UNIVERSIDADE DE CAXIAS DO SUL
ÁREA DE CONHECIMENTO DE CIÊNCIAS JURÍDICAS
CAMPUS UNIVERSITÁRIO DE SÃO SEBASTIÃO DO CAÍ

NAIRA PONTES MÜNCHEN

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A RESPONSABILIDADE CIVIL DAS EMPRESAS QUANTO AO VAZAMENTO DE DADOS PESSOAIS. A LEI Nº 13.709/2018

SÃO SEBASTIÃO DO CAÍ/RS
2025

NAIRA PONTES MÜNCHEN

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A RESPONSABILIDADE CIVIL DAS EMPRESAS QUANTO AO VAZAMENTO DE DADOS PESSOAIS. A LEI Nº 13.709/2018

Trabalho de conclusão apresentado no Curso de Direito da Universidade de Caxias do Sul, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientadora: Prof. Drª Cláudia Maria Hansel.

SÃO SEBASTIÃO DO CAÍ

2025

NAIRA PONTES MÜNCHEN

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A RESPONSABILIDADE CIVIL DAS EMPRESAS QUANTO AO VAZAMENTO DE DADOS PESSOAIS. A LEI Nº 13.709/2018

Trabalho de conclusão apresentado no Curso de Direito da Universidade de Caxias do Sul, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientadora: Prof. Drª Cláudia Maria Hansel.

Aprovada em: 01/12/2025

Banca Examinadora

_____

Orientadora: Prof. Drª Cláudia Maria Hansel
Universidade de Caxias do Sul – UCS

_____

Prof. Me. Fernanda Martinotto
Universidade de Caxias do Sul - UCS

_____

Prof. Me. Patrícia Montemezzo
Universidade de Caxias do Sul - UCS

Dedico este trabalho à minha família, aos meus amigos, professores e colegas de curso. Cada etapa deste projeto foi construída a partir das pessoas que fizeram parte da minha trajetória e da relevância do tema que me propus a estudar. Que esta pesquisa possa contribuir, de alguma forma, para todos aqueles que buscam compreender melhor a proteção de dados e seus impactos.

Dedico, por fim, a Deus, por ter me guiado, fortalecido e iluminado durante todo o processo de elaboração deste trabalho.

AGRADECIMENTOS

Em primeiro lugar agradeço aos meus pais, que são meu alicerce e que acreditaram em mim quando eu já não acreditava. Ao meu esposo, que não mediu esforços para que eu não perdesse nenhuma aula, estando ao meu lado na maioria das noites desses árduos oitos anos de caminhada. Agradeço também a Deus, por me conceder saúde e sabedoria para enfrentar os contratempos do caminho percorrido.

Manifesto,ainda, minha gratidão às amigas - tanto de longa quanto de curta data - especialmente àquelas que compartilharam comigo as salas de aula, dividindo as mesmas angústias e vitórias a cada semestre. Por fim, meu sincero agradecimento a minha orientadora, que, com resiliência e dedicação, me guiou e compartilhou seus conhecimentos da melhor forma possível.

A todos vocês, minha eterna gratidão.

Se você perdeu dinheiro, perdeu pouco. Se perdeu a honra, perdeu muito. Se perdeu a coragem, perdeu tudo.

– Vincent van Gogh

RESUMO

A crescente digitalização das relações sociais e econômicas intensificou o tratamento de dados pessoais, ampliando riscos de incidentes de dados pessoais e reforçando a necessidade de regulamentação específica. Nesse cenário, a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) instituiu no Brasil um marco normativo destinado a assegurar a privacidade, a segurança e a autodeterminação informativa. O presente trabalho tem por objetivo analisar a responsabilidade civil das empresas nos casos de incidentes de dados pessoais, investigando se agentes de tratamentos podem ser responsabilizados pelos danos decorrentes de violação à LGPD.Em seguida, examina-se o papel da Autoridade Nacional de Proteção de Dados (ANPD), suas competências fiscalizatórias e o processo de consolidação institucional, especialmente após as Resolução nº 1/2021 e nº 4/2023. O estudo também aborda os fundamentos legais do tratamento de dados, direitos dos titulares e hipóteses autorizadas previstas na legislação.Por fim, analisa-se a responsabilidade civil das empresas diante de incidentes de dados pessoais reais de vazamento, identificando padrões de falhas, setores mais afetados e decisões judiciais que reconhecem o dano moral presumido.Conclui-se que, no contexto da LGPD, a responsabilidade civil das empresas se firmou de forma objetiva e preventiva, funcionando como instrumento essencial de proteção à privacidade e de fortalecimento da cultura nacional de segurança da informação.

Palavras-chave: LGPD, Vazamento de dados, Responsabilidade civil, ANPD, Proteção de dados pessoais, Código de Defesa do Consumidor.

ABSTRACT

The increasing digitalization of social and economic relations has intensified the processing of personal data, expanding the risks of security incidents and reinforcing the need for specific regulation. In this context, the Brazilian General Data Protection Law (LGPD – Law Nº. 13,709/2018) established a legal framework aimed at safeguarding privacy, security, and informational self-determination. This study analyzes the civil liability of companies in cases of personal data breaches, investigating whether data controllers may be held accountable for damages resulting from violations of the LGPD. Initially, it presents a historical overview of data protection in the international and national spheres, highlighting the legislative developments that culminated in the LGPD. It then examines the role and supervisory functions of the Brazilian Data Protection Authority (ANPD), with emphasis on its institutional consolidation following Resolutions Nº. 1/2021 and Nº. 4/2023. The research also addresses the legal bases for data processing, the rights of data subjects, and the authorized hypotheses established by the legislation. Finally, it analyzes the civil liability of companies based on real cases of data breaches, identifying recurring failures, the economic sectors most affected, and judicial decisions recognizing presumed moral damage. The study concludes that, under the LGPD, the civil liability of companies is consolidated as objective and preventive, serving as an essential mechanism for protecting privacy and strengthening Brazil's national culture of information security.

Keywords: LGPD, Data breach, Civil liability, ANPD, Personal data protection, Consumer defender code.

LISTA DE SIGLAS E ABREVIAÇÕES

ANPD	Autoridade Nacional de Proteção de Dados
ARPANET	Advanced Research Projects Agency Network
ART	Artigo
CD	Conselho Diretor
CDC	Código de Defesa do Consumidor
CPF	Cadastro de Pessoa Física
DDOS	Ataque Distribuído de Negação de Serviço
EC	Emenda Constitucional
FGV	Fundação Getúlio Vargas
GDPR	Regulamento Geral de Proteção de Dados Pessoais
INPD	Instituto Nacional de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados Pessoais
ONU	Organização das Nações Unidas
PL	Projeto de Lei
PLC	Projeto de Lei Complementar
PLS	Projeto de Lei do Senado
PSTI	Provedor de serviço de tecnologia da informação
RDC	Resolução de Diretoria Colegiada
SESC	Serviço Social do Comércio
STJ	Superior Tribunal de Justiça
TI	Tecnologia da Informação
UE	União Europeia
WWW	World Wide Web

LISTA DE FIGURAS

Figura 1 - Proteção de dados no cenário mundial..... 15
Figura 2 - Proteção de dados no Brasil..... 19
Figura 3 - Petições de titular recebidas por setor - 2022..... 30
Figura 4 - Comunicado de incidente de segurança recebidos pela ANPD (2021-2024)..... 31
Figura 5 - Comunicados recebidos por trimestre e ano (2021-2024)..... 31
Figura 6 - Atividades fiscalizatórias..... 37

LISTA DE QUADROS

Quadro 1 - Lista de países com proteção de dados nível GDPR..... 44
Quadro 2 - Comparativo entre os requisitos de adequação da GDPR e as disposições..... 46
Quadro 3 - Incidentes de dados pessoais no Brasil e consequências..... 63

SUMÁRIO

1 INTRODUÇÃO.....12
2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.....14
2.1 PROTEÇÃO DE DADOS NO MUNDO, E O BERÇO DE SEU SURGIMENTO……..14
2.2 INFLUÊNCIA DO CRESCIMENTO TECNOLÓGICO NA PROTEÇÃO DE DADOS.. 26
2.3 RELEVÂNCIA DA PROTEÇÃO DE DADOS NO BRASIL..... 29
3 A QUALIFICAÇÃO JURÍDICA DA FISCALIZAÇÃO DE DADOS POR PARTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD..... 34
3.1 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD: ATRIBUIÇÕES...34
3.2 SANÇÕES APLICÁVEIS RESULTANTE DA FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.....36
4 A PROTEÇÃO DE DADOS NA FORMA DA LEI Nº 13.709/2018.....41
4.1 PROTEÇÃO ADVINDA DA LEI Nº 13.709/2018.....41
4.2 LACUNAS DO LEGISLADOR.....43
4.3 FUNDAMENTOS DA LGPD.....49
4.4 RESPONSABILIDADE CIVIL NOS INCIDENTES DE DADOS PESSOAIS..... 51
4.5 CONCEITO DE RESPONSABILIDADE CIVIL.....52
4.6 HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS..... 56
4.7 ANÁLISE DA RESPONSABILIDADE DAS EMPRESAS EM CASOS DE INCIDENTES DE DADOS PESSOAIS..... 58
5 CONSIDERAÇÕES FINAIS..... 67
REFERÊNCIAS..... 69

1 INTRODUÇÃO

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), inaugurou no ordenamento jurídico brasileiro um novo paradigma de tutela da privacidade e da autodeterminação informativa, estabelecendo regras específicas para coleta, armazenamento, compartilhamento e tratamento de dados pessoais. A crescente digitalização das relações sociais, o aumento exponencial do fluxo informacional e a expansão das tecnologias da informação intensificaram a circulação de dados, ampliando tanto as possibilidades de desenvolvimento econômico quanto os riscos relacionados a usos indevidos, vazamentos e incidentes de segurança.

Nesse contexto, o presente trabalho tem como tema a responsabilidade civil das empresas nos casos de incidentes de dados pessoais, analisados a partir das disposições da LGPD. Como problema de pesquisa, busca-se responder: às empresas que descumprem as normas legais relativas ao tratamento de dados pessoais podem ser responsabilizadas civilmente pelos danos decorrentes de incidentes de dados pessoais?

O estudo justifica-se diante da centralidade que os dados pessoais assumiram no cenário contemporâneo e da vulnerabilidade acentuada dos titulares, especialmente consumidores que, diante da dependência digital, tornaram-se hipervulneráveis a práticas abusivas, falhas de segurança e incidentes envolvendo seus dados. Além disso, a multiplicidade de incidentes de dados pessoais ocorridos nos últimos anos - alguns de grande escala - evidenciam a urgência de compreender os mecanismos legais de prevenção, fiscalização e responsabilização.

O objetivo geral consiste em analisar de que forma o ordenamento jurídico brasileiro, especialmente por meio da LGPD, estrutura a responsabilidade civil aplicável às empresas nos casos de incidentes de dados pessoais.

Para atender ao objetivo proposto, divide-se o trabalho de conclusão em três seções mais introdução e conclusão. A primeira seção intitulada de “Lei Geral de Proteção de Dados Pessoais”, tem como objetivo apresentar o panorama histórico da proteção de dados no cenário mundial e brasileiro, bem como apresentar a influência do crescimento tecnológico na proteção de dados e a relevância da proteção de dados no Brasil. A segunda seção intitulada de “A qualificação jurídica da fiscalização de dados por parte da Autoridade Nacional de Proteção de Dados -

ANPD”, tem como objetivo tratar do surgimento da ANPD, demonstrar suas atribuições em especial a fiscalizatória e trazer as sanções que podem ser atribuídas às pessoas físicas e jurídicas em casos de má administração dos dados dos titulares bem como em casos de incidentes de dados pessoais. A terceira seção intitulada “A proteção de dados na forma da Lei nº 13.709/2018”, tem como objetivo estudar a letra da Lei, examinando os princípios e fundamentos legais que autorizam o tratamento de dados pessoais, bem como, debater os fundamentos teóricos da responsabilidade civil e analisar a responsabilidade das empresas nos casos de incidentes de dados pessoais, incluindo precedentes, atuação da ANPD e estudo de casos.

Quanto a metodologia, adotou-se abordagem qualitativa, com pesquisa bibliográfica e documental, contemplando legislação, doutrina, jurisprudências, relatórios teóricos e análises de casos públicos de incidentes de dados pessoais.Cabe mencionar, ainda, a utilização da ferramenta de inteligência artificial ChatGPT (versão GPT-5.1), desenvolvida pela OpenAI, como apoio exclusivamente para revisão linguística, identificação de inconsistências gramaticais e apoio para adequação às normas da ABNT. Ressalta-se que todas as sugestões fornecidas pela ferramenta foram avaliadas pelo autor antes de sua incorporação ao texto final, mantendo-se a autonomia intelectual sobre o conteúdo produzido.

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representa um marco regulatório no ordenamento jurídico, estabelecendo direitos, deveres e princípios que orientam o tratamento de dados pessoais. Sua criação não ocorreu de forma isolada, mas decorre de um processo histórico marcado por avanços tecnológicos, a crescente circulação de dados e a necessidade de adaptar a legislação nacional com padrões internacionais de proteção da privacidade.

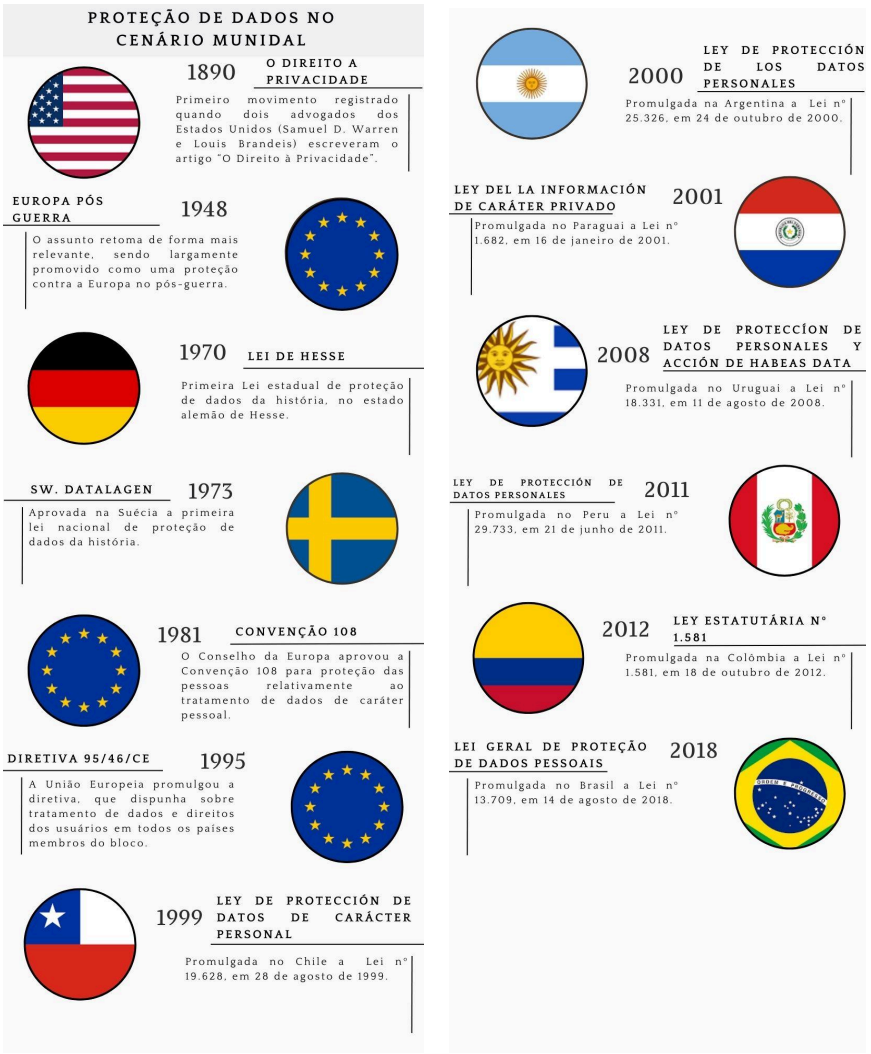
Ao mesmo tempo em que reflete tendências globais, como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD responde às demandas internas por segurança jurídica, transparência e responsabilidade no uso de informações.

Nessa seção, serão abordados o contexto internacional e as origens da proteção de dados, a influência do crescimento tecnológico e a relevância da sua aplicação no cenário brasileiro.

2.1 PROTEÇÃO DE DADOS NO MUNDO, E O BERÇO DE SEU SURGIMENTO

Antes mesmo de se falar em Lei Geral de Proteção de Dados Pessoais, é importante entender onde surgiram os primeiros lampejos da ideia de proteger a privacidade e os dados pessoais. Abaixo, foi elaborada uma linha do tempo para melhor compreensão.

Figura 1 - Proteção de dados no cenário mundial.



Fonte: Elaboração própria com base em ZUP (2021).

A história da proteção de dados começa a se formar ainda no século XIX quando em 1890, nos Estado Unidos, os advogados Samuel D. Warren e Louis Brandeis publicaram o artigo “O Direito e à Privacidade”, na Harvard Law Review, considerado o primeiro marco teórico sobre o direito à privacidade como um direito fundamental.

Após a Segunda Guerra Mundial, em 1948, o tema ganhou status internacional com a Declaração Universal dos Direitos Humanos da ONU, que, em seu Art. 12, protege os indivíduos contra ingerências arbitrárias na vida privada. Poucos anos depois, a Convenção Europeia de Direitos Humanos (1950) reforçou esse entendimento, vinculando o direito à privacidade ao novo contexto democrático do pós-guerra. Esses instrumentos pavimentaram o caminho para a futura regulamentação da proteção de dados no continente europeu.

O debate moderno sobre dados pessoais começou a surgir nos anos de 1970, quando os computadores passaram a ser usados para armazenar informações em larga escala. Em 1970, o estado alemão de Hesse aprovou a primeira lei de proteção de dados do mundo, refletindo a preocupação com abusos estatais em uma sociedade ainda marcada pela memória do nazismo. Poucos anos após, em 1973, a Suécia se tornou o primeiro país a adotar uma lei nacional, a *Datalagen,* voltada à regulação do uso de cadastros públicos informatizados.

No início da década de 1980, a Europa vivia um período de reconstrução política e social após as turbulências do pós-guerra e o fortalecimento das democracias ocidentais, em contraste com os regimes do Leste, ainda sob a influência da União Soviética.Assim, em 1981, o Conselho da Europa aprovou a Convenção 108, o primeiro tratado internacional juridicamente vinculante voltado exclusivamente à proteção de dados pessoais. Ela estabeleceu princípios básicos: tratamento leal e lícito, limitação da coleta, qualidade e segurança dos dados, além de prever a cooperação entre os Estados. O texto deixou claro que a proteção de dados não era apenas uma questão técnica, mas um direito humano ligado à dignidade e à vida privada.

Nos anos 1990, a União Europeia consolidou sua liderança com a Diretiva 95/46/CE, que harmonizou a proteção de dados nos Estados-membros e se tornou referência internacional.

No final dos anos 1999 e início dos anos 2000, o movimento começa a se espalhar pela América Latina. O Chile promulgou, em 28 de agosto de 1999, a primeira lei latino-americana de proteção de dados, a *Ley de Protección de Datos de Carácter Personal*, o dispositivo garante direitos aos “titulares” dos dados tratados (as pessoas a quem os dados se referem), como o direito à correção e exclusão dos dados, assim como obrigações, como a limitação do uso dos dados coletados ao propósito informado pelo responsável por seu tratamento, refletindo a consolidação de sua democracia após a ditadura militar.

> A ditadura militar chilena começou em 11 de setembro de 1973, quando o presidente Salvador Allende foi deposto do poder por meio de um golpe militar liderado pelo general Augusto Pinochet. Durante 15 anos, Pinochet governou com mãos de ferro, sendo implacável contra seus opositores. Em 1988, Pinochet sofreu uma derrota com o resultado de um plebiscito, no qual 56% dos eleitores rejeitaram a sua continuidade no poder. Logo após o

> fim da ditadura, os militares acusados de crimes contra os Direitos Humanos foram julgados e condenados à prisão (Higa, *[s.d.]*, p.01).

Seguindo pela Argentina, a mesma que na década de 1990 adotou medidas neoliberais, o que reduziu a participação do Estado na economia e permitiu uma maior abertura econômica. O peso argentino foi substituído pelo dólar como unidade monetária, o que implicou em direcionar as políticas econômicas argentinas para a atração de dólares, oferecendo altas taxas de juros para rendimentos na moeda estadunidense. Para manter essa política, a Argentina acabou ficando muito endividada, resultando em uma crise econômica sem precedentes. (Silva, JCL ,*[s.d.]*, p.01) - promulgou a *Ley nº 25.326 de Protección de los Datos Personales*, que trouxe disposições e princípios relativos à proteção de dados, fazendo com que o país fosse reconhecido pela União Europeia como o país com nível adequado de proteção de dados.

No Paraguai, não há uma lei geral de proteção de dados, como na Suécia, Chile e Argentina (países listados anteriormente), contando apenas com um dispositivo genérico sobre o tema, a *Ley nº 1.682 que Regulamenta la Información de Carácter Privado*, foi promulgada em 16 de janeiro de 2001, abordando de maneira ampla quais dados podem ser tratados, como, e estabelecendo sanções para as organizações que descumprirem tais disposições.

O Uruguai, em 2008, no meio da crise financeira mundial, “foi o único do continente americano que não passou por uma recessão econômica técnica (dois trimestres consecutivos de retração)” (Times, 2012,p.01), e no mesmo ano aprovou a *Ley de Protección de Datos Personales y Acción de Habeas Data,* em 11 de agosto de 2008. A lei incorporou o *habeas data* como instrumento de defesa do cidadão.

Cumpre mencionar que a Argentina e Uruguai são os dois únicos países do continente sul-americano que são considerados “adequados” pela Comissão Europeia, órgão da UE que determina os níveis de adequação em matéria de proteção de dados pessoais e simplifica o fluxo internacional. (Oliveira, 2023,p.03)

Para o país estar de acordo com os requisitos do Art.45 da GDPR, a lei regulamentadora, bem como possíveis autoridades regulamentadoras devem conter: Estado de direito e direitos fundamentais, princípios para o tratamento de dados, tratar sobre o direitos dos titulares, base legal para o tratamento, transferência internacional de dados, deve existir uma autoridade de supervisão autônoma, trazer

sanções e responsabilização bem como recursos judiciais e administrativos para o cidadão poder recorrer contra violações, o país deve aderir tratados e convenções internacionais de direitos humanos e proteção de dados bem como devem existir medidas técnicas e administrativas adequada para a segurança e prevenção de incidentes de dados pessoais.

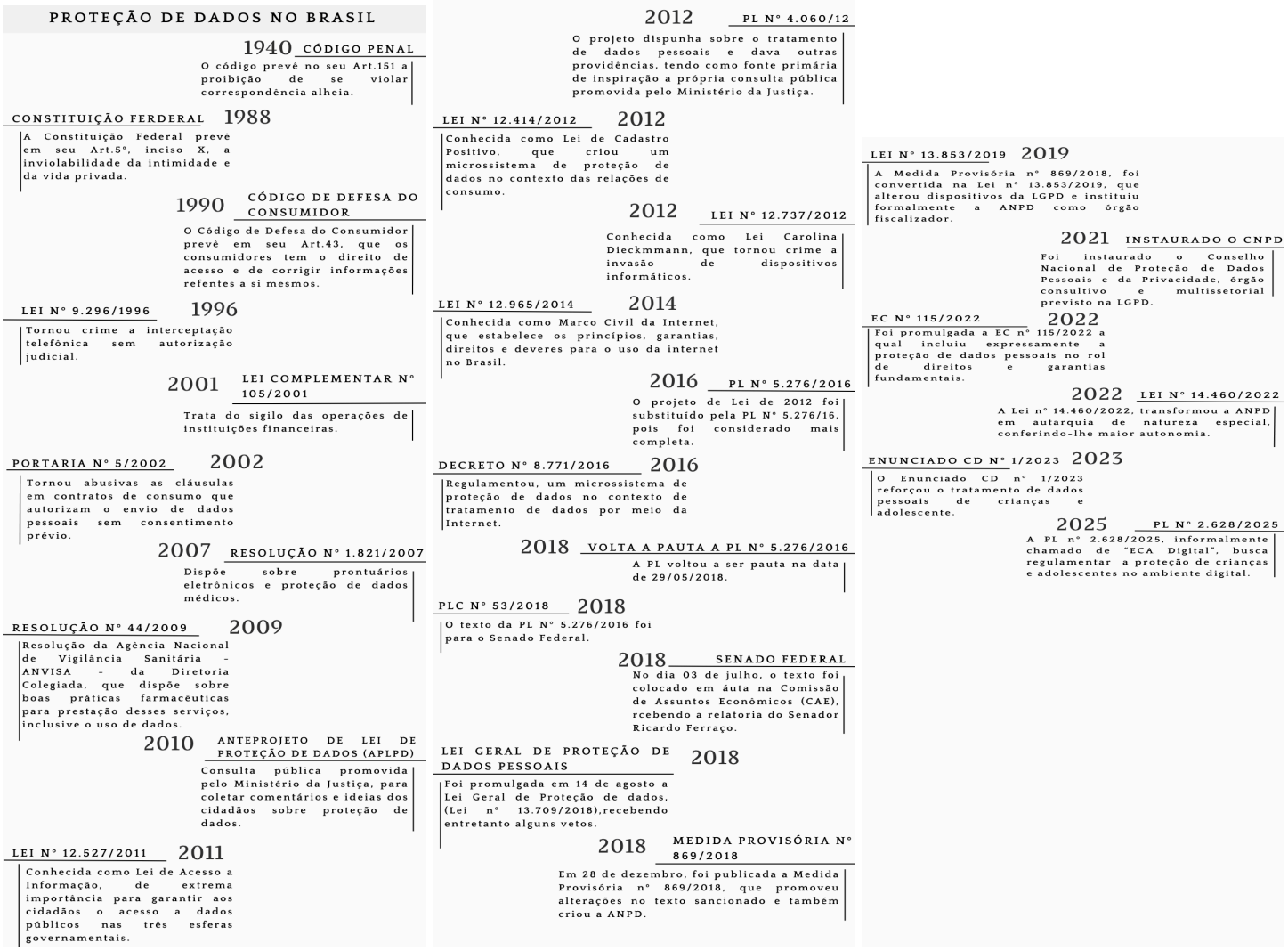
No Peru, foi promulgada a *Ley de Protección de Datos Personales* em 21 de junho de 2011. A lei peruana, assim como as outras já mencionadas, traz os princípios do tratamento de dado pessoais, os direitos do titular, as obrigações do titular e do responsável pelo tratamento, o funcionamento dos bancos de dados e de uma autoridade nacional para a proteção de dados, além de sanções administrativas aplicáveis ao responsável pelo tratamento.

Para fechar o quadro da evolução histórica mundial da proteção de dados, temos mais um país da América Latina, a Colômbia. No país colombiano vigora a *Ley Estatutaria nº 1.581,* que foi promulgada em 18 de outubro de 2012, que dispõe sobre a proteção de dados pessoais. Ela detalha os princípios que regem o tratamento de dados, os direitos dos titulares e a responsabilidade das organizações responsáveis por esse tipo de tratamento.

Diante desse panorama internacional, percebe-se que a proteção de dados pessoais não surgiu de forma isolada, mas como resultado de um movimento global da consolidação dos direitos fundamentais, especialmente após períodos de instabilidade econômica,política, guerras e avanços tecnológicos. À medida que diferentes países estruturaram suas legislações para assegurar a privacidade e regular uso de informações, formou-se um ambiente jurídico que influenciou diretamente o debate latino-americano - e, consequentemente, o brasileiro.

Assim, embora o Brasil tenha seguido seu próprio recurso normativo, sua evolução se conecta com as tendências e aprendizados internacionais, refletindo tanto os desafios internos quanto a necessidade de alinhamento com padrões globais de proteção de dados. Nesse contexto, torna-se essencial compreender como, ao longo das décadas, o ordenamento jurídico brasileiro incorporou garantias relacionadas à privacidade, até culminar na promulgação da Lei Geral de Proteção de Dados Pessoais em 2018, conforme demonstrado na linha do tempo a seguir.

Figura 2 - Proteção de dados no Brasil.



Fonte: Elaboração própria com base em ZUP (2021) e SILVA. APV (2025).

Em 1940 com a entrada em vigor do Código Penal, em seu Art. 151, o código prevê a proibição de se violar correspondência alheia, ainda que não trata especificamente de proteção de dados, o artigo é um marco por tratar pela primeira vez em contexto legal, do direito à privacidade, em tempos em que o país passava por grandes transformações na sociedade brasileira e no contexto internacional.

> Internamente, a década marcou o auge e o fim do Estado Novo (1937-1946), seguido por um período de abertura democrática. Além disso, o Brasil passava por um processo de urbanização acelerada, com a intensificação dos movimentos migratórios do campo para as cidades. No entanto, a pobreza, a desigualdade social e a baixa escolaridade da população dificultavam a industrialização, limitavam a formação de um mercado consumidor e impediam o desenvolvimento socioeconômico do país (SESC, 2021, p.01).

A Constituição Federal de 1988, ou “Constituição Cidadã”, como ficou conhecida por ter sido concebida no processo de redemocratização, iniciado com o encerramento da ditadura militar, também teve certa preocupação com o tema ao prever, em seu Art.5º, inciso X, a inviolabilidade da intimidade e da vida privada, assegurando ainda o direito a indenização pelo dano material e moral decorrente de sua violação. A Constituição ainda garante a inviolabilidade das comunicações em trânsito, que somente podem ser interceptadas por meio de ordem judicial.

Em 1990, o Código de Defesa do Consumidor, trouxe, no Art.43, o direito dos consumidores de acessar e corrigir informações sobre si mesmos.

Na mesma linha da interceptação telefônica trazida pela Constituição Federal, em 24 de julho de 1996 foi promulgada a Lei nº 9.296/1996 - Lei da Interceptação Telefônica, que tornou crime a interceptação telefônica sem autorização judicial. A partir de 2001, o Brasil passou a regulamentar mais detalhadamente a proteção de dados pessoais, com a Lei de Sigilo das Operações Financeiras (Lei Complementar nº 105/2001), que estabeleceu o dever de as instituições financeiras manterem sigilo sobre as operações, mas permitindo exceções, como o fornecimento de informações a órgãos de proteção ao crédito e mediante autorização judicial.

Em 2002, a Portaria nº 5/2002 da Secretaria de Direito Econômico do Ministério da Justiça declarou abusivas as cláusulas em contratos de consumo que autorizaram o envio de dados pessoais sem consentimento prévio. Essa norma complementou o rol de cláusulas abusivas do Código de Defesa do Consumidor.

Em 2007 a proteção de dados tomou novos ares com a Resolução nº 1.821/2007 do Conselho Federal de Medicina, que dispõe sobre prontuários eletrônicos e produção de dados médicos. Foi a primeira a aprovar o Manual de Certificação para o Sistema de Registros Eletrônico em Saúde (versão 3.0), além de autorizar a digitalização dos prontuários com o objetivo de eliminar o uso do papel.

Seguindo o ramo da saúde, em 2009 foi editada a Resolução da Diretoria Colegiada nº 44/2009 da Anvisa, que estabeleceu as normas para as boas práticas farmacêuticas em farmácias e drogarias no Brasil, incluindo o uso de dados pessoais.

O Art.59 da referida RDC dispõe:

> Art.59. É responsabilidade do estabelecimento farmacêutico detentor do sítio eletrônico, ou da respectiva rede de farmácia ou drogaria, quando for o caso, assegurar a confidencialidade dos dados, a privacidade do usuário e a

> garantia de que acessos indevidos ou não autorizados a estes dados sejam evitados e que seu sigilo seja garantido.
> Parágrafo único. Os dados dos usuários não podem ser utilizados para qualquer forma de promoção, publicidade, propaganda ou outra forma de indução de consumo de medicamentos (Brasil. RDC Nº 44, 2009, p.12).

Em 2010, o Ministério da Justiça redigiu o Anteprojeto de Lei de Proteção de Dados (APLPD) e o disponibilizou para consulta e comentários públicos. Foi criado um blog sobre proteção de dados e aberta uma Consulta Pública sobre o tema, ambos hospedados no site “culturadigital.br”.

> No cenário mundial foi promovido pelo site WikiLeaks, o vazamento de uma série de documentos confidenciais dos Estados Unidos agitou de diplomacia mundial. Os relatórios registravam a comunicação entre embaixadas em diversos países, incluindo o Brasil. Com dados inéditos sobre as guerras do Afeganistão e do Iraque, a ação ficou conhecida com o maior vazamento da história do exército americano (G1, 2023, p.02).

No setor público, o principal marco foi a promulgação da Lei nº 12.527, de 18 de novembro de 2011 - a Lei de Acesso à Informação, de extrema importância por garantir aos cidadãos o acesso a dados públicos nas três esferas do governo.

O ano de 2012 foi marcado por avanços significativos. Inicialmente, com o Projeto de Lei nº 4.060/2012, de autoria do Deputado Milton Monti, que tratava da proteção de dados pessoais e teve como base a consulta pública promovida em 2010 pelo Ministério da Justiça.O projeto visava modificar a legislação relativa à interceptação de comunicações telefônicas e eletrônicas, assegurando a privacidade e a comunicação dos cidadãos, mas também prevendo exceções para investigações criminais.

A PL nº 4.060/2012 trata da regulação e controle da interceptação, garantindo direitos à privacidade e à comunicação, mas também permitindo exceções para garantir a investigação de crimes.

No mesmo ano, foi aprovada a Lei do Cadastro Positivo (Lei nº 12.414/2012), que complementou o Código de Defesa do Consumidor, que criou um microssistema de proteção de dados no contexto das relações de consumo, focando em dados de adimplência e modelagem de crédito. A norma já tratava de princípios como finalidade, necessidade e revisão de decisões automatizadas.

Com o avanço da tecnologia e a evolução da internet a toda vapor em 30 de novembro de 2012, foi promulgada a Lei nº 12.737, conhecida como Lei Carolina Dieckmmann, o primeiro texto legal a tipificar os crimes cibernéticos, especialmente

invasões a dispositivos sem a permissão do proprietário. Essa lei surgiu após um episódio de maio de 2011, quando a atriz Carolina Dieckmmann teve seu computador pessoal invadido por um *hacker* (criminoso virtual), possibilitando que ele tivesse acesso a 36 fotos pessoais de cunho íntimo.

> De acordo com a denúncia, o invasor exigiu R$ 10 mil para não publicar as fotos. Como a atriz recusou a exigência, acabou tendo suas fotos divulgadas na internet. Isso criou uma grande discussão popular sobre a criminalização desse tipo de prática, que ainda foi excessivamente fomentada pela mídia.A atriz abraçou a causa e cedeu seu nome à lei. Ressalta-se que, antes do surgimento da lei, o ato de invadir um ambiente virtual e subtrair dados pessoais já era crime, mas não havia nenhuma norma que tratava especificamente sobre o assunto (FMP.EDU, 2021, p.02).

A nova lei acrescentou os Artigos 154-A e 154-B ao Código Penal, e alterou a redação dos Artigos 266 e 298. A seguir a redação dos dispositivos incluídos:

> **Invasão de dispositivo informático** (Incluído pela Lei nº 12.737, de 2012)
> 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.
> **Ação penal** (Incluído pela Lei nº 12.737, de 2012) Vigência
> 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 (Brasil. Código Civil, 1940-2012, p.35-36).

A conduta do agente deve ensejar violação de dispositivo, portanto, com o intuito de adulterar, obter ou destruir dados sem autorização do titular ou proprietário do dispositivo. A produção, oferecimento, distribuição, venda ou difusão de programa de computador ou de outros dispositivos também são condutas que se encaixam no crime tipificado no Art.154-A, do Código Penal, incluído pela Lei Carolina Dieckmmann.

Com a Copa do Mundo de 2014 sediada no Brasil, houve um aumento significativo nos incidentes de dados pessoais. *Hackers* ativistas intensificaram os ataques, utilizando técnicas como o *phishing* - que consiste em simular sites de bancos ou lojas para enganar usuários - e ataques de negação de serviços (*DDoS*) contra sites do governo e empresas privadas.

> Segundo o CERT.br, que contabilizou **28.808 casos**. Outros tipos de sites relacionados a demais atividades não financeiras foram utilizados em phishing em uma taxa de **73% maior que em 2013**. Também foram registrados **54% a mais de ataques a servidores**.
> No que diz respeito a ataques DoS, não estão em maior número de ocorrências mas é a categoria que teve maior aumento de incidências, somando **223.935 registros**. Para se ter ideia do assustador aumento, isso representa **217 vezes mais** incidentes em comparação ao ano de 2013. As principais causas que motivam tais ataques são ativismo e jogos online (Cavalcante, 2015, p.02).

Diante desse cenário, foi promulgada, em 23 de abril de 2014, a Lei nº 12.965, conhecida como Marco Civil da Internet, que estabeleceu os princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O Projeto de Lei nº 4.060/2012 voltou à tona no ano de 2016, mas foi substituído pela PL nº 5.276/2016, considerada mais abrangente. Essa nova proposta buscava criar um sistema mais robusto de proteção à privacidade e aos dados pessoais, modernizando a legislação brasileira diante do avanço das tecnologias digitais.

Enquanto a PL nº 4.060/2012 focava na interceptação de comunicações para fins de investigações criminais, a PL nº 5.276/2016 tratava da proteção de dados pessoais em ambientes digitais e empresariais,visando regular o tratamento dessas informações.

Ainda em 2016, no dia 11 de maio, foi promulgado o Decreto nº 8.771/2016, que regulamenta dispositivos do Marco Civil da Internet, especialmente os Artigos 11,13 e 15. O decreto garantiu a neutralidade de rede, proteção de dados pessoais e segurança da informação na internet. Segundo Andrade,

> O texto define que a neutralidade de rede deve ser observada pelos provedores de conexão, que não podem bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados.
> [...]
> Qualquer violação ao princípio da neutralidade deve ser apurada pela Anatel em conjunto com o Comitê Gestor da Internet no Brasil, observando os critérios técnicos estabelecidos.
> Com relação à proteção de dados, o decreto impõe aos provedores de aplicações de internet e de conexão a obrigação de garantir a segurança das informações pessoais dos usuários, utilizando medidas como controle de acesso, autenticação e registro de acesso aos sistemas.
> A guarda e proteção dos dados devem respeitar padrões de segurança compatíveis com a natureza das informações tratadas (Andrade,*[s.d.]* p.02-03).

Assim, o Decreto nº 8.771/2016 se destaca como uma medida essencial na efetivação do Marco Civil da Internet, promovendo o equilíbrio entre a segurança da informação, proteção de dados pessoais e respeito à neutralidade da rede. Estabelecendo diretrizes claras para provedores, o decreto fortalece a construção de um ambiente digital mais seguro, transparente e com respeito aos direitos dos usuários.

A Proposta de Lei nº 5.276/2016, que visava a proteção de dados pessoais, foi declarada prejudicada em 2018, uma vez que o texto que prevaleceu e deu origem à LGPD foi o substitutivo apresentado no Senado Federal - o PLC nº 53/2018, de autoria do deputado Orlando Silva. Esse projeto foi constituído com base nas propostas da própria PL nº 5.276/2016 e da PL nº 4.060/2012, ambas voltadas à proteção da privacidade no ambiente digital.

No dia 03 de julho de 2018, o PLC nº 53/2018 foi incluído na pauta Comissão de Assuntos Econômicos (CAE) do Senado Federal, sob relatoria do senador Ricardo Ferraço, que até então era relator do PLS nº 330/2013 - outro projeto de lei geral de proteção de dados pessoais que tramitava paralelamente no Senado Federal.

Em 10 de julho, após forte mobilização da sociedade civil e de diversos setores da sociedade, o projeto foi pautado no plenário do Senado Federal, sendo aprovado por unanimidade. Em seguida, o texto foi encaminhado para sanção presidencial, a qual ocorreu em 14 de agosto, com alguns vetos - em especial aos Artigos 55 a 59 que instituíam e organizavam a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. A justificativa dos vetos foi a existência de vício de iniciativa, sob o argumento de que tais órgãos não poderiam ser criados por projeto de origem legislativa, mas sim por iniciativa normativa do Poder Executivo.

Finalmente, com a promulgação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), foi instituída como o principal marco regulatório sobre tratamento de dados pessoais no Brasil, aplicando-se tanto a pessoas físicas quanto jurídicas, do setor público ou privado. A LGPD estabelece regras claras quanto à coleta, uso, armazenamento e compartilhamento de dados pessoais, assegurando os princípios da finalidade, necessidade, transparência e segurança.Além disso, define sanções administrativas em casos de descumprimento de suas diretrizes, como multas e bloqueio de dados.

A proteção de dados pessoais, portanto, é uma pauta de relevância global, fruto de décadas de evolução jurídica e tecnológica. A LGPD reflete essa trajetória ao consolidar o direito à privacidade como direito fundamental, alinhando o Brasil a legislações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, e fortalecendo a cidadania digital.

A partir da entrada em vigor da LGPD, o Brasil ingressou de forma definitiva no cenário global de proteção de dados pessoais. No entanto, sua efetiva implementação demandou passos institucionais adicionais. Nesse sentido em 28 de dezembro, foi publicada a Medida Provisória n° 869/2018, posteriormente convertida na Lei nº 13.853/2019, que alterou dispositivos da LGPD e instituiu formalmente a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por zelar pela proteção de dados pessoais, implementar e fiscalizar o cumpriemnto da legislação.

O processo de estruturação da ANPD representou etapa fundamental para a concretização do regime brasileiro de proteção de dados, uma vez que consolidou a autoridade regulatória como elemento indispensável ao modelo jurídico-institucional da LGPD, em convergência com padrões internacionais, especialmente o europeu.

Em 2021, reforçando essa evolução institucional, foi instaurado o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), órgão consultivo e multissetorial previsto na LGPD desde sua origem. O Conselho passou a desempenhar papel estratégico no diálogo entre governo, sociedade civil, academia e setor privado, auxiliando na construção de diretrizes, recomendações e debates públicos sobre privacidade e proteção de dados no país, fortalecendo o caráter democrático e participativo no sistema brasileiro.

Em seguida, um marco constitucional ampliou significativamente a relevância jurídica do tema. Em 10 de fevereiro de 2022, foi promulgada a Emenda Constitucional nº 115/2022, que incluiu expressamente a proteção de dados pessoais (Art.5º,inciso LXXIX) - inclusive nos meios digitais - no rol de direitos e garantias fundamentais, além de atribuir à União competência privativa para legislar sobre o tema. Sua aprovação consagrou a proteção de dados como valor constitucional estruturante e elevou o grau de proteção conferido ao titular, aproximando o Brasil dos sistemas mais avançados do mundo.

No mesmo ano, reforçando a maturidade institucional do tema, foi editada a Lei nº 14.460/2022, que transformou a ANPD em autarquia de natureza especial,

conferindo-lhe maior autonomia administrativa, técnica e financeira. Tal mudança fortaleceu sua atuação regulatória e fiscalizatória e garantiu maior segurança jurídica em processos sancionatórios, regulamentares e orientativos.

Em 2023, a ANPD avançou na consolidação normativa do sistema ao aprovar importantes orientações, dentre elas o Enunciado CD/ANPD nº 1/2023, dedicando ao tratamento de dados pessoais de crianças e adolescentes. O documento reforçou que, nessas hipóteses a interpretação da LGPD deve observar o melhor interesse do menor como princípio absoluto, resguardando-o de práticas abusivas e garantindo proteção reforçada, em consonância com o Art.14 da LGPD e com o Estatuto da Criança e do Adolescente.

Atualmente, a discussão legislativa segue em evolução. Em 2025, ganhou destaque o Projeto de Lei nº 2.628/2025, informalmente chamado de “ECA Digital”, que busca regulamentar, de maneira específica e mais detalhada, a proteção da criança e do adolescente no ambiente digital, abordando temas como publicidade direcionada, deveres das plataformas digitais, verificação de idade e mecanismos de segurança para menores. A proposta representa o contínuo aperfeiçoamento normativo brasileiro em sintonia com desafios modernos, como redes sociais, inteligência artificial e economia de dados.

Por fim, a trajetória histórica de proteção de dados no Brasil evidencia um movimento contínuo de amadurecimento institucional e normativo, que culmina em um sistema robusto, multifacetado e constitucionalmente estruturado. Da criminalização primária da violação de correspondências em 1940 a constitucionalização da proteção de dados em 2022, passando pela criação da LGPD e ANPD, o país consolidou um arcabouço jurídico alinhado aos mais elevados padrões internacionais, especialmente o modelo europeu inaugurado pelo GDPR.

Trata-se de evolução que reflete não apenas transformações tecnológicas e sociais, mas, sobretudo, o reconhecimento da privacidade e da autodeterminação informativa como pilares da cidadania contemporânea e da vida digital democrática.

2.2 INFLUÊNCIA DO CRESCIMENTO TECNOLÓGICO NA PROTEÇÃO DE DADOS

A evolução tecnológica, impulsionada principalmente pelo surgimento da internet, transformou radicalmente as formas de interação humana, comunicação e consumo de informações. Desde a sua criação nos anos 1960 com fins militares, até

se tornar uma infraestrutura global acessada por bilhões de pessoas, a internet passou a desempenhar papel central na sociedade contemporânea. De acordo com Schwab,

> A tecnologia não é uma força externa, sobre a qual não temos nenhum controle. Não estamos limitados por uma escolha binária entre “aceitar e viver com ela” ou “rejeitar e viver sem ela”. Na verdade, tomamos a dramática mudança tecnológica como um convite para refletirmos sobre quem somos e como vemos o mundo. Quanto mais pensamos sobre como aproveitar a revolução tecnológica, mais analisamos a nós mesmos e os modelos sociais subjacentes que são incorporados e permitidos por essas tecnologias. E mais oportunidades teremos para moldar a revolução de uma forma que melhore o estado do mundo (Schwab, 2016, p. 14).

Com isso, a coleta e o tratamento de dados pessoais tornaram-se atividades rotineiras, porém muitas vezes negligenciadas quanto a sua segurança e finalidade. Nesse contexto, a necessidade de regulamentações como a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) tornou-se cada vez mais evidente.

A história da internet teve início com o projeto ARPANET, desenvolvido nos Estados Unidos durante a Guerra Fria, com o objetivo de estabelecer uma rede de comunicação entre centros militares e o Pentágono. A primeira mensagem entre computadores foi enviada em 1969, marcando o início de uma nova era digital. Nos anos seguintes, especialmente a partir da década de 1980, a internet passou a ter usos comerciais e privados, ampliando-se globalmente.

> A internet chegou ao Brasil, em 1988. Isso se deu por meio de uma conexão estabelecida entre um computador do Laboratório Nacional de Computação Científica, da Universidade Federal do Rio de Janeiro (UFRJ), e a rede da Universidade de Maryland, nos Estados Unidos (Silva, DN; 2025, p.06).

Com a crescente popularização da internet - impulsionada, entre outros fatores, pela criação da *World Wide Web*, pelo desenvolvimento de cabos de fibra óptica e pelo surgimento de plataformas digitais como o *Google* e redes sociais - a sociedade passou a operar em um modelo altamente conectado, no qual dados pessoais são inseridos e transferidos constantemente.

Corroborando com esta ideia Silva e Silva (2013, p.02) vem dispor que:

> O crescente uso das tecnologias da informação e da comunicação, em especial da Internet, imprimiu maior dinamicidade às relações econômicas, a participação política e às interações sociais, redesenhando as formas de ser e estar no mundo. Em nenhum outro momento histórico foi tão fácil e rápido acessar informações, produzir e compartilhar conteúdos, comunicar e

> interagir em sites de redes sociais, *blogs e microblogs*, tudo de maneira instantânea. O intenso desenvolvimento capitaneado pelo segmento de Tecnologias da Informação (TI) acelera ainda mais esse processo, pois cada dia são lançados no mercado equipamentos, aplicativos, plataformas e ferramentas que maximizam a experiência de navegação na *web*, o que faz com que o número crescente de pessoas almeje a inclusão digital, ocasionando consequentemente, uma dependência por estes sistemas.

Cadastros, compras online, operações bancárias, localização geográfica, preferências de consumo e interações sociais passaram a compor vastos bancos de dados controlados, na maior parte dos casos, por empresas privadas. Nesse cenário, surgiram também os riscos de uso indevido, vazamento, comercialização indevida ou até mesmo roubo de informações sensíveis.

É justamente nesse ponto que a crítica ao uso descontrolado da tecnologia se evidencia, conforme destacam Barros, Barros e Oliveira (2017, p.09):

> Pode-se afirmar que a internet alavancou o acesso às informações e possibilitou a troca de dados, em diferentes formatos, entre pessoas e organizações. No entanto, não se pode negar que é a organização das empresas e também do poder público em rede que alavancou a invasão da vida privada de clientes e dos cidadãos em busca de dados pessoais.

Essa reflexão mostra que os mesmos agentes que promovem o avanço digital também são os que, em grande medida, expõem os cidadãos à violação da privacidade. A ausência de regulamentação robusta no início da era digital permitiu práticas abusivas por parte de muitas organizações. Empresas passaram a coletar e utilizar dados sem transparência ou consentimento, gerando sérias ameaças à privacidade e à segurança dos indivíduos.

Essa realidade demandou respostas jurídicas proporcionais ao desafio, resultando na promulgação de legislações específicas voltadas à proteção de dados. No Brasil, esse processo culminou na criação do Marco Civil da Internet, que estabelece princípios e garantias para o uso da rede, e posteriormente na Lei Geral de Proteção de Dados Pessoais (LGPD),que entrou em vigor em 2020.

A LGPD representa um marco essencial para garantir que o avanço tecnológico ocorra de forma ética, segura e responsável. A mesma impõe às empresas uma série de obrigações quanto à coleta, armazenamento, compartilhamento e exclusão de dados pessoais, além de prever sanções em casos de vazamento ou uso indevido. O crescimento tecnológico, portanto, embora tenha sido motor de inovação e desenvolvimento, também gerou vulnerabilidades

significativas que exigiram do Estado a formulação de mecanismos legais para a tutela dos direitos fundamentais à privacidade, à intimidade e à autodeterminação informativa.

Assim, percebe-se que a transformação digital, desde o surgimento da internet até os dias atuais, criou um cenário de oportunidades,mas também de riscos. Nesse contexto, a proteção de dados pessoais emerge como um dos principais desafios jurídicos da contemporaneidade, exigindo das empresas não apenas responsabilidade legal, mas também ética na gestão da informação dos usuários.

2.3 RELEVÂNCIA DA PROTEÇÃO DE DADOS NO BRASIL

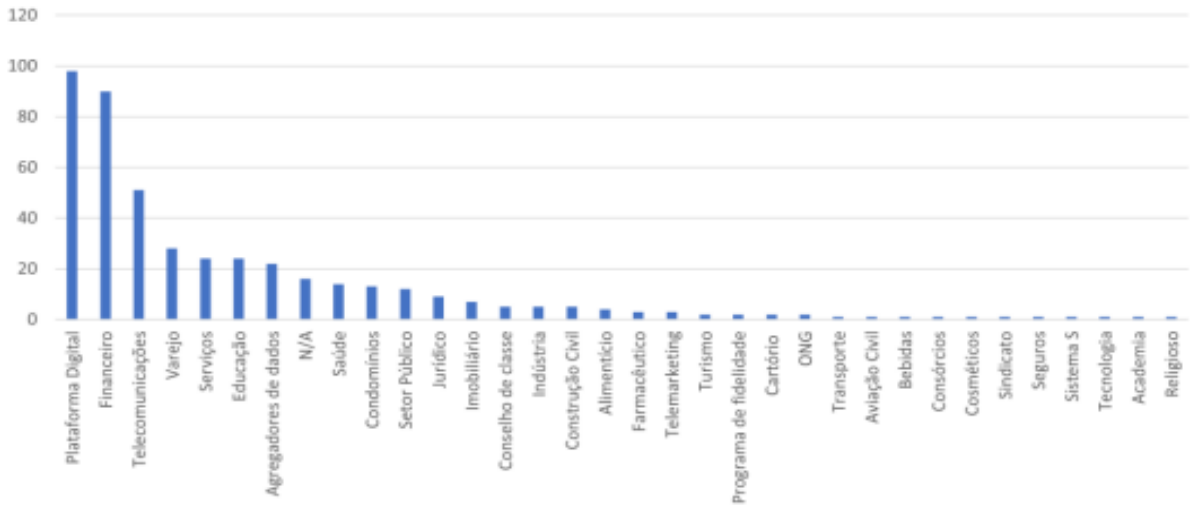
Após a promulgação da Lei Geral de Proteção de Dados Pessoais, o Brasil passou a registrar uma série de incidentes relacionados ao vazamento de dados pessoais. O maior vazamento de dados da história ocorreu em 20 de janeiro de 2021.

Segundo Belli (2021, p.01), no portal FGV, as bases de dados disponíveis – de graça ou à venda – incluem nomes, Cadastros de Pessoa Física (CPF), fotos de rostos, endereços, números de telefone, scores de crédito, salários e mais. Foram expostos os dados de 223 milhões de brasileiros. Esse número pode soar estranho, considerando que a população brasileira é de aproximadamente 210 milhões de pessoas, mas isso ocorre porque os conjuntos de dados vazados incluem também os dados pessoais de milhões de indivíduos falecidos. 104 milhões de registros de veículos também estão disponíveis. As 37 bases de dados à venda incluem literalmente todos os tipos de dados pessoais que se possa imaginar, e muitos mais que ninguém imaginaria. Esses incluem o número da identidade,estado civil, uma lista de todos os parentes de primeiro grau (pais,filhos, irmãos, cônjuge), endereço residencial completo (incluindo latitude e longitude), score de crédito, número do Título de Eleitor, profissão e até mesmo um *link* para o perfil no *LinkedIn*.

Desde a promulgação da lei, diversos setores sofreram incidentes de vazamentos de dados pessoais, sendo possível destacar alguns setores que foram alvo de incidentes significativos. Segundo o relatório do ciclo de monitoramento de 2022, disponibilizado pela ANPD (2022, p.08), as plataformas digitais foram o setor com maior presença de petições de titular, totalizando 96 requerimentos (21,2% do

total). O setor Financeiro ficou em segundo lugar, com 90 (19,9%), seguido pelas Telecomunicações, com 51 (11,2%). Para além desses, é oportuno citar Varejo, com 28 (6,1%); e Agregadores de Dados, com 26 processos (5,7%).

Figura 3 - Petições de titular recebidas por setor - 2022.



Fonte: ANPD (2022, SP).

Os requerimentos são fontes fundamentais de dados que subsidiam as ações de fiscalização. Nesse contexto, as informações que chegam por meio de denúncias e petições de titulares são recebidas, analisadas e transformadas em dados úteis, como o gráfico acima. Analisando rapidamente a figura, vê-se que o setor financeiro é o segundo com mais denúncias sobre vazamento de dados atualmente no país, ficando atrás somente das plataformas digitais.

Além da análise setorial, os dados também revelam um crescimento progressivo dos comunicados de incidentes de segurança recebidos pela ANPD desde 2021, evidenciando a aplicação da vulnerabilidade no tratamento de dados no Brasil:

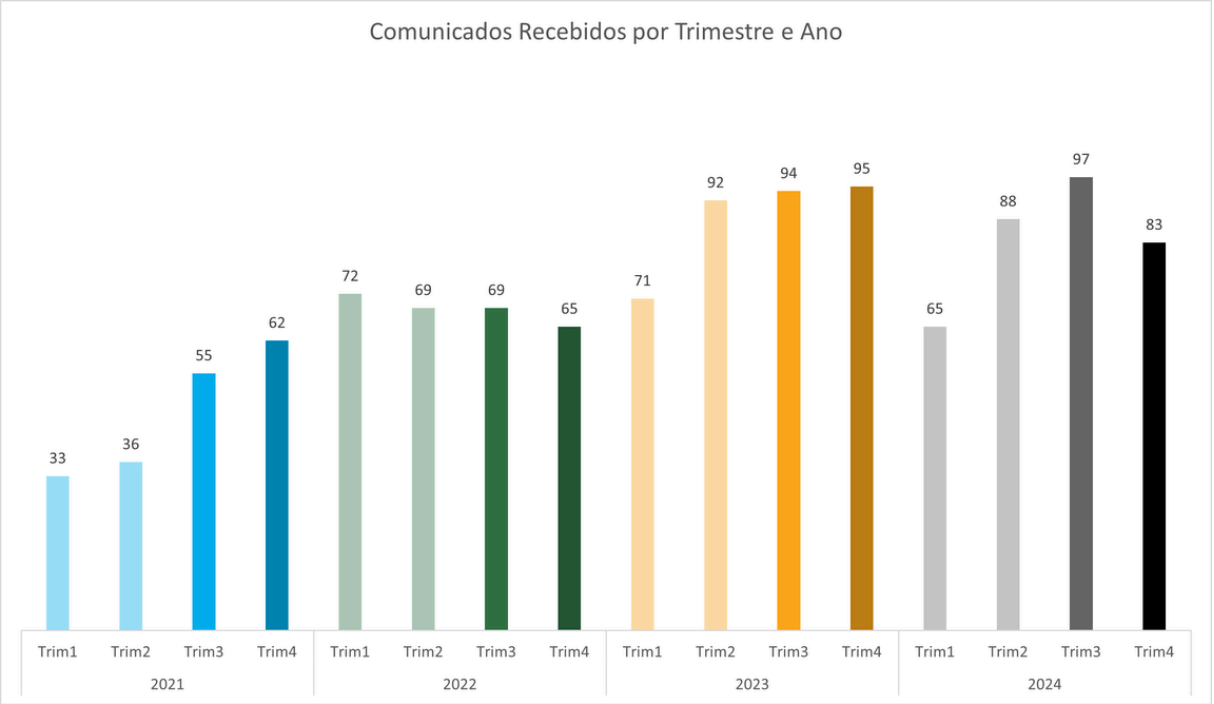
Figura 4 - Comunicado de incidente de segurança recebidos pela ANPD (2021-2024).

Ano	Comunicados no Ano	Acumulado desde 2021
2021	186	186
2022	275	461
2023	352	813
2024	333	1146

Fonte: ANPD (2024,SP).

A análise detalhada por trimestre reforça essa tendência, demonstrando que os incidentes de dados pessoais não apenas aumentaram em volume, mas também de forma contínua ao longo dos anos, com picos expressivos em determinados períodos:

Figura 5 - Comunicados recebidos por trimestre e ano (2021-2024).



Fonte: ANPD (2024,SP).

Outro aspecto relevante é a natureza dos incidentes de dados pessoais reportados. Em 2023 e 2024, os ataques de *ransomware*, a exploração de vulnerabilidades em sistemas de informação e o roubo de credenciais por meio de

engenharia social estiveram entre os eventos mais recorrentes.

A diversidade dos incidentes evidencia que as ameaças não se restringem a ataques externos, mas incluem também falhas operacionais e descuidos no tratamento da informação, como envio incorreto de dados, divulgação indevida ou perda de dispositivos eletrônicos.

A Lei Geral de Proteção de Dados Pessoais estabelece uma série de responsabilidades para empresas e instituições financeiras no que diz respeito à proteção dos dados de seus clientes. Quando ocorre um vazamento, a responsabilidade é clara: as empresas devem ser responsabilizadas pelos danos causados, incluindo o impacto financeiro nas vítimas, e podem ser penalizadas severamente pela ANPD.

Os precedentes têm demonstrado que a responsabilização das instituições financeiras é um reflexo da importância que o Brasil tem dado à proteção de dados pessoais e à segurança digital. Um exemplo recente e impactante dessa realidade foi o ataque *hacker* ocorrido em julho de 2025 à empresa de tecnologia C&M *Software*, especializada em serviços para o setor financeiro. Segundo a Polícia Civil de São Paulo:

> João Nazareno Roque, de 48 anos, era operador de TI da C&M *Software* e foi cooptado para fornecer dados internos e credenciais da empresa ao grupo criminoso. Este grupo, composto por pelo menos quatro pessoas, se passou pela instituição BMP (uma das clientes da C&M) e emitiu ordens falsas de Pix para outras empresas (Alves, 2025, p.02).

Utilizando essas informações, os criminosos emitiram ordens falsas de Pix e desviaram mais de R$ 540 milhões de instituições como a BMP. As operações de Pix foram suspensas temporariamente, e diversas instituições, incluindo Banco Carrefour, Banco Paulista e até uma organização religiosa, foram atacadas. A Polícia informou ainda que:

> O ataque afetou o ambiente de mensageria operado por um Provedor de Serviços de Tecnologia da Informação (PSTI), o que resultou na suspensão temporária das transações via Pix em diversas instituições financeiras (Alves, 2025, p.03).

Esse episódio reforça a compreensão de que as ameaças não são apenas externas, mas muitas vezes envolvem fraudes internas e abusos de confiança, o que demonstra a necessidade de políticas de segurança mais robustas, aliadas a uma cultura organizacional que valoriza a proteção de dados como eixo estratégico. Além

disso, evidencia a complexidade da responsabilização em cadeias de proteção de serviços, especialmente quando empresas terceirizadas operam estruturas sensíveis.

Desse modo, resta claro a relevância jurídica do tema, especialmente diante do crescente número de incidentes de dados pessoais que vêm impactando diretamente os direitos fundamentais dos titulares, como a privacidade e a segurança da informação. A LGPD consolidou um novo paradigma normativo no ordenamento jurídico brasileiro, impondo obrigações específicas aos agentes de tratamento e conferindo protagonismo à Autoridade Nacional de Proteção de Dados no exercício fiscalizatório.

3 A QUALIFICAÇÃO JURÍDICA DA FISCALIZAÇÃO DE DADOS POR PARTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD

A fiscalização do tratamento de dados pessoais constitui um dos pilares para a efetividade da proteção da privacidade no Brasil. Mais do que um mecanismo de controle, trata-se de uma atividade de natureza jurídica que assegura a observância dos princípios, direitos e deveres previstos na Lei Geral de Proteção de Dados Pessoais. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) emerge como órgão central responsável por harmonizar a aplicação da legislação, conciliando o dever de zelar pela tutela dos titulares com a necessidade de orientar agentes de tratamento e promover a cultura de proteção de dados no país.

A qualificação jurídica dessa fiscalização revela-se portanto indispensável para compreender os limites e alcance da atuação da ANPD, bem como os reflexos práticos de sua intervenção nas esferas públicas e privadas.

3.1 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD: ATRIBUIÇÕES

Em tempos de crescente digitalização e circulação massiva de informações pessoais, a existência de estruturas institucionais capazes de garantir a efetividade das normas regulatórias tornou-se indispensável. Com isso foi criada a Autoridade Nacional de Proteção de Dados (ANPD), que trata de:

> uma importante figura para a garantia da eficácia e aplicação prática das normas trazidas com a regulação de proteção de dados no Brasil. Trouxe mais segurança e estabilidade para a futura aplicação da lei Geral de Proteção de Dados. Não basta ter uma lei de proteção de dados pessoais, é preciso educar, capacitar, por isso a importância da ANPD (Garrido, 2020, p.12).

Embora a LGPD previsse, em seu texto original, a criação de uma entidade responsável por fiscalizar a regulamentar a aplicação da referida lei, a Autoridade Nacional de Proteção de Dados foi de fato instituída apenas com a Medida Provisória nº 869/2018, publicada em 27 de dezembro de 2018, posteriormente convertida na Lei nº 13.853/2019, sancionada em 8 de julho de 2019. Inicialmente vinculada à Presidência da República, a ANPD foi posteriormente transformada, pela Lei nº 14.460/2022, em uma autarquia de natureza especial, com maior independência administrativa, técnica e financeira.

A atuação da ANPD visa assegurar a correta implementação da LGPD, promovendo não apenas a fiscalização e aplicação de sanções, mas também ações educativas, orientativas e cooperativas. Para Garrido (2020, p.62), a ANPD está incumbida de tornar a LGPD mais clara, acessível e ajustável para a realidade do Brasil pós-pandemia, tanto para os titulares de dados quanto para os agentes de tratamento, garantindo maior segurança jurídica às transações que envolvem o tratamento das informações pessoais.

Entre suas competências principais, previstas no Art. 55-J da LGPD, estão: a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais, a fiscalização de agentes de tratamento de dados, a aplicação de sanções administrativas, o incentivo a boas práticas e normas técnicas, além da promoção de cooperação internacional na área.

A ANPD também desempenha papel orientador, conforme destaca Garrido (2020, p.200):

> Os agentes de tratamento devem ser definidos a partir de seu caráter institucional, não sendo considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento.

Essa compreensão é fundamental para evitar confusões conceituais na aplicação da LGPD e para delimitar corretamente as responsabilidades dentro de uma organização.

O funcionamento efetivo da ANPD foi regulamentado pelo Decreto nº 10.474/2020, de 26 de agosto de 2020, aprovou a sua estrutura regimental e organização interna. A estrutura é composta por órgãos como o Conselho Diretor, a Ouvidora, a Corregedoria, unidades técnicas e administrativas, e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) - este último com caráter consultivo e participação plural da sociedade.

Assim, a criação e a evolução da ANPD representam um passo decisivo no fortalecimento da governança de dados no Brasil, aproximando o país de padrões internacionais de proteção da privacidade e dos direitos fundamentais em ambientes digitais, especialmente em um cenário pós-pandêmico de crescente digitalização e vulnerabilidade informacional.

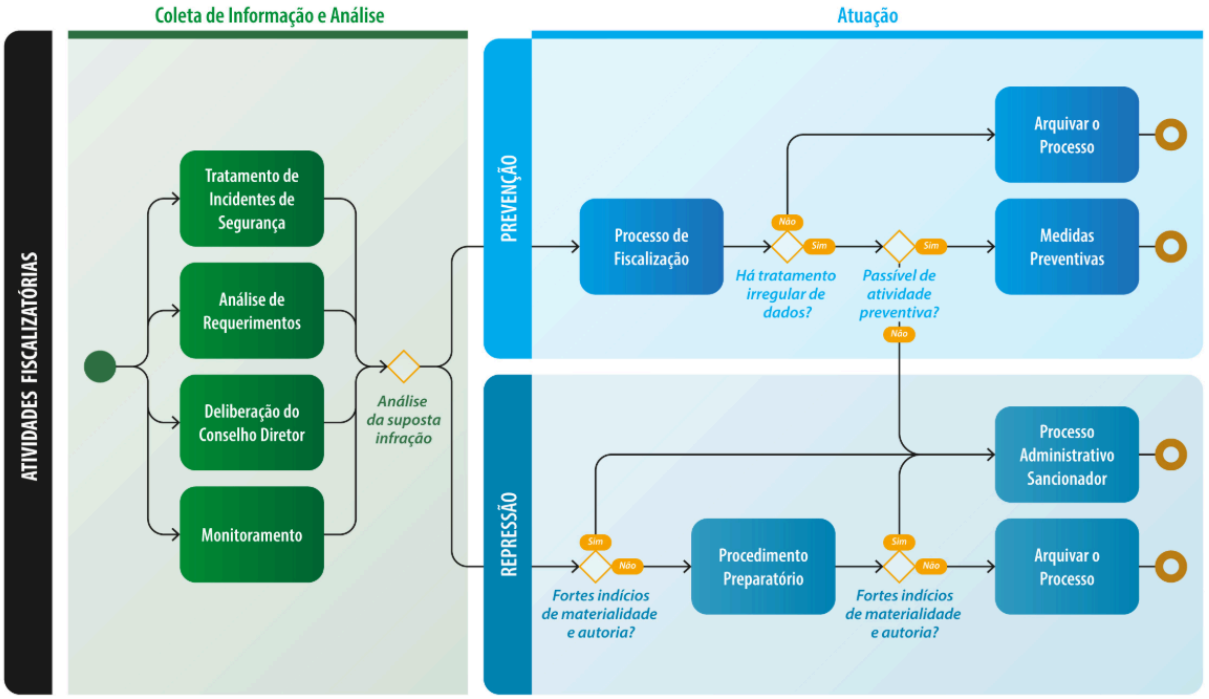
3.2 SANÇÕES APLICÁVEIS RESULTANTE DA FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A atuação fiscalizatória da Autoridade Nacional de Proteção de Dados foi estruturada de maneira progressiva, a fim de conferir segurança jurídica e clareza aos agentes de tratamento quanto às consequências do cumprimento da Lei Geral de Proteção de Dados Pessoais. Nesse sentido, dois marcos normativos se destacam: a Resolução CD/ANPD nº 1, de outubro de 2021, e a Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

A Resolução nº 1/2021 estabelece o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, funcionando como procedimental para a atuação da ANPD. Nela foram definidos os instrumentos de fiscalização, as fases do processo sancionador e as garantias processuais asseguradas aos investigados, como contraditório e ampla defesa. O regulamento deixa claro que a fiscalização não se limita à imposição de sanções, mas compreende também atividades de monitoramento, orientação e prevenção, revelando o caráter educativo da autoridade.

O procedimento fiscalizatório segue um fluxo estruturado que contempla tanto medidas preventivas quanto repressivas. Na esfera preventiva, o processo busca verificar se há tratamento irregular de dados e, sendo o caso, aplicar medidas corretivas antes mesmo da instauração de sanções. Já na esfera repressiva, a ANPD pode instaurar procedimento preparatório e, havendo fortes indícios de materialidade e autoria, dar início ao processo administrativo sancionador. O quadro a seguir, elaborado pela Autoridade, sintetiza esse caminho, desde a coleta de informações e análise de suposta infração até a eventual aplicação de medidas preventivas ou sanções administrativas:

Figura 6 - Atividades fiscalizatórias.



Fonte: ANPD (2021,SP).

Além disso, a resolução detalhou as etapas do processo administrativo, os prazos, os meio de defesa e os critérios formais para instauração de procedimentos sancionatórios, aplicando-se subsidiariamente a Lei nº 9.784/1999 - que estabelece as normas básicas sobre o processo administrativo no âmbito da Administração Pública Federal.

Já a Resolução nº 4/2023 complementa e aprofunda a atuação sancionadora da ANPD ao aprovar o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Se a Resolução anterior criou o arcabouço procedimental, a presente Resolução trouxe os parâmetros concretos para a dosimetria das penalidades, fixando critérios objetivos para calcular o valor-base das multas e para graduar a severidade das sanções.

Entre esses critérios estão:

> Art. 7º Na definição da sanção, devem ser considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência específica;
> VI - a reincidência genérica;
> VII - o grau do dano, nos termos do Apêndice I deste Regulamento;
> VIII - a cooperação do infrator;

> IX - 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 a LGPD;
> X - a adoção de política de boas práticas e governança;
> XI - a pronta adoção de medidas corretivas; e
> XII - a proporcionalidade entre a gravidade da falta e a intensidade da sanção (Brasil. LGPD, 2018, p.04).

Além disso, o regulamento disciplina a aplicação de todas as sanções previstas no Art.52 da LGPD, como advertências, multas simples ou diárias, bloqueio e eliminação de dados pessoais, suspensão parcial das atividades de tratamento e até a proibição total da atividade.

Ao se comparar as duas resoluções, percebe-se que elas exercem funções complementares no sistema regulatório brasileiro. Enquanto a Resolução nº 1/2021 fixou o “como” do processo sancionador - ou seja, as regras procedimentais, prazos, instâncias e garantias processuais -, a Resolução nº 4/2023 definiu o “quanto” e o “em que medida”, ao regulamentar a dosimetria das sanções, estabelecendo critérios de proporcionalidade e razoabilidade para a aplicação das penalidades. Nesse sentido, pode-se afirmar que a primeira resolução cuidou da estrutura formal da atuação fiscalizatória da ANPD, ao passo que a segunda tratou do conteúdo material da sanção, preenchendo uma lacuna essencial para que a LGPD pudesse ser aplicada de forma efetiva.

Em síntese, a Resolução nº 1/2021 representa o marco inicial da capacidade sancionadora da ANPD, ao instituir regras de procedimento e fiscalização, enquanto a Resolução nº 4/2023 representa a etapa de maturidade, ao estabelecer critérios objetivos de dosimetria que evitam arbitrariedades e reforçam a segurança jurídica. Ambas, portanto, compõem um binômio fundamental: de um lado, a previsibilidade quanto ao processo; de outro, a previsibilidade quanto ao resultado, o que fortalece a credibilidade da autoridade e o previsibilidade quanto ao resultado, o que fortalece a credibilidade da autoridade e o próprio regime da proteção de dados pessoais no Brasil.

Além das regulamentações procedimentais e de dosimetria trazidas pelas Resoluções nº 1/2021 e nº 4/2023, é imprescindível observar o rol de sanções administrativas previsto diretamente na LGPD, em seu Art.52. O dispositivo elenca medidas que variam em gravidade e impacto, permitindo à ANPD aplicar desde advertências, de caráter eminentemente pedagógico, até sanções mais severas,como multa simples ou diárias, publicização da infração, bloqueio ou

eliminação de dados de tratamento de dados. Esse leque normativo garante à autoridade um conjunto de instrumentos flexíveis, adaptáveis à gravidade da conduta e ao potencial risco para os direitos dos titulares.

Para que as sanções sejam aplicadas de maneira proporcional e razoável, a LGPD estabeleceu, em seu §1º do mesmo artigo, critérios orientadores que são tal qual os trazidos pela Resolução nº 4/2023 em seu Art.7º. A Resolução nº 4/2023 veio justamente operacionalizar esses parâmetros, fornecendo um sistema objetivo de dosimetria que reduz a margem de subjetividade da autoridade ao fixar as penalidades.

Outro aspecto relevante é a função pedagógica e dissuasória das sanções. A ANPD tem reiterado que sua atuação não deve ser interpretada exclusivamente como repressiva, mas também como instrumento para induzir mudanças de comportamento e difundir a cultura de proteção de dados. Assim, sanções como advertência e publicização da infração ganham especial importância, pois além de penalizar, produzem efeito educativo e reputacional que contribui para a prevenção de novas violações.

Não se pode deixar de mencionar, entretanto, os limites da atuação sancionatória da ANPD, a LGPD lista alguns:

> - multa simples, de até 2% (dois por cento) do faturamento da empresa, limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> - multa diária,dentro do limite total citado; [...] (Brasil. LGPD,2018,p.16).

Ainda que esses valores sejam expressivos, para grandes conglomerados econômicos, tais limites podem não ter caráter verdadeiramente dissuasório. Por outro lado, para pequenas e médias empresas, tais sanções podem representar risco à continuidade das atividades, o que exige da ANPD cautela ao aplicar seus poderes regulatórios.

Por fim, cabe observar que a prática sancionatória da ANPD ainda se encontra em fase de consolidação. Os primeiros processos administrativos começaram a ser instaurados apenas em 2023, e a expectativa é que, com a entrada em vigor do Regulamento de Dosimetria, a aplicação de multas financeiras relevantes se intensifique com o passar dos anos.

Dessa forma, observa-se que a Autoridade Nacional de Proteção de Dados exerce papel central na consolidação do regime jurídico de proteção de dados no

Brasil, não apenas como órgão sancionador, mas também como agente orientador e educativo. A estruturação de seus processos fiscalizatórios e a definição de critérios objetivos para a aplicação de sanções consolidam um sistema normativo mais previsível, equilibrado e transparente.

Com isso, a ANPD se torna o elo entre a teoria da proteção de dados e sua aplicação prática, garantindo que os princípios da Lei nº 13.709/2018 sejam efetivamente observados por todos os agentes de tratamento.

Superada a análise da função fiscalizatória da Autoridade, a próxima seção dedica-se ao exame das formas de proteção asseguradas pela LGPD, suas lacunas legislativas e os fundamentos jurídicos que sustentam sua aplicação, bem como, debater os fundamentos teóricos da responsabilidade civil e analisar a responsabilidade das empresas nos casos de incidentes de dados pessoais, incluindo precedentes, atuação da ANPD e estudo de casos.

4 A PROTEÇÃO DE DADOS NA FORMA DA LEI Nº 13.709/2018

A consolidação da Lei Geral de Proteção de Dados Pessoais - Lei n º 13.709/2018 - representa o ponto culminante de um longo processo de amadurecimento jurídico, tecnológico e institucional em torno da tutela da privacidade no Brasil. Após a contextualização histórica de evolução da proteção de dados no cenário internacional e nacional, bem como análise da influência do avanço tecnológico e da relevância prática da fiscalização exercida pela Autoridade Nacional de Proteção de Dados (ANPD), torna-se indispensável examinar a própria estrutura normativa da LGPD.

Essa seção dedica-se a compreender como a lei organiza os mecanismos de proteção ao titular, quais são seus fundamentos e até que ponto suas disposições atendem plenamente às demandas contemporâneas de segurança e transparência informacional, bem como entender a responsabilidade das empresas nos casos de incidentes de dados pessoais.

Busca-se portanto, não apenas descrever a proteção conferida pela legislação, mas também identificar suas lacunas e desafios na efetivação dos direitos fundamentais à privacidade e à autodeterminação informativa e analisar a responsabilidade atribuída às empresas nos casos de incidentes de dados pessoais.

4.1 PROTEÇÃO ADVINDA DA LEI Nº 13.709/2018

No decorrer dos anos, a sociedade passou por diferentes modelos organizacionais e econômicos, em que cada ciclo foi marcado pela presença de um fator determinante para o seu desenvolvimento. Após a Segunda Guerra Mundial, com os avanços dos meios computacionais e da tecnologia da informação, tornou-se evidente a importância que os dados pessoais passaram a representar para o funcionamento das instituições públicas e privadas. O uso massivo de informações tornou-se essencial não apenas para fins administrativos e comerciais, mas também como instrumento de poder e de influência social.

Como destacam Silva e Silva (2013, p.02), o crescimento da tecnologia da informação e da comunicação, sobretudo a Internet, “imprimiu maior dinamicidade às relações econômicas, à participação política e às interações sociais, redesenhando as formas de ser e estar no mundo”. Essas transformações fizeram

surgir uma dependência crescente das fontes de dados pessoais, em especial em razão das transações digitais e do comércio eletrônico. Nesse cenário, a informação tornou-se o insumo central da economia contemporânea, exigindo um novo paradigma jurídico voltado à proteção da privacidade e da autodeterminação informativa.

Foi nesse contexto que se instituiu, em 14 de agosto de 2018, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Ela dispõe sobre o tratamento de dados pessoais tanto no meio físico quanto digital, aplicando-se a pessoas físicas e jurídicas, públicas e privadas. A LGPD surgiu como resposta à fragmentação normativa até então existente - um mosaico de leis setoriais que, muitas vezes, gerava insegurança jurídica e dificultava a competitividade do país em um cenário global cada vez mais orientado pela economia digital.

O Art.1º da referida lei estabelece que seu objetivo principal é "[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Brasil. LGPD,2018, p.01). Contendo os seus fundamentos impostos no Art.2º, o qual estabelece:

> 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 (Brasil. LGPD, 2018, p.01).

Assim, percebe-se que a LGPD tem base constitucional, dialogando diretamente com o Art.5º, incisos X e XII, da Constituição Federal, que asseguram a inviolabilidade da vida privada e das comunicações.

Para Cots e Oliveira (2019,p.49), "a observância da privacidade concerne no fato de possibilitar que os indivíduos exerçam o controle sobre o que é permitido na sua vida pessoal", o que reforça a noção de autodeterminação informativa como direito essencial. Em complemento, os autores sustentam que a LGPD oferece ao titular o poder de decisão sobre o tratamento de seus dados, impondo ao controlador o dever de transparência e de informação clara quanto à finalidade de coleta.

Dessa forma, a LGPD se apresenta como a guardiã jurídica da privacidade no Brasil, conferindo proteção contra incidentes de dados pessoais, uso indevido e tratamento abusivo de informações pessoais. Como observa Menezes e Colaço (2019), sua aplicabilidade é ampla, incidindo sobre qualquer operação de tratamento de dados realizada no território nacional, independente do meio utilizado, do local da sede do controlador ou da origem dos dados, desde que o titular se encontre no Brasil no momento da coleta.

Essa abrangência reflete a maturidade normativa e a busca por uma cultura de proteção efetiva de dados pessoais no país.

4.2 LACUNAS DO LEGISLADOR

Apesar de representar um avanço jurídico notável, a Lei nº 13.709/2018 (LGPD) ainda apresenta lacunas que desafiam sua plena efetividade e a consolidação de um sistema nacional de proteção de dados plenamente equivalente aos padrões internacionais. Sua formulação ocorreu em um contexto de intensa pressão social e política para modernizar a legislação brasileira, o que resultou em algumas omissões e ambiguidades interpretativas.

Uma das principais críticas refere-se à ausência de definição precisa sobre o que configura “legítimo interesse” em hipóteses de interesse público ou interesse do controlador. Essa indefinição permite interpretações amplas e, por vezes, conflitantes, especialmente em operações que envolvam o setor público e grandes bases de dados sensíveis.

Além disso, a falta inicial de regulamentação clara sobre as sanções administrativas e critérios de dosimetria comprometeu, por um período de tempo, a atuação sancionatória da ANPD, situação que foi posteriormente corrigida com a edição das Resoluções nº 1/2021 e nº 4/2023, já analisadas na seção anterior.

Outro ponto importante diz respeito à posição do Brasil no cenário internacional da proteção de dados. A LGPD foi inspirada diretamente no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, considerado o modelo mais avançado do mundo, mas ainda não havia,até recentemente, o reconhecimento formal do país como detentor de um nível de proteção adequado para o livre fluxo internacional de informações. Essa ausência limitava a

competitividade das empresas brasileiras que dependem de transferências transfronteiriças de dados.

Contudo, em setembro de 2025, “a Comissão Europeia divulgou a versão preliminar da decisão de adequação que reconhece o Brasil como país com nível de proteção de dados pessoais equivalentes ao europeu” (INPD,2025, p.01). Essa decisão representa uma etapa decisiva no processo de harmonização entre os dois regimes jurídicos e indica que o país se encontra em fase avançada de consolidação institucional e normativa. A ANPD, por sua vez, também está em processo de deliberação interna sobre a adequação recíproca da União Europeia, conforme previsto em seu Regulamento de Transferência Internacional de Dados, o que demonstra um movimento de integração bilateral.

Segundo o diretor-presidente da ANPD, Waldemar Gonçalves, destacou que a negociação reflete um interesse recíproco e duradouro de Brasil e União Europeia em alinhar regimes jurídicos e impulsionar sinergias econômicas, destacando que a harmonização é estratégica para fortalecer as relações comerciais e, ao mesmo tempo, preservar os direitos dos titulares” (INPD,2025, p.02).

Assim, embora o reconhecimento definitivo da adequação ainda depende de etapas formais na União Europeia, como a emissão de parecer pelo Conselho Europeu de Proteção de Dados (EDPB) e a aprovação por um comitê de representantes dos Estados-membros, o avanço sinaliza que o Brasil está muito próximo de ingressar na lista dos países considerados adequados, ao lado de Reino Unido, Canadá, Japão, Coreia do Sul, Argentina e Uruguai.

Quadro 1 - Lista de países com proteção de dados nível GDPR.

País	Decisão de adequação	Lei local
Suíça	26 de julho de 2000	Lei Federal de Proteção de Dados (FADP); Promulgada em 1992; Atualizada em 2023.
Canadá	20 de dezembro de 2001	Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA); Promulgada em 2000.
Argentina	03 de junho de 2003	Lei de Proteção de

		Dados Pessoais (PDPA); Promulgada em 2000.
Guernsey	21 de novembro de 2003	Lei de Proteção de Dados (Bailado de Guernsey); Promulgada em 2001; Atualizada em 2017.
Jersey	21 de novembro de 2003	Lei de Proteção de Dados; Promulgada em 2003; Atualizada em 2018.
Ilha de Man	28 de abril de 2010	Lei de Proteção de Dados. Promulgada em 2002; Atualizada em 2018.
Andorra	19 de outubro de 2010	Lei sobre a Proteção de Dados Pessoais. Promulgada em 2003; Atualizada em 2021.
Ilhas Faroé	08 de dezembro de 2010	Lei de Proteção de Dados Pessoais; Promulgada em 2001; Atualizada em 2020.
Israel	31 de janeiro de 2011	Lei de Proteção à Privacidade (PPL); Promulgada em 1981; Atualizada em 2024.
Uruguai	21 de agosto de 2012	Lei de Proteção de Dados Pessoais e *Habeas Data*; Promulgada em 2008.
Nova Zelândia	19 de dezembro de 2012	Lei de Privacidade; Promulgada em 1993; Atualizada em 2020.

Japão	23 de janeiro de 2019	Lei de Proteção de Informações Pessoais (APPI); Promulgada em 2003; Atualizada em 2022.
Reino Unido	28 de junho de 2021	Lei de Proteção de Dados; Promulgada em 2018; Atualizada em 2025.
República da Coreia	17 de dezembro de 2021	Lei de Proteção de Informações Pessoais (PIPA); Promulgada em 2011; Atualizada em 2025.

Fonte:Elaboração própria com base em Dastra (2024).

Para o país ser considerado adequado segundo a UE, deve ter em sua legislação os seguintes tópicos dispostos:

Quadro 2 - Comparativo entre os requisitos de adequação da GDPR e as disposições.

Critério da GDPR (Art.45).	Exigência europeia.	Dispositivo correspondente na LGPD.	Nível de convergência.	Comentário analítico.
Estado de Direito e direitos fundamentais.	O país deve garantir o respeito aos direitos humanos, à privacidade e à liberdade individuais.	O Art.1º e 2º: proteção da liberdade, privacidade e livre desenvolvimento da personalidade.	Plenamente atendido.	A LGPD se fundamenta na Constituição Federal (Art.5º,X e XII), em sintonia com a GDPR.
Princípios do tratamento de dados.	O tratamento deve seguir princípios como finalidade, proporcionalidade e transparência.	O Art.6º: traz 10 princípios orientadores do tratamento de dados pessoais.	Plenamente atendido.	A LGPD espelha-se quase integralmente nos princípios previstos na GDPR.
Direito dos titulares.	Garantir direitos de: acesso, retificação, exclusão, portabilidade e oposição.	Art.17 a 22: direitos equivalentes, incluindo revisão de decisões automatizadas.	Plenamente atendido.	A LGPD assegura aos titulares amplo controle sobre seus dados.

Base legal para o tratamento.	Exige bases legais legítimas, como consentimento, obrigação legal e interesse legítimo.	Art. 7º: traz 10 bases legais equivalentes às da GDPR.	Plenamente atendido.	Estrutura idêntica às hipóteses de tratamento do Regulamento Europeu.
Transferências internacionais de dados.	Requer garantias adequadas e mecanismos de supervisão.	Arts. 33 a 36: exigem salvaguardas, cláusulas contratuais e autorização da ANPD.	Parcialmente atendido.	O Brasil ainda finaliza o regulamento técnico sobre transferências internacionais.
Fiscalização independente.	Deve existir uma autoridade de supervisão autônoma e tecnicamente independente.	Arts. 55-A a 55-L: criam a ANPD, transformada em autarquia pela Lei nº 14.460/2022.	Plenamente atendido.	A independência da ANPD reforça a confiança regulatória e aproxima o Brasil dos padrões da UE.
Sanções e responsabilização.	Deve haver sanções efetivas e proporcionais.	Arts. 52 a 54: preveem multas, advertências, bloqueio e eliminação de dados.	Plenamente atendido.	A ANPD já aplica penalidades e publica relatórios de fiscalização.
Recursos judiciais e administrativos.	O cidadão deve poder recorrer contra violações.	Arts. 18, §1º, e 42, combinados com o art. 5º, XXXV da CF.	Plenamente atendido.	A LGPD garante o direito de peticionar à ANPD e recorrer ao Judiciário.
Compromissos internacionais.	O país deve aderir a tratados e convenções internacionais de direitos humanos e proteção de dados.	O Brasil é signatário da Convenção Americana de Direitos Humanos (Pacto de San José).	Parcialmente atendido.	O país ainda não aderiu formalmente à Convenção 108+ do Conselho da Europa.
Segurança e prevenção de incidentes.	Devem existir medidas técnicas e administrativas adequadas.	Art. 46: impõe medidas de segurança para proteger dados pessoais.	Plenamente atendido.	Compatível com o art. 32 da GDPR sobre segurança do tratamento.

Fonte: Elaboração própria com base na GDPR (Regulamento UE 2016/679), LGPD (Lei nº 13.709/2018), ANPD (2022) e Comissão Europeia (2025).

De forma geral, o Brasil apresenta alta convergência regulatória com o Regulamento Europeu, atendendo praticamente todos os critérios exigidos para o reconhecimento da adequação internacional. As únicas lacunas em fase de aperfeiçoamento estão relacionadas à formalização dos mecanismos de transferência internacional de dados e à adesão à Convenção 108, que ainda se encontra em análise pela Autoridade Nacional de Proteção de Dados (ANPD).

Esses pontos não impedem o reconhecimento, mas demandam monitoramento contínuo pela União Europeia, prática comum nas decisões de adequação recentes.

O parecer europeu destaca elementos estruturais da legislação brasileira, da Autoridade Nacional de Proteção de Dados (ANPD) e os critérios restritivos para o uso do legítimos interesse como base para tratamentos. Uma vez aprovada de forma definitiva, a decisão será um marco para empresas de ambos os lados.

Para Beatriz Haikal (2025,p.02)

> Isso permitirá que dados pessoais circulem sem barreiras adicionais entre a UE e o Brasil, sendo dispensado qualquer mecanismo adicional previsto no art. 33 da LGPD.

Isso significa a eliminação da necessidade de ferramentas como cláusulas contratuais padrão para cada operação de transferência internacional, reduzindo custos, complexidade jurídica e burocracia para empresas que operam globalmente.

Dessa forma, observa-se que as lacunas legislativas e institucionais da LGPD estão em processo de superação, por meio da atuação contínua da ANPD e da aproximação entre os regimes de proteção europeu e brasileiro.O país caminha para garantir um patamar de equivalência internacional, o que não apenas fortalece a credibilidade do sistema nacional de proteção de dados, mas também aumenta a confiança jurídica e econômica nas operações digitais. Ainda assim, por se tratar de uma estrutura normativa recente, a maturidade regulatória da LGPD depende da consolidação prática de sua aplicação e da evolução das políticas públicas voltadas à educação digital e à cultura de proteção de dados.

4.3 FUNDAMENTOS DA LGPD

A Lei Geral de Proteção de Dados Pessoais estrutura-se sobre os pilares normativos que orientam sua interpretação e aplicação na prática. Antes mesmo de delinear princípios, o legislador estabeleceu fundamentos que refletem a base axiológica da lei.

Conforme dispõe o Art.2º da LGPD, são os fundamentos:

> 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 (Brasil. LGPD,2018,p.01).

Esses fundamentos evidenciam o caráter duplo e equilibrado da Lei, ao mesmo tempo em que protege direitos fundamentais vinculados à personalidade e à dignidade da pessoa humana, também promove ambiente favorável ao desenvolvimento econômico e tecnológico. A partir dessa base, Art.6º da LGPD estabelece que as atividades de tratamento de dados pessoais deve observar a boa-fé e os seguintes princípios:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil. LGPD, 2018, p. 03 - 04).

Esses princípios formam o núcleo ético da proteção de dados. O princípio da finalidade impõe que o tratamento ocorra apenas para propósitos legítimos e previamente informados ao titular. O da adequação assegura que o uso dos dados seja compatível com o contexto e a finalidade informada. Já o da necessidade determina a limitação do tratamento ao mínimo indispensável, evitando excesso e abusos.

O princípio do livre acesso garante ao titular a consulta gratuita e facilitada sobre a forma e duração do tratamento, enquanto o da qualidade dos dados obriga o controlador a assegurar exatidão e atualização das informações. A transparência, por sua vez, obriga que o tratamento seja compreensível e acessível, respeitando os segredos comerciais e industriais.

Os princípios da segurança e prevenção tem papel técnico essencial, impondo medidas de proteção contra acessos não autorizados, perdas ou incidentes de dados pessoais, e estimulando ações proativas para evitar danos futuros. Já o da não discriminação proíbe o uso de dados para fins ilícitos ou abusivos, como práticas de exclusão social, racial ou política. Por fim, o princípio da responsabilização e prestação de contas impõe que o agente de tratamento comprove a adoção de medidas eficazes para garantir a conformidade com a lei.

Como explica Santos (2019), esses princípios funcionam como “instrumentos de balizamento ético e jurídico”, assegurando que a coleta e o uso de dados ocorram de forma legítima e transparente. De modo semelhante, Teixeira (2019) ressalta que o princípio da finalidade é essencial para impedir que informações pessoais sejam utilizadas para propósitos diversos dos originalmente consentidos, prevenindo práticas abusivas.

Portanto, a LGPD consolida um modelo jurídico equilibrado entre o desenvolvimento econômico e a proteção da dignidade humana, buscando assegurar que a inovação tecnológica ocorra à custa da privacidade. Sua aplicação efetiva depende não apenas da atuação da ANPD, mas também da conscientização

social e da responsabilidade das instituições em promover uma cultura sólida de governança de dados.

Além disso, a Lei Geral de Proteção de Dados Pessoais adota uma lógica normativa que não se limita à enunciação formal de princípios, mas demanda sua efetiva concretização prática, especialmente por meio de políticas de governança e mecanismos de responsabilização preventiva. Nesse contexto, destaca-se o conceito de *accountability,* ou responsabilização proativa, pelo qual os agentes de tratamento devem não apenas cumprir a lei, mas demonstrar, documentalmente, que adotam medidas de controle, prevenção e gestão de riscos.

A aplicação desses princípios se materializa diretamente nos direitos dos titulares previstos no Art.18 da LGPD, como acesso, correção, portabilidade, anonimização e eliminação de dados. Assim, a dimensão principiológica da lei não é meramente teórica, mas serve como parâmetro de conformidade institucional, sendo referência obrigatória tanto para o Poder Judiciário quanto para a atuação da ANPD.

Com efeito, a Autoridade Nacional de Proteção de Dados desempenha papel essencial na concretização desses valores, editando guias, manuais, regulamentos e aplicando sanções que reforçam a cultura de proteção de dados. A ANPD atua como órgão regulador e educativo, promovendo a transformação da LGPD em prática organizacional, e não apenas em norma aberta.

Portanto, observa-se que a LGPD estrutura um modelo principiológico cuja efetividade depende da articulação entre deveres normativos, fiscalização estatal e responsabilidade jurídica dos agentes de tratamento. Essa dimensão se revele especialmente relevante nos casos de incidentes de segurança e vazamento de dados pessoais, que exigem análise criteriosa sob a ótica civil, administrativa e, em alguns casos, penal - matéria que será aprofundada, quando se examinará a configuração da responsabilidade civil e os mecanismos de reparação aplicáveis.

4.4 RESPONSABILIDADE CIVIL NOS INCIDENTES DE DADOS PESSOAIS

A consolidação da Lei Geral de Proteção de Dados Pessoais e o fortalecimento institucional da Autoridade Nacional de Proteção de Dados marcaram um avanço expressivo no cenário jurídico brasileiro ao estabelecer parâmetros claros de governança informacional e proteção da privacidade. Todavia, mesmo com um arcabouço normativo robusto, o risco de incidentes de segurança permanece

latente, e o vazamento de dados pessoais tornou-se um dos maiores desafios contemporâneos no campo da responsabilidade civil. A tutela da privacidade, quando violada, impõe a necessidade de reparação pelos danos decorrentes, exigindo das organizações uma postura diligente, transparente e preventiva.

Neste contexto, será analisada a responsabilidade civil decorrente de falhas no tratamento de dados pessoais, abordando inicialmente seu conceito e fundamentos teóricos, para, em seguida, analisar as hipóteses de tratamento de dados previstas na legislação. Posteriormente, será abordada a responsabilidade das empresas nos casos concretos de vazamento, observando a aplicação dos princípios da boa-fé, da prevenção e reparação integral, finalizando com a análise dos riscos associados ao comércio de dados pessoais, prática que se mostra cada vez mais sensível em uma economia orientada pela informação.

Assim, busca-se compreender não apenas os contornos jurídicos da reparação, mas também o papel ético e social das empresas na proteção dos direitos fundamentais dos titulares de dados.

4.5 CONCEITO DE RESPONSABILIDADE CIVIL

A responsabilidade civil é regida pelo Código Civil brasileiro, especialmente nos Artigos 186 e 927.

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito (Brasil. Código Civil,2002, p. 17).
>
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo (Brasil. Código Civil,2002, p.67).

De acordo com esses dispositivos, quem causar dano a alguém, seja por ação ou omissão voluntária, negligência ou imprudência, fica obrigado a reparar o prejuízo causado que pode ser de ordem material e moral.

A responsabilidade civil também é aplicada em outras áreas do direito. No Código de Defesa do Consumidor, por exemplo, a responsabilidade civil visa proteger os interesses e direitos dos consumidores, que por sua vez são a parte mais vulnerável da relação comercial.

Nesse contexto, a responsabilidade civil se aplica quando um fornecedor de produtos ou serviços causar danos a um consumidor, sendo obrigado a reparar esses danos.

Nessa senda, é importante ressaltar o conceito de culpa. Segundo Oliveira (2019, p.09):

> Para que uma pessoa seja responsabilizada civilmente, é necessário comprovar que ela agiu de forma ilícita ou negligente, ou seja, que houve culpa. No entanto, em algumas situações, a responsabilidade civil pode ser objetiva, ou seja, dispensando comprovação de culpa, como ocorre em acidentes de consumo, por exemplo.

Um ponto essencial para compreender a responsabilidade civil no contexto dos incidentes de dados pessoais é a distinção entre a responsabilidade subjetiva e objetiva. Na responsabilidade subjetiva, exige-se a comprovação de culpa, conforme articulado nos Artigos 186 e 927 do Código Civil. No entanto, em determinadas situações previstas em lei, a responsabilização ocorre de forma objetiva, isto é, independentemente da demonstração de culpa do agente. Nesses casos, basta comprovar o dano e o nexo de causalidade para que surja o dever de indenizar.

Maria Helena Diniz (2021,p.40) em seu livro intitulado “Curso de direito civil brasileiro: responsabilidade civil.*”,* em um trecho traz que:

> O comportamento do agente será reprovado ou censurado quando, ante circunstâncias concretas do caso, se entende que ele poderia ou deveria ter agido de modo diferente. Portanto, o ato ilícito qualifica-se pela culpa. Não havendo culpa, não haverá, em regra, qualquer responsabilidade.
> Logo, a lei impõe a quem o praticar o dever de reparar o prejuízo resultante.

Segundo Maria Helena Diniz (2021,p.64),para haver dano indenizável é imprescindível a ocorrência dos seguintes requisitos:

> a) diminuição ou destruição de um bem jurídico, patrimonial ou moral, pertencente a uma pessoa;
> b) efetividade ou certeza do dano, pois a lesão não poderá ser hipotética ou conjectural;
> c) causalidade, já que deverá haver uma relação entre a falta e o prejuízo causado, ou seja, o dano deverá estar encadeado com a causa produzida pelo lesante;
> d) subsistência do dano no momento da reclamação do lesado;
> e) legitimidade: para que possa pleitear a reparação, precisará ser titular do direito atingido;
> f) ausência de causas excludentes de responsabilidade, porque podem ocorrer danos, que não resultem dever ressarcitório como os causados por caso fortuito, força maior ou culpa exclusiva da vítima.

Outro ponto importante é calcular a estimativa dos danos. Ao ser responsabilizado civilmente, o causador do dano deve reparar o prejuízo sofrido pela vítima.

Essa reparação pode ser feita de diversas formas, como pagamento de uma indenização em dinheiro, restituição de bens ou serviços, entre outros. (Oliveira,2019, p.09).

Desse modo, para que seja caracterizada a responsabilidade civil, é de suma importância a presença de determinados pressupostos, os quais são extraídos em sua maioria do Artigo 186 do Código Civil.

Com isso, resta claro que quem causar dano a outrem de qualquer natureza que for terá a obrigatoriedade de ressarcir os danos causados, garantido assim a justiça e a reparação dos direitos violados.

Diante desse panorama, é possível observar que a responsabilidade civil, ao longo do tempo, evoluiu para atender às novas demandas sociais e tecnológicas. Com o avanço da era digital e a crescente circulação de informações pessoais em meio eletrônico, o conceito clássico de dano passou a abranger também os prejuízos decorrentes da violação de dados e da exposição indevida de informações sensíveis. Assim a responsabilidade civil assume papel central na efetivação da proteção de dados pessoais, funcionando como instrumento de garantia dos direitos fundamentais à privacidade e à segurança da informação.

A doutrina contemporânea evidencia que, com a digitalização e o crescimento exponencial do fluxo de informações, o dano não se limita mais a prejuízos materiais, abrangendo também violações à intimidade, privacidade e honra. Assim, a LGPD reforça os elementos estruturais da responsabilidade civil ao prever dever de reparação em caso de incidentes envolvendo dados pessoais.

A jurisprudência do Superior Tribunal de Justiça (STJ) reforça essa linha interpretativa. No REsp 2121904/SP (2025), a Corte reconheceu que o vazamento de dados sensíveis gera dano moral presumido, dispensando a prova do prejuízo efetivo. A decisão é paradigmática porque consolida o entendimento de que a simples exposição indevida de dados sensíveis — como informações de saúde, bancárias ou biométricas — constitui violação à dignidade e à privacidade, sendo suficiente para caracterizar o dever de indenizar.

> Ementa: CIVIL. RECURSO ESPECIAL. CONTRATO DE SEGURO DE VIDA. RELAÇÃO DE CONSUMO. CÓDIGO DE DEFESA DO

> CONSUMIDOR. LEI GERAL DE PROTEÇÃO DE DADOS. VAZAMENTO DE DADOS SENSÍVEIS. RESPONSABILIDADE OBJETIVA. DANO MORAL PRESUMIDO. RECURSO CONHECIDO EM PARTE. DESPROVIMENTO. 1. Ação de obrigação de fazer c/c indenização por danos morais e materiais, da qual foi extraído o presente recurso especial, interposto em 28/6/2023 e concluso ao gabinete em 22/2/2024. 2. O propósito recursal é definir se, em contrato de seguro de vida, o vazamento de dados sensíveis do segurado gera: (a) dano moral presumido e (b) responsabilização objetiva da empresa seguradora. 3. Inexistência de negativa de prestação jurisdicional. Acórdão do Tribunal de origem devidamente fundamentado para solucionar integralmente a controvérsia submetida à sua apreciação. 4. Não há cerceamento de defesa nas hipóteses em que o julgador resolve a questão controvertida, de forma fundamentada, sem a produção da prova requerida pela parte, em virtude de considerar suficientes os elementos que integram os autos. 5. A matéria que não foi objeto de debate no acórdão recorrido, mesmo após a interposição de embargos declaratórios, não pode ser conhecida por meio de recurso especial. Súmula nº 211/STJ. 6. Cabe ao fornecedor o ônus de comprovar que cumpriu com seu dever de proteger dados pessoais do consumidor, sobretudo quando se tratam de dados sensíveis, nos termos do CDC (arts. 6º, VIII e 14, caput e §3º) e da LGPD (arts. 6º, X, 8º, §2º, 42, §2º e 48, §3º). 7. Há especial proteção legal aos chamados dados pessoais sensíveis: aqueles que, quando revelados, podem gerar algum tipo de discriminação, sobretudo os que incidem 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" (art. 5º, II, da LGPD). 8. O tratamento de dados pessoais sensíveis observa requisitos significativamente mais rigorosos, sobretudo com a exigência, em regra, do consentimento específico e destacado do titular (art. 11 da LGPD). 9. Em contrato de seguro de vida, deve-se empreender um rigoroso esforço para a proteção dos dados pessoais, já que, para sua celebração, a seguradora, para a avaliação dos riscos, recebe dados sensíveis sobre aspectos pessoais, familiares, financeiros e de saúde do segurado. 10. O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, por si só, submete o consumidor a riscos em diversos aspectos de sua vida, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal. **11. Por isso, em seguro de vida, na hipótese de vazamento de dados sensíveis do segurado, verifica-se a responsabilização objetiva da seguradora e a caracterização de dano moral presumido.** 12. Conforme entendimento desta Corte, a revisão da compensação por danos morais só é viável em recurso especial quando o valor fixado for exorbitante ou ínfimo, o que não se constata no recurso sob julgamento. **13. Hipótese em que o acórdão recorrido, ao manter a responsabilização da seguradora, reconheceu que: i) houve vazamento de dados pessoais do consumidor; ii) tais dados são classificados como sensíveis, de modo a abranger informações fiscais, bancárias e sobre a saúde do consumidor; iii) há nexo de causalidade entre o vazamento de dados sensíveis do consumidor e falhas na prestação do serviço pela recorrente, que não atendeu a seu dever de garantir a proteção dos dados sensíveis do consumidor.** 14. Recurso especial parcialmente conhecido e, nessa extensão, desprovido.(REsp 2121904/SP, 3ª Turma, Relator(a) Ministra Nancy Andrighi, 3ª Turma, DJEN 17/02/2025) (Grifo nosso).

No âmbito das relações de consumo, o próprio Código de Defesa do Consumidor estabelece a responsabilidade objetiva do fornecedor por falhas na prestação de serviço (Art.14, do CDC), reconhecendo que o consumidor é a parte mais vulnerável da relação. A LGPD segue a mesma lógica protetiva: seu Art.42

prevê que o controlador ou operador responderá pelos danos decorrentes do tratamento de dados quando descumprir a legislação ou deixar de adotar as medidas de segurança adequadas, reforçando que a reparação independe de comprovação de culpa. Assim, a responsabilidade objetiva se justifica pela própria natureza do risco criado pela atividade de tratamento de dados, que envolve fluxos constantes de informações, vulnerabilidade tecnológica e potenciais impactos significativos sobre direitos fundamentais.

Como observa a doutrina, a responsabilidade civil no âmbito digital cumpre função preventiva e pedagógica, uma vez que desloca o foco da análise para a estrutura de governança e seguranças das empresas, incentivando-as a adotar medidas eficazes para proteção de base de dados. Em outras palavras, o agente que decide realizar tratamento de dados pessoais assume também os riscos inerentes a essa atividade - inclusive de falhas técnicas, ataques cibernéticos e incidentes de dados pessoais. Por isso, uma vez demonstrada a violação dos dados e o prejuízo ao titular, nasce o dever de indenizar salvo se houver causa excludente expressamente prevista em lei, como culpa exclusiva da vítima ou fortuito externo.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) incorporou princípios e obrigações que dialogam diretamente com a responsabilidade civil, estabelecendo parâmetros objetivos para o tratamento adequado das informações e prevendo sanções em casos de descumprimento. A aplicação das normas civis aos incidentes de vazamento de dados representa, portanto, uma ampliação do alcance protetivo da lei, reafirmando o dever das empresas em agir com diligência e boa-fé na gestão das informações que lhes são confiadas.

4.6 HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabeleceu um marco jurídico destinado a proteger a privacidade e assegurar a autodeterminação informativa, condicionando o tratamento de dados pessoais à existência de fundamento legal expresso. Assim, o tratamento não é livre, mas depende de uma base legal prevista em lei, conforme dispõe o Art.7º e 11 da Lei nº 13.709/2018.

Tal sistemática representa um movimento de alinhamento do Brasil aos princípios estruturantes do Regulamento Europeu de Proteção de Dados (GDPR),

reforçando que o uso de dados pessoais deve “ser considerado também a finalidade, a necessidade e a proporcionalidade da utilização dos dados (Teffé, Viola, 2019, p.14).

Ainda, segundo Teffé e Viola (2019), a LGPD cumpre o papel de delimitar claramente as hipóteses autorizadas de tratamento, trazendo segurança jurídica e previsibilidade na relação entre titular e controlador. Os autores enfatizam que a legislação parte da premissa de que os dados constituem um elemento fundamental da personalidade, pois a informação pessoal não é apenas um objeto econômico ou operacional, mas expressão direta da autonomia e da identidade do indivíduo.

Desse modo, qualquer atividade de coleta, armazenamento, compartilhamento ou eliminação de dados deve estar previamente autorizada por base legal e vinculada a uma finalidade legítima.

Em seu Art.7º, a LGPD estabelece hipóteses como o consentimento do titular, o cumprimento de obrigação legal, a execução de contrato, o exercício regular de direitos em processo judicial, a proteção da vida, a tutela da saúde, o legítimo interesse do controlador e a proteção do crédito. Além disso, o tratamento com base no interesse legítimo exige avaliação rigorosa, devendo o controlador demonstrar que não viola direitos fundamentais do titular.

A ANPD (2021,p.06) entende que no contexto de “uma pessoa jurídica, a organização é o agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus representantes ou prepostos”. No caso de dados sensíveis, o Art.11 da LGPD estabelece um regime mais protetivo, permitindo o tratamento apenas em situações excepcionais e justificadas, como consentimento específico, cumprimento de obrigação legal, proteção da vida ou prevenção à fraude. Os dados denominados pessoais sensíveis são os elencados no Art.5º, inciso II, da LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...] (Brasil. LGPD, 2018, p.02).

Segundo Garrido (2020, p.129):

> Os dados sensíveis merecem tratamento especial porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa.

Dessa forma, embora as bases legais incluam essas hipóteses, o núcleo interpretativo da norma permanece na garantia da dignidade da pessoa humana e na imposição de práticas transparentes e seguras.

4.7 ANÁLISE DA RESPONSABILIDADE DAS EMPRESAS EM CASOS DE INCIDENTES DE DADOS PESSOAIS

A responsabilidade civil e o vazamento de dados pessoais é um assunto que faz cada vez mais parte do cotidiano das pessoas. Com o avanço da tecnologia e a crescente utilização da internet, a proteção da privacidade dos dados de seus usuários torna-se de suma importância.

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais (LGPD), é a principal legislação que visa regular e impor responsabilidade para as empresas que manipulam dados pessoais. A responsabilidade das empresas por vazamento de dados está fundamentada majoritariamente na responsabilidade objetiva, prevista no Art.42 da LGPD e no Art. 14 do Código de Defesa do Consumidor, sendo suficiente a comprovação do dano e o nexo causal.

A seguir precedentes do Tribunal de Justiça do Rio Grande do Sul:

> Ementa: RECURSO INOMINADO. PEDIDO DE BALCÃO. CONSUMIDOR. AÇÃO INDENIZATÓRIA POR DANOS MATERIAIS E MORAIS. FRAUDE BANCÁRIA. AUTOR VÍTIMA DE GOLPE. VAZAMENTO DE DADOS PESSOAIS DO CONSUMIDOR DE DENTRO DA INSTITUIÇÃO FINANCEIRA. FALHA NO SISTEMA DE SEGURANÇA QUE PERMITIU A TRANSFERÊNCIA BANCÁRIA FRAUDULENTA. VIOLAÇÃO A LEI 13.709/2018 (LGPD). RESPONSABILIDADE DA INSTITUIÇÃO FINANCEIRA PELA VIOLAÇÃO DA SEGURANÇA DOS DADOS. EMPRÉSTIMO REALIZADO EM NOME DO DEMANDANTE. PARTE RÉ QUE DEIXOU DE ADOTAR MEDIDAS DE SEGURANÇAS - ARTS. 44 E 46 DA LGPD. APLICAÇÃO DO ART. 14 DO CDC. INCIDÊNCIA DA SÚMULA 479 DO STJ. RESPONSABILIDADE OBJETIVA DO BANCO RÉU. NECESSIDADE DE AUTORIZAÇÃO EXPRESSA E CLARA PARA FINS DE DESCONTOS SOB A FORMA DE CONSIGNAÇÃO EM BENEFÍCIO PREVIDENCIÁRIO, PARA TANTO NÃO SE MOSTRANDO SUFICIENTES FOTOS, VIA SELFIES, COMO TÊM SE TORNADO COMUM. RESTITUIÇÃO DOS VALORES INDEVIDAMENTE DESCONTADOS, DIANTE DE ERRO NÃO JUSTIFICÁVEL, AUTORIZA A REPETIÇÃO EM DOBRO, NOS TERMOS DO ART. 42 DO CDC. SENTENÇA DE PARCIAL

> PROCEDÊNCIA MANTIDA. RECURSO DESPROVIDO.(Recurso Inominado, Nº 50058266820238212001, Primeira Turma Recursal Cível, Turmas Recursais, Relator: Patrícia Antunes Laydner, Julgado em: 03-09-2024) (Grifo nosso).

Esse precedente evidencia que, quando há falha interna no sistema de segurança bancária que permite a fraude, presume-se a responsabilidade objetiva das instituições financeiras. O Tribunal reafirma que o vazamento de dados dentro do próprio banco caracteriza fortuito interno e, por isso, impõe o dever de indenizar, nos termos da LGPD e do CDC.

> Ementa: RECURSO INOMINADO. CONSUMIDOR. AÇÃO INDENIZATÓRIA POR MATERIAIS. DANOS FRAUDE BANCÁRIA. AUTOR VÍTIMA DE GOLPE. VAZAMENTO DE DADOS PESSOAIS DO CONSUMIDOR DE DENTRO DA INSTITUIÇÃO FINANCEIRA. FALHA NO SISTEMA DE SEGURANÇA QUE PERMITIU A TRANSFERÊNCIA BANCÁRIA FRAUDULENTA. VIOLAÇÃO A LEI 13.709/2018 (LGPD). RESPONSABILIDADE DA INSTITUIÇÃO FINANCEIRA PELA VIOLAÇÃO DA SEGURANÇA DOS DADOS. PARTE RÉ QUE DEIXOU DE ADOTAR MEDIDAS DE SEGURANÇAS - ARTS. 44 E 46 DA LGPD. APLICAÇÃO DO ART. 14 DO CDC. INCIDÊNCIA DA SÚMULA 479 DO STJ. RESPONSABILIDADE OBJETIVA DO BANCO RÉU. DEVER DE RESSARCIR OS VALORES AO AUTOR. SENTENÇA DE PROCEDÊNCIA MANTIDA. RECURSO DESPROVIDO.(Recurso Inominado, n.º 51564618120228210001, Primeira Turma Recursal Cível, Turmas Recursais, Relator: Patrícia Antunes Laydner, Julgado em: 02-04-2024) (Grifo nosso).

Assim como no julgamento anterior, o Tribunal reforça que a instituição financeira responde objetivamente quando não adota medidas adequadas de segurança previstas nos Arts.44 e 46 da LGPD. A decisão demonstra a uniformidade do entendimento das Turmas Recursais quanto ao dever dos bancos de prevenir incidentes e ressarcir os danos decorrentes da exposição indevida de dados.

> Ementa: RECURSO INOMINADO. CONSUMIDOR. AÇÃO INDENIZATÓRIA POR DANOS MATERIAIS E MORAIS. FRAUDE BANCÁRIA. AUTORA VÍTIMA DE GOLPE. LIGAÇÃO RECEBIDA ORIUNDA DO PRÓPRIO NÚMERO DO BANCO INDICADO NO VERSO CARTÃO. VAZAMENTO DE DO DADOS PESSOAIS DO CONSUMIDOR DE DENTRO DA INSTITUIÇÃO FINANCEIRA. FALHA NO SISTEMA DE SEGURANÇA QUE PERMITIU A TRANSFERÊNCIA BANCÁRIA FRAUDULENTA. APLICAÇÃO DO ART. 14 DO CDC. INCIDÊNCIA DA SÚMULA 479 DO STJ. RESPONSABILIDADE OBJETIVA DO BANCO RÉU. DEVER DE RESSARCIR OS VALORES À AUTORA. SENTENÇA DE PARCIAL PROCEDÊNCIA MANTIDA. RECURSO DESPROVIDO. (Recurso Inominado, n.º 50077392320218210072, Quarta Turma Recursal Cível, Turmas Recursais, Relator: Nara Cristina Neumann Cano Saraiva, Julgado em: 06-10-2023) (Grifo nosso).

O precedente reafirma a mesma linha interpretativa: havendo vazamento de dados que possibilite golpes e transações bancárias não autorizadas, a

responsabilidade do banco é objetiva. A decisão destaca que a fraude originada a partir de informações vazadas dentro da própria instituição financeira confirma a falha no serviço prestado e atrai a incidência da Súmula 479 do STJ.

Ao analisar os precedentes, revela a crescente responsabilização das instituições financeiras quando ocorre o vazamento de dados de seus clientes, especialmente quando tais incidentes de dados pessoais são acompanhados de fraudes e golpes. O Poder Judiciário tem entendido que as instituições devem adotar medidas de segurança robustas, sob pena de responderem civilmente pelos prejuízos causados.

A LGPD impõe obrigações específicas às empresas no tocante à segurança da informação. Os Artigos 44 e 46 dispõem que o tratamento será irregular quando não fornecer a segurança que o titular pode esperar, e que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, destruição ou perda acidental.

> 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;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> [...]
> 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.
> § 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.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (Brasil. LGPD.2018,p.14).

Da mesma forma, o Código de Defesa do Consumidor em seu Art.14, reforça a responsabilidade objetiva do fornecedor de serviços, determinando que o mesmo responde pela reparação dos danos causados ao consumidor por defeitos relativos à prestação de serviços, independentemente da existência de culpa. Essa regra, somada à Súmula 479 do STJ, cria uma base sólida para a responsabilização

civil principalmente das instituições financeiras e de quaisquer controladores de dados que deixem de assegurar o nível de proteção esperado.

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido (Brasil. CDC,1990,p. 04).

> Súmula 479:
> As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias (Brasil. STJ,2012).

No contexto digital, a aplicação dessa responsabilidade assume novas dimensões. A LGPD estabelece, em seu Art.42, que o controlador ou o operador que causa dano patrimonial, moral, individual ou coletivo, em virtude do tratamento de dados pessoais, é obrigado a repará-lo.

> 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.
>
> § 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;
>
> 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 (Brasil. LGPD, 2018, p.14).

Já o Art.43 reforça que os agentes de tratamento só se eximem da responsabilidade se provarem que não realizaram o tratamento que gerou o dano ou que fizeram em conformidade com a lei.

> 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 (Brasil. LGPD,2018,p.14).

No ano de 2024, a ANPD notificou 20 grandes empresas de diversos setores como tecnologia, telefonia, educação, saúde e varejo, entre elas: Dell, Vivo, UniNassau, Clínica Vamos Sorrir, Cacau Show (G1,2024,p.02-03) por descumprirem obrigações fundamentais da LGPD - em especial, a indicação do contato do encarregado pelos tratamentos de dados e também por não disponibilizarem canais de comunicação adequados para atender aos titulares de dados.

A ANPD afirmou que: “se as irregularidades persistirem, as empresas poderão sofrer processos administrativos e penalidades previstas da LGPD, que incluem advertências e multas de até 2% do faturamento da empresa, limitada a R$50 milhões por infração” (G1,2024, p.02).

Como mencionado em seções anteriores a jurisprudência do Superior Tribunal de Justiça (STJ) reforça no REsp 2121904/SP (2025), que o vazamento de dados sensíveis gera dano moral presumido, ou seja, dispensando a prova do prejuízo efetivo. Além disso, é relevante observar que a responsabilidade das empresas não se restringe à reparação posterior, mas envolve um dever de governança preventiva.

No contexto do vazamento de dados, a responsabilidade civil das empresas se estabelece quando ocorre uma violação desses dados, que pode ocorrer por uma falha de segurança, um ataque cibernético ou qualquer outra forma de acesso não autorizada, nesses casos a empresa pode ser responsabilizada pelos danos causados aos titulares dos dados.

De acordo com Souza e Silva (2019):

> A responsabilização das empresas pelos vazamentos de dados pessoais está fundamentada na teoria da responsabilidade civil objetiva, prevista no Código Civil brasileiro. Segundo essa teoria, basta a comprovação da existência do dano e do nexo de causalidade entre a conduta da empresa e o prejuízo sofrido pelo titular dos dados, sem a necessidade de demonstração de culpa por parte da empresa. Ou seja, a empresa é responsabilizada independentemente de ter agido de forma negligente, imprudente ou dolosa.

A própria LGPD adota o conceito de *accountability,* pelo qual o agente deve não apenas cumprir a lei, mas comprovar que adota políticas, controles e medidas

técnicas adequadas para mitigar riscos de incidentes de dados pessoais. Essa obrigação aproxima a atuação empresarial das práticas de *compliance* digital, em que a responsabilidade é tanto jurídica quanto ética.

A Autoridade Nacional de Proteção de Dados tem reforçado, em seus relatórios de fiscalização, que a responsabilidade das empresas deve observar critérios de proporcionalidade e gravidade, conforme definidos na Resolução nº 4/2023, que regulamenta a dosimetria das sanções administrativas. Entre as circunstâncias agravantes estão a reincidência, a natureza dos dados vazados e a ausência de cooperação da empresa durante a apuração. Essa normatização supre a lacuna inicial da LGPD, permitindo uma atuação sancionatória mais efetiva e previsível.

Do ponto de vista econômico e social, os incidentes de dados pessoais geram impacto que transcende a esfera individual dos titulares. A proteção de dados é elemento constitutivo da confiança nas relações digitais, e sua violação afeta não apenas a vítima direta, mas todo o ecossistema de trocas econômicas e informacionais. Assim, o dever de cuidado imposto às empresas é uma extensão da função social da atividade econômica.

Diante desse cenário, a responsabilidade das empresas no caso de incidentes de dados pessoais transcende o aspecto jurídico, assumindo também uma dimensão ética, econômica e reputacional.A proteção da privacidade dos indivíduos não é apenas uma obrigação legal, mas um compromisso essencial para preservar a confiança do público e a integridade das relações comerciais.

O Quadro 3, a seguir, reúne alguns dos principais incidentes de dados pessoais registrados nos últimos anos, permitindo compreender como os princípios da LGPD e da responsabilidade civil vem sendo aplicados na prática e quais lições podem ser extraídas desses episódios.

Quadro 3 - Incidentes de dados pessoais no Brasil e consequências.

Caso	**Ano**	**Entidade/Empresa**	**Pessoas afetadas**	**Tipo de dados vazados**	**Consequências**
Vazamento Netshoes	2018	Netshoes	2 milhões	Nome; CPF; E-mail;	Indenização de R$ 500 mil (MPDFT).

				Histórico de compras.	
Vazamento Enel Osasco	2020	Enel SP	290 mil	Dados cadastrais e consumo.	Procon notificado; Investigação em curso.
Falha no Ministério da Saúde	2020	Ministério da Saúde/SUS	243 milhões	Nome; CPF; Endereço; Telefone.	Investigação interna; Sistemas ficaram fora do ar.
Vazamento de chaves PIX	2021	Banco Central/ Acesso pagamentos	160.147 mil	Nome; CPF; Banco; Agência e conta.	Notificação aos titulares; Investigações e possíveis sanções.
Operação Deepwater	2021	Base nacional	223 milhões	Nome; CPF; Renda; Endereço; Fotos.	Investigação da PF e ANPD; Prisões efetuadas.
Vazamento de chaves PIX	2025	Banco Central / CNJ	11.003.398 milhões	Nome; Nome do banco; Número da agência; Número da Conta.	CNJ reforçou a segurança; Notificou a PF e a ANPD.

Fonte: Elaboração própria com base em Aragão (2022), Máximo (2025).

A análise dos incidentes de de dados pessoais ocorridos no Brasil nos últimos anos evidencia que o risco de violação informacional não se limita ao setor privado tradicional, mas permeia diferentes ramos essenciais da infraestrutura nacional. Os casos estudados envolvem instituições financeiras, órgãos públicos, empresas de varejo digital e concessionárias de serviços essenciais, demonstrando que qualquer organização que trate dados pessoais está sujeita a falhas estruturais ou ataques cibernéticos, exigindo elevado grau de conformidade com a Lei Geral de Proteção de Dados Pessoais.

Entre os incidentes de dados pessoais analisados, observa-se que:

- **Setor financeiro (Banco Central/PIX - incidentes relacionados a instituições bancárias e meios de pagamento):** evidenciou

vulnerabilidade na custódia de dados associados ao sistema financeiro digital, setor considerado crítico. O vazamento expos chaves PIX e dados bancários, reforçando a importância de mecanismos avançados de segurança na infraestrutura nacional;

- **Administração pública e saúde pública (Ministério da Saúde/SUS):** tratou-se do maior volume de dados expostos no setor, o vazamento expos nome, CPF, endereço, fotos. Esse episódio demonstra que órgãos estatais também devem observar rigorosamente os princípios da LGPD e investir em segurança, dado seu papel estratégico e a enorme base populacional sob sua guarda;
- **Setor de comércio eletrônico (e-commerce) - Netshoes:** o vazamento expos nome, CPF, e-mail e histórico de compras. O incidente evidencia a fragilidade de sistemas de varejo digital, segmento que manipula grandes bases de dados e depende diretamente da confiança do consumidor. O acordo de indenização firmado demonstra a aplicação prática do modelo de responsabilização civil, reforçando o caráter sancionatório e pedagógico da LGPD;
- **Serviços essenciais (energia elétrica) - Enel:** o vazamento expos dados cadastrais e consumo. Ao envolver dados de consumidores vinculados a um serviço básico, o vazamento evidencia que concessionárias de serviço público também estão sujeitas a responsabilização. O episódio reforça a necessidade de implementação de políticas rígidas de governança de dados, dada a natureza crítica desses serviços;
- **Vazamento nacional massivo - Operação Deepwater:** o vazamento expos nome, CPF, renda, endereços e fotos. Caso particularmente grave, envolvendo base com mais de 223 milhões de dados, superando a população brasileira. Essa situação demonstra que a circulação e comercialização ilícita de dados é um cria um cenário de fragilidade histórica na proteção de dados pessoais no país.

A diversidade de setores envolvidos - financeiro, saúde pública, varejo digital, concessionária de energia elétrica e administração pública - evidencia que o tratamento de dados é transversal e estratégico exigindo robustez tecnológica,

governança corporativa, resposta rápida a incidentes e postura preventiva permanente. Além disso, confirma-se a tendência de judicialização e responsabilização, em consonância com o modelo de proteção adotado internacionalmente e como o fortalecimento da atuação fiscalizatória da ANPD.

De modo geral, os incidentes de dados pessoais demonstram que a responsabilidade civil das empresas em casos de vazamento de dados no Brasil se consolida como forma objetiva e preventiva, com foco tanto na reparação quanto na prevenção de novos incidentes. Essa abordagem reafirma o papel da LGPD como instrumento de proteção da dignidade humana e da confiança nas relações digitais, pavimentando o caminho para o fortalecimento de uma cultura nacional de proteção de dados.

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste trabalho permitiu compreender a crescente importância da proteção de dados pessoais no cenário jurídico brasileiro e o papel central desempenhado pela responsabilidade civil na reparação de danos decorrentes de incidentes de dados pessoais. Observou-se que a Lei Geral de Proteção de Dados Pessoais (LGPD) estruturou um sistema normativo robusto, pautado em princípios como boa-fé, finalidade, necessidade, segurança e prevenção, que orientam a atuação de todos os agentes de tratamento.

A reconstrução histórica demonstrou que a proteção da privacidade evolui gradualmente no cenário mundial e no país, desde previsões esparsas em legislações anteriores até a formação de um marco regulatório abrangente, culminando na criação da ANPD e na institucionalização da governança de dados.

Ao examinar a responsabilidade civil, verificