4.056, de 25 de maio de 2020, que estabelece os procedimentos necessários para a adesão ao arranjo de pagamentos instantâneos (PIX), desde o seu lançamento.
Responsável: DECEM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Carta%20Circular&numero=4070

93. **Título:** Resolução Conjunta n° 1, 4/5/2020
Data/Hora Documento: 4/5/2020 12:00
Assunto: Dispõe sobre a implementação do Open Finance.
Responsável:
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=1

94. **Título:** Circular n° 3.970, 28/11/2019
Data/Hora Documento: 28/11/2019 18:00
Assunto: Estabelece os critérios gerais de comunicação eletrônica de dados no âmbito do Sistema Financeiro Nacional (SFN), dispõe sobre os requisitos e as vedações aplicáveis ao Provedor de Serviços de Tecnologia da Informação (PSTI) e dá outras providências.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3970

95. **Título:** Resolução CMN n° 4.753, 26/9/2019
Data/Hora Documento: 26/9/2019 18:01
Assunto: Dispõe sobre a abertura, a manutenção e o encerramento de conta de depósitos.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4753

96. **Título:** Comunicado n° 34.005, 14/8/2019
Data/Hora Documento: 14/8/2019 18:01
Assunto: Divulga atuação do Banco Central do Brasil no mercado de câmbio por meio de oferta simultânea de dólar à vista e de contratos de swap (swap reverso).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=34005

97. **Título**: Comunicado n° 33.455, 24/4/2019
Data/Hora Documento: 24/4/2019 18:30
Assunto: Divulga os requisitos fundamentais para a implementação, no Brasil, do Sistema Financeiro Aberto (Open Banking).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33455

98. **Título:** Circular n° 3.909, 16/8/2018
Data/Hora Documento: 16/8/2018 18:00
Assunto: 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 de pagamento autorizadas a funcionar pelo Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3909

99. **Título:** Resolução CMN n° 4.677, 31/7/2018
Data/Hora Documento: 31/7/2018 18:01
Assunto: Estabelece limites máximos de exposição por cliente e limite máximo de exposições concentradas.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4677

100. **Título:** Resolução CMN n° 4.606, 19/10/2017
Data/Hora Documento: 19/10/2017 18:12
Assunto: Dispõe sobre a metodologia facultativa simplificada para apuração do requerimento mínimo de Patrimônio de Referência Simplificado (PRS5), os requisitos para opção por essa metodologia e os requisitos adicionais para a estrutura simplificada de gerenciamento contínuo de riscos.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4606

101. **Título:** Resolução CMN n° 4.557, 23/2/2017
Data/Hora Documento: 23/2/2017 18:33
Assunto: Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4557

102. **Título:** Carta Circular n° 3.802, 25/1/2017
Data/Hora Documento: 25/1/2017 16:06
Assunto: Divulga esclarecimentos relativos às medidas que devem ser adotadas por instituidores de arranjos de pagamento em funcionamento relacionadas à abertura de participação nos respectivos arranjos de pagamento, nos termos da Circular nº 3.682, de 4 de novembro de 2013, com a redação dada pela Circular nº 3.815, de 7 de dezembro de 2016.
Responsável: DEBAN
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Carta%20Circular&numero=3802

103. **Título:** Circular n° 3.809, 25/8/2016
Data/Hora Documento: 25/8/2016 16:00
Assunto: Estabelece os procedimentos para o reconhecimento de instrumentos mitigadores no cálculo da parcela dos ativos ponderados pelo risco (RWA) referente às exposições ao risco de crédito sujeitas ao cálculo do requerimento de capital mediante abordagem padronizada (RWAcpad), de que trata a Resolução nº 4.193, de 1º de março de 2013.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3809

104. **Título:** Resolução CMN n° 4.474, 31/3/2016
Data/Hora Documento: 31/3/2016 18:45
Assunto: Dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil, bem como sobre o procedimento de descarte das matrizes físicas dos documentos digitalizados e armazenados eletronicamente.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4474

105. **Título:** Resolução CMN n° 4.282, 4/11/2013
Data/Hora Documento: 4/11/2013 00:00
Assunto: Estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), de que trata a Lei nº 12.865, de 9 de outubro de 2013.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4282

106. **Título:** Resolução CMN n° 4.222, 23/5/2013
Data/Hora Documento: 23/5/2013 00:00
Assunto: Altera e consolida as normas que dispõem sobre o estatuto e o regulamento do Fundo Garantidor de Créditos (FGC).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4222

107. **Título:** Circular n° 3.641, 4/3/2013
Data/Hora Documento: 4/3/2013 00:00
Assunto: Estabelece os procedimentos para o cálculo da parcela dos ativos ponderados pelo risco (RWA) referente às exposições em ouro, em moeda estrangeira e em ativos sujeitos à variação cambial cujo requerimento de capital é calculado mediante abordagem padronizada (RWAcam), de que trata a Resolução nº 4.193, de 1º de março de 2013.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3641

108. **Título:** Resolução CMN n° 4.021, 29/9/2011
Data/Hora Documento: 29/9/2011 00:00
Assunto: Disciplina a cobrança de tarifas pela prestação de serviços vinculados a operações de câmbio manual para compra ou venda de moeda estrangeira relacionada a viagens internacionais e institui a obrigatoriedade de informação do Valor Efetivo Total (VET) nas operações da espécie.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4021

109. **Título:** Resolução CMN n° 3.919, 25/11/2010
Data/Hora Documento: 25/11/2010 00:00
Assunto: Altera e consolida as normas sobre cobrança de tarifas pela prestação de serviços por parte das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil e dá outras providências.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=3919

110. **Título:** Resolução CMN n° 3.814, 26/11/2009
Data/Hora Documento: 26/11/2009 00:00
Assunto: Condiciona o crédito agroindustrial para expansão da produção e industrialização da cana-de-açúcar ao Zoneamento Agroecológico e veda o financiamento da expansão do plantio nos Biomas Amazônia e Pantanal e Bacia do Alto Paraguai, entre outras áreas.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=3814

111. **Título:** Resolução CMN n° 3.712, 16/4/2009
Data/Hora Documento: 16/4/2009 00:00
Assunto: Altera os prazos para renegociação das operações de crédito rural, no âmbito da Lei nº 11.775, de 17 de setembro de 2008.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&n

umero=3712

112. **Título:** Resolução CMN n° 3.578, 29/5/2008
Data/Hora Documento: 29/5/2008 00:00
Assunto: Estabelece prazos e disposições complementares para a efetivação do contido nos arts. 15, 16, 17 e 18 da Medida Provisória n° 432, de 27 de maio de 2008.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=3578

113. **Título:** Resolução CMN n° 3.575, 29/5/2008
Data/Hora Documento: 29/5/2008 00:00
Assunto: Estabelece prazos e disposições complementares para a efetivação do contido nos arts. 10 e 11 da Medida Provisória nº 432, de 27 de maio de 2008.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=3575

114. **Título:** Resolução CMN n° 3.474, 3/7/2007
Data/Hora Documento: 3/7/2007 00:00
Assunto: Altera programas de investimento, amparados em recursos equalizados pelo Tesouro Nacional junto ao Banco Nacional de Desenvolvimento Econômico e Social (BNDES).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=3474

115. **Título:** Circular n° 3.106, 10/4/2002
Data/Hora Documento: 10/4/2002 00:00
Assunto: Dispõe sobre a realização de operações de derivativos de crédito de que trata a Resolução 2.933, de 28 de fevereiro de 2002.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3106

116. **Título:** Resolução CMN n° 2.828, 30/3/2001
Data/Hora Documento: 30/3/2001 00:00
Assunto: Dispõe sobre a constituição e o funcionamento de agências de fomento.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=2828

117. **Título:** Resolução CMN n° 2.212, 16/11/1995
Data/Hora Documento: 16/11/1995 00:00
Assunto: Altera dispositivos das Resoluções nºs 2.099, de 17/8/1994, e 2.122, de 30/11/1994.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=2212

118. **Título:** Resolução CMN n° 2.197, 31/8/1995
Data/Hora Documento: 31/8/1995 00:00
Assunto: Autoriza a constituição de entidade privada, sem fins lucrativos, destinada a administrar mecanismo de proteção a titulares de créditos contra instituições financeiras.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=2197

Resultados da busca pelo termo “Segurança digital” com os seguintes filtros:

Tipo de documento: Todos
Conteúdo: Proteção de dados
Período: 01/01/1988 - 01/10/2025
Situação: Em vigor

Total de resultados encontrados na busca no site do BC: 80 resultados

1. Após leitura de cada um dos resultados encontrados, foram destacados em azul os que apresentam trechos relacionados com a temática

Total de resultados compatíveis com a temática trabalhada: 24 resultados

2. Todos que possuem relação com a temática foram baixados em arquivo PDF e organizados em uma pasta para posterior análise

3. **Título:** Instrução Normativa BCB n° 667, 22/9/2025
Data/Hora Documento: 22/9/2025 20:44
Assunto: Disciplina a dispensa da observância do limite de emissão de Pix de valor superior a R$15.000,00 (quinze mil reais) por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.
Responsável: DEGEF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=667

4. **Título:** Instrução Normativa BCB n° 666, 22/9/2025
Data/Hora Documento: 22/9/2025 20:30
Assunto: Disciplina a dispensa da observância do limite de emissão de Transferência Eletrônica Disponível – TED de valor igual ou superior a R$15.000,00 (quinze mil reais) por instituição que se conecta à Rede do Sistema Financeiro Nacional – RSFN por meio de Provedor de Serviços de Tecnologia da Informação – PSTI.
Responsável: DEGEF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=666

5. **Título:** Instrução Normativa BCB n° 664, 11/9/2025
Data/Hora Documento: 11/9/2025 21:15
Assunto: Estabelece prazos para o Provedor de Serviços de Tecnologia da Informação – PSTI, em funcionamento na data da entrada em vigor da Resolução BCB nº 498, de 5 de setembro de 2025, promover as adaptações necessárias com vistas a sua adequação às regras sobre política de segurança da informação e sobre política de gestão de fraudes estabelecidas na referida Resolução.
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=664

6. **Título:** Resolução BCB n° 498, 5/9/2025
Data/Hora Documento: 5/9/2025 18:05
Assunto: Disciplina, no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI e dá outras providências.
Responsável: DINOR, DIRAD, DIFIS, DIORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=498

7. **Título:** Comunicado n° 43.789, 3/9/2025
Data/Hora Documento: 3/9/2025 11:00
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso

exclusivo nas mensagerias dos domínios MES e SPB, nos ambientes de homologação e de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=43789

8. **Título:** Comunicado n° 43.595, 1/8/2025
Data/Hora Documento: 1/8/2025 09:30
Assunto: Divulga, para fins de recebimento de eventuais objeções, nomes de pessoas eleitas ou nomeadas para ocupar cargos de administração em instituições autorizadas a funcionar
Responsável: DEORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=43595

9. **Título:** Instrução Normativa BCB n° 633, 5/6/2025
Data/Hora Documento: 5/6/2025 18:11
Assunto: Divulga a versão 3.7 do Manual de Segurança do Pix, que compõe o Regulamento do Pix.
Responsável: DECEM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=633

10. **Título**: Resolução BCB n° 481, 4/6/2025
Data/Hora Documento: 4/6/2025 18:05
Assunto: Institui o Posto de Controle do Banco Central do Brasil – PCBC, para armazenamento de informações classificadas em grau de sigilo e acesso a essas informações, e aprova o seu regulamento.
Responsável: PRESI
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=481

11. **Título:** Instrução Normativa BCB n° 615, 6/5/2025
Data/Hora Documento: 6/5/2025 12:46
Assunto: Divulga a versão 7.0 do Manual de APIs do Open Finance.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=615

12. **Título:** Resolução BCB n° 462, 9/4/2025
Data/Hora Documento: 9/4/2025 18:03
Assunto: Aprova o regulamento do Comitê de Administração – Coad do Banco Central do Brasil.
Responsável: PRESI, DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=462

13. **Título:** Resolução CMN n° 5.202, 27/3/2025
Data/Hora Documento: 27/3/2025 18:01
Assunto: Altera a Resolução CMN nº 4.994, de 24 de março de 2022, que dispõe sobre as diretrizes de aplicação dos recursos garantidores dos planos administrados pelas entidades fechadas de previdência complementar.
Responsável: MF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5202

14. **Título:** Instrução Normativa BCB n° 597, 26/3/2025
Data/Hora Documento: 26/3/2025 14:21
Assunto: Estabelece o regramento dos ciclos de testes homologatórios a ser observado por instituições autorizadas, ou em processo de autorização, pelo Banco Central do Brasil, para o exercício das atividades de escrituração, registro e depósito centralizado de duplicata escritural.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=597

15. **Título:** Comunicado n° 42.992, 25/3/2025
Data/Hora Documento: 25/3/2025 15:04
Assunto: Divulga intenção de cancelar a autorização para funcionamento da Dank Sociedade de Crédito Direto S.A.
Responsável: DEORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=42992

16. **Título:** Resolução BCB n° 455, 20/2/2025
Data/Hora Documento: 20/2/2025 18:00
Assunto: Divulga a Política de Governança de Produtos de Software do Banco Central do Brasil – PGPS-BC.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=455

17. **Título:** Resolução BCB n° 454, 30/1/2025
Data/Hora Documento: 30/1/2025 18:01
Assunto: Dispõe sobre a Estratégia de Uso de Software e de Serviços de Computação em Nuvem do Banco Central do Brasil.
Responsável: DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=454

18. **Título:** Resolução BCB n° 450, 15/1/2025
Data/Hora Documento: 15/1/2025 18:02
Assunto: Dispõe sobre as atividades essenciais para o cumprimento da missão institucional do Banco Central do Brasil, que devem ser mantidas em funcionamento em caso de paralisação ou greve.
Responsável: PRESI, DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=450

19. **Título:** Instrução Normativa BCB n° 581, 30/12/2024
Data/Hora Documento: 30/12/2024 16:14
Assunto: Altera a Instrução Normativa BCB nº 511, de 30 de agosto de 2024, que estabelece os procedimentos necessários para a adesão ao Pix, para ajustar dispositivos referentes à instituição usuária, ao Pix Automático e a recursos no âmbito dos processos de adesão ao Pix.
Responsável: DECEM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=581

20. **Título:** Comunicado n° 42.334, 29/10/2024
Data/Hora Documento: 29/10/2024 17:17
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, nos ambientes de homologação e de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=42334

21. **Título:** Resolução BCB n° 424, 10/10/2024
Data/Hora Documento: 10/10/2024 18:02
Assunto: Divulga o Regulamento do Comitê de Gestão Estratégica – CGE do Banco Central do Brasil.
Responsável: PRESI
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=424

22. **Título:** Comunicado n° 42.164, 20/9/2024
Data/Hora Documento: 20/9/2024 08:26

Assunto: Divulga, para fins de recebimento de eventuais objeções, nomes de pessoas eleitas ou nomeadas para ocupar cargos de administração em instituições autorizadas a funcionar
Responsável: DEORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=42164

23. **Título:** Instrução Normativa BCB n° 511, 30/8/2024
Data/Hora Documento: 30/8/2024 11:19
Assunto: No âmbito do Pix, estabelece os procedimentos necessários para pleitear: a adesão ao Pix; a alteração na modalidade de participação no Pix; a alteração na forma de acesso ao Diretório de Identificadores de Contas Transacionais (DICT) e de participação no Sistema de Pagamentos Instantâneos (SPI); a alteração de participante responsável, liquidante ou prestador de serviços no DICT; a oferta de produtos e serviços adicionais ou facultativos; e a atualização cadastral das demais informações pertinentes.
Responsável: DECEM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=511

24. **Título:** Resolução BCB n° 405, 1/8/2024
Data/Hora Documento: 1/8/2024 18:04
Assunto: Aprova o regulamento das reuniões da Diretoria Colegiada do Banco Central do Brasil.
Responsável: PRESI
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=405

25. **Título:** Resolução BCB n° 396, 27/6/2024
Data/Hora Documento: 27/6/2024 18:01
Assunto: Divulga alterações no Regimento Interno do Banco Central do Brasil.
Responsável: PRESI, DIRAD, DIFIS, DIORF, DIPEC, DIPOM, DINOR, DIREC
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=396

26. **Título:** Instrução Normativa BCB n° 480, 13/6/2024
Data/Hora Documento: 13/6/2024 19:40
Assunto: Estabelece procedimentos referentes ao Programa de Gestão e Desempenho - PGD do Banco Central do Brasil.
Responsável: DEPES
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=480

27. **Título:** Resolução BCB n° 393, 13/6/2024
Data/Hora Documento: 13/6/2024 18:00
Assunto: Institui o novo Programa de Gestão e Desempenho das atividades desenvolvidas pelos servidores das carreiras do Banco Central do Brasil.
Responsável: PRESI, DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=393

28. **Título:** Comunicado n° 41.722, 10/6/2024
Data/Hora Documento: 10/6/2024 16:27
Assunto: Comunica a ativação dos certificados digitais do Banco Central do Brasil, para uso exclusivo nos ambientes de homologação e de produção do SPI/ICOM, DICT e ARQ, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=41722

29. **Título:** Resolução BCB n° 374, 27/3/2024
Data/Hora Documento: 27/3/2024 08:31
Assunto: Dispõe sobre as Linhas Financeiras de Liquidez (LFL) do Banco Central do Brasil e aprova os regulamentos que disciplinam o seu funcionamento.

Responsável: DIPOM, DIFIS, DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=374

30. **Título:** Comunicado n° 41.191, 30/1/2024
Data/Hora Documento: 30/1/2024 15:26
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, nos ambientes de homologação e de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=41191

31. **Título:** Resolução BCB n° 366, 17/1/2024
Data/Hora Documento: 17/1/2024 18:00
Assunto: Divulga o Regulamento do Sistema de Informações Banco Central (Sisbacen).
Responsável: DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=366

32. **Título:** Resolução BCB n° 340, 21/9/2023
Data/Hora Documento: 21/9/2023 18:00
Assunto: Divulga o novo Regimento Interno do Banco Central do Brasil.
Responsável: DIRAD
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=340

33. **Título:** Resolução BCB n° 338, 23/8/2023
Data/Hora Documento: 23/8/2023 08:30
Assunto: Institui procedimentos para acesso de entes públicos aos dados vinculados às chaves Pix armazenadas no Diretório de Identificadores de Contas Transacionais (DICT) e divulga Regulamento para adesão dos interessados.
Responsável: DIREC, DIORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=338

34. **Título:** Resolução CMN n° 5.076, 18/5/2023
Data/Hora Documento: 18/5/2023 18:03
Assunto: Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, e a Resolução nº 4.606, de 19 de outubro de 2017.
Responsável: DINOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5076

35. **Título:** Instrução Normativa BCB n° 382, 16/5/2023
Data/Hora Documento: 16/5/2023 10:13
Assunto: Altera a Instrução Normativa BCB n° 243, de 16 de março de 2022, que divulga procedimentos a serem observados para participação direta no Sistema de Pagamentos Instantâneos (SPI), para a abertura da Conta Pagamentos Instantâneos (Conta PI) e define os limites máximos de tempo para validação e para liquidação das ordens de pagamentos instantâneos, de que trata o Regulamento anexo à Resolução BCB nº 195, de 3 de março de 2022.
Responsável: DEBAN
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=382

36. **Título:** Resolução BCB n° 315, 27/4/2023
Data/Hora Documento: 27/4/2023 09:00
Assunto: Institui o Comitê Executivo de Gestão (CEG) do Projeto-Piloto da Plataforma do Real Digital (Piloto RD) e aprova o Regulamento do Piloto RD.
Responsável: SECRE

https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=315

37. **Título:** Resolução BCB n° 314, 26/4/2023
Data/Hora Documento: 26/4/2023 18:26
Assunto: Dispõe sobre a execução dos serviços de compensação de cheques apresentados à Centralizadora da Compensação de Cheques (Compe) e sobre questões operacionais relacionadas ao cheque.
Responsável: DINOR, DIORF, DIPOM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=314

38. **Título:** Instrução Normativa BCB n° 373, 25/4/2023
Data/Hora Documento: 25/4/2023 09:45
Assunto: Altera a Instrução Normativa BCB nº 291, de 29 de julho de 2022, que estabelece os procedimentos necessários para a adesão ao Pix, para ajustar dispositivos referentes à etapa cadastral e à etapa homologatória; para inserir anexos referentes ao questionário de autoavaliação em segurança; bem como para estabelecer disposições transitórias relacionadas ao envio do mencionado questionário.
Responsável: DECEM
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=373

39. **Título:** Resolução BCB n° 304, 20/3/2023
Data/Hora Documento: 20/3/2023 14:01
Assunto: Aprova o Regulamento que disciplina, no âmbito do Sistema de Pagamentos Brasileiro, o funcionamento dos sistemas de liquidação, o exercício das atividades de registro e de depósito centralizado de ativos financeiros e a constituição de ônus e gravames sobre ativos financeiros registrados ou depositados, e consolida normas sobre a matéria.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=304

40. **Título:** Comunicado n° 39.876, 6/3/2023
Data/Hora Documento: 6/3/2023 16:29
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, nos ambientes de homologação e de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=39876

41. **Título:** Resolução BCB n° 287, 24/1/2023
Data/Hora Documento: 24/1/2023 18:01
Assunto: Divulga a Política de Segurança da Informação do Banco Central do Brasil (PSIBC).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=287

42. **Título:** Resolução BCB n° 286, 24/1/2023
Data/Hora Documento: 24/1/2023 18:00
Assunto: Institui o Regulamento de Governança do Portal de Internet do Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=286

43. **Título:** Resolução BCB n° 273, 12/12/2022
Data/Hora Documento: 12/12/2022 09:00
Assunto: Constitui o Grupo de Trabalho Interdepartamental “GTI Tokenização”, no âmbito do Banco Central do Brasil, para realizar estudo sobre as atividades de registro, custódia, negociação e

liquidação de ativos financeiros em infraestruturas de registro distribuído (Distributed Ledger Technologies – DLTs).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=273

44. **Título:** Resolução BCB n° 265, 25/11/2022
Data/Hora Documento: 25/11/2022 14:14
Assunto: Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de conglomerado prudencial classificado como Tipo 3 enquadrado no Segmento 2 (S2), Segmento 3 (S3) ou Segmento 4 (S4).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=265

45. **Título:** Resolução BCB n° 249, 5/10/2022
Data/Hora Documento: 5/10/2022 18:10
Assunto: Divulga a Política de Governança da Informação do Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=249

46. **Título:** Instrução Normativa BCB n° 305, 15/9/2022
Data/Hora Documento: 15/9/2022 19:08
Assunto: Divulga a versão 4.0 do Manual de Segurança do Open Finance.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=305

47. **Título:** Comunicado n° 39.153, 15/9/2022
Data/Hora Documento: 15/9/2022 18:36
Assunto: Comunica a descontinuidade do procedimento de validação de credenciamento de acesso ao Extrato do Registro de Informações no Banco Central do Brasil (Sistema Registrato) por aplicativo de instituições financeiras.
Responsável: DEATI
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=39153

48. **Título:** Comunicado n° 38.683, 23/5/2022
Data/Hora Documento: 23/5/2022 15:53
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, nos ambientes de homologação e de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=38683

49. **Título:** Comunicado n° 38.579, 27/4/2022
Data/Hora Documento: 27/4/2022 15:46
Assunto: Comunica a habilitação da Autoridade Certificadora (AC) Soluti SPB para emissão de certificados digitais no padrão SPB e a publicação da versão 5.03 do Manual de Segurança do SFN.
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=38579

50. **Título:** Comunicado n° 38.484, 25/3/2022
Data/Hora Documento: 25/3/2022 11:25
Assunto: Aposição de assinatura digital em documentos de instrução de processo de autorização conduzido pelo Departamento de Organização do Sistema Financeiro (Deorf), nos termos da Instrução Normativa BCB nº 77, de 11 de fevereiro de 2021, alterada pela Instrução Normativa BCB nº 231, de 25 de janeiro de 2022.
Responsável: DEORF

https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=38484

51. **Título:** Resolução CMN n° 4.994, 24/3/2022
Data/Hora Documento: 24/3/2022 18:11
Assunto: Dispõe sobre as diretrizes de aplicação dos recursos garantidores dos planos administrados pelas entidades fechadas de previdência complementar.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4994

52. **Título:** Instrução Normativa BCB n° 243, 16/3/2022
Data/Hora Documento: 16/3/2022 10:30
Assunto: Divulga procedimentos a serem observados para participação direta no Sistema de Pagamentos Instantâneos (SPI), para a abertura da Conta Pagamentos Instantâneos (Conta PI) e define os limites máximos de tempo para validação e para liquidação das ordens de pagamentos instantâneos, de que trata o Regulamento anexo à Resolução BCB nº 195, de 3 de março de 2022.
Responsável: DEBAN
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=243

53. **Título:** Instrução Normativa BCB n° 231, 25/1/2022
Data/Hora Documento: 25/1/2022 17:36
Assunto: Altera a Instrução Normativa BCB nº 77, de 11 de fevereiro de 2021, que estabelece procedimentos, relativos ao envio de documentos e informações, de respostas a exigências e de interposição de recursos, à formalização de exigências, à comunicação da decisão e às demais comunicações relacionadas com a instrução e com o exame de processos de autorização conduzidos pelo Departamento de Organização do Sistema Financeiro (Deorf), e dá outras providências.
Responsável: DEORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=231

54. **Título:** Comunicado n° 38.185, 13/1/2022
Data/Hora Documento: 13/1/2022 16:18
Assunto: Comunica a ativação dos certificados digitais do Banco Central do Brasil, para uso exclusivo nos ambientes de homologação e de produção do SPI/ICOM, DICT e ARQ, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=38185

55. **Título:** Resolução CMN n° 4.963, 25/11/2021
Data/Hora Documento: 25/11/2021 18:30
Assunto: Dispõe sobre as aplicações dos recursos dos regimes próprios de previdência social instituídos pela União, pelos Estados, pelo Distrito Federal e pelos Municípios.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4963

56. **Título:** Resolução BCB n° 150, 6/10/2021
Data/Hora Documento: 6/10/2021 18:17
Assunto: Consolida normas sobre os arranjos de pagamento, aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=150

57. **Título:** Resolução BCB n° 134, 1/9/2021
Data/Hora Documento: 1/9/2021 18:00

Assunto: Dispõe sobre a custódia de numerário do Banco Central do Brasil e aprova seu Regulamento.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=134

58. **Título:** Resolução BCB n° 131, 20/8/2021
Data/Hora Documento: 20/8/2021 08:01
Assunto: Consolida as normas sobre o rito do processo administrativo sancionador, a aplicação de penalidades, o termo de compromisso, as medidas acautelatórias, a multa cominatória e o acordo administrativo em processo de supervisão, previstos na Lei nº 13.506, de 13 de novembro de 2017, e os parâmetros para a aplicação das penalidades administrativas previstas na Lei nº 9.613, de 3 de março de 1998.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=131

59. **Título:** Comunicado n° 37.509, 10/8/2021
Data/Hora Documento: 10/8/2021 17:29
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, no ambiente de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=37509

60. **Título:** Resolução BCB n° 124, 5/8/2021
Data/Hora Documento: 5/8/2021 18:01
Assunto: Institui procedimentos para acesso de entes públicos ao Cadastro de Clientes do Sistema Financeiro Nacional (CCS) e divulga Regulamento para adesão dos interessados.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=124

61. **Título:** Comunicado n° 37.372, 7/7/2021
Data/Hora Documento: 7/7/2021 17:01
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, no ambiente de homologação, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=37372

62. **Título:** Comunicado n° 37.320, 25/6/2021
Data/Hora Documento: 25/6/2021 17:17
Assunto: Comunica publicação de nova versão do Manual de Segurança do SFN e divulga procedimentos e prazos para a implantação da nova versão do protocolo de segurança das mensagens e dos arquivos do Catálogo de Serviços do SFN que trafegam na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=37320

63. **Título:** Resolução BCB n° 105, 9/6/2021
Data/Hora Documento: 9/6/2021 18:00
Assunto: Aprova o Regulamento do Sistema de Transferência de Reservas (STR), da conta Reservas Bancárias e da Conta de Liquidação no Banco Central do Brasil.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=105

64. **Título:** Resolução BCB n° 90, 26/4/2021

Data/Hora Documento: 26/4/2021 14:01
Assunto: Divulga o Plano Diretor de Gestão de Pessoas do Banco Central do Brasil para o período compreendido entre 2021 e 2023.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=90

65. **Título:** Instrução Normativa BCB n° 77, 11/2/2021
Data/Hora Documento: 11/2/2021 10:05
Assunto: Estabelece procedimentos relativos ao envio de documentos e informações, de respostas a exigências e de interposição de recursos, à formalização de exigências, à comunicação da decisão e às demais comunicações relacionadas com a instrução e com o exame de processos de autorização conduzidos pelo Departamento de Organização do Sistema Financeiro (Deorf), e dá outras providências.
Responsável: DEORF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=77

66. **Título:** Resolução CMN n° 4.883, 23/12/2020
Data/Hora Documento: 23/12/2020 17:17
Assunto: Dispõe sobre a consolidação dos dispositivos inseridos nos Capítulos 1, 2 e 3 do Manual de Crédito Rural (MCR), acerca de princípios, conceitos básicos e operação aplicáveis ao crédito rural.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4883

67. **Título:** Resolução BCB n° 55, 16/12/2020
Data/Hora Documento: 16/12/2020 08:05
Assunto: Aprova o Regulamento do Sistema Especial de Liquidação e de Custódia (Selic).
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=55

68. **Título:** Resolução Coremec n° 1, 9/12/2020
Data/Hora Documento: 9/12/2020 18:00
Assunto: Aprova o Regimento Interno do Comitê de Regulação e Fiscalização dos Mercados Financeiro, de Capitais, de Seguros, de Previdência e Capitalização (Coremec).
Responsável:
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Coremec&numero=1

69. **Título:** Comunicado n° 36.480, 4/12/2020
Data/Hora Documento: 4/12/2020 17:23
Assunto: Divulga o rol de instituições participantes obrigatórias do Open Banking, bem como valores relativos ao patrimônio líquido e de seu conglomerado prudencial, conforme o caso, para fins do custeio das atividades de manutenção da estrutura inicial responsável pela governança do processo de implementação no País do Open Banking.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=36480

70. **Título:** Comunicado n° 36.263, 9/10/2020
Data/Hora Documento: 9/10/2020 11:59
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, no ambiente de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=36263

71. **Título:** Comunicado n° 36.233, 1/10/2020

Data/Hora Documento: 1/10/2020 12:57
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, no ambiente de homologação, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=36233

72. **Título:** Resolução BCB n° 1, 12/8/2020
Data/Hora Documento: 12/8/2020 09:30
Assunto: Institui o arranjo de pagamentos Pix e aprova o seu Regulamento.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1

73. **Título:** Comunicado n° 35.895, 6/7/2020
Data/Hora Documento: 6/7/2020 10:53
Assunto: Divulga as associações e grupos de associações elegíveis a participar do processo eletivo para a indicação de representantes para o Conselho Deliberativo da estrutura inicial responsável pela governança do processo de implementação no País do Sistema Financeiro Aberto (Open Banking), bem como divulga o cronograma do processo eletivo e orientações para o registro de voto.
Responsável: DENOR
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=35895

74. **Título:** Resolução Conjunta n° 1, 4/5/2020
Data/Hora Documento: 4/5/2020 12:00
Assunto: Dispõe sobre a implementação do Open Finance.
Responsável:
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=1

75. **Título:** Comunicado n° 34.834, 6/12/2019
Data/Hora Documento: 6/12/2019 17:04
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, no ambiente de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=34834

76. **Título:** Comunicado n° 33.084, 30/1/2019
Data/Hora Documento: 30/1/2019 14:53
Assunto: Comunica a atualização de certificados digitais do Banco Central do Brasil para uso exclusivo nas mensagerias dos domínios MES e SPB, no ambiente de produção, na Rede do Sistema Financeiro Nacional (RSFN).
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33084

77. **Título:** Comunicado n° 32.066, 21/5/2018
Data/Hora Documento: 21/5/2018 16:10
Assunto: Comunica a publicação de nova versão do Manual de Acesso ao STR via Internet.
Responsável: DEBAN
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=32066

78. **Título:** Resolução CMN n° 4.557, 23/2/2017
Data/Hora Documento: 23/2/2017 18:33
Assunto: Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4557

79. **Título:** Resolução CMN n° 4.474, 31/3/2016
Data/Hora Documento: 31/3/2016 18:45
Assunto: Dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil, bem como sobre o procedimento de descarte das matrizes físicas dos documentos digitalizados e armazenados eletronicamente.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4474

80. **Título:** Comunicado n° 18.655, 2/7/2009
Data/Hora Documento: 2/7/2009 17:27
Assunto: Divulga nova versão do Regulamento do Grupo Técnico de Segurança da Rede do Sistema Financeiro Nacional.
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=18655

81. **Título:** Comunicado n° 10.193, 3/10/2002
Data/Hora Documento: 3/10/2002 16:53
Assunto: Divulga o regulamento do Grupo Técnico de Segurança do Sistema de Pagamentos Brasileiro.
Responsável: DEINF
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=10193

82. **Título:** Comunicado n° 8.454, 18/5/2001
Data/Hora Documento: 18/5/2001 18:16
Assunto: Comunica decisoes do Banco Central do Brasil, relativas a implementacao da Reestruturacao do Sistema de Pagamen- tos Brasileiro.
Responsável: SECRE
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=8454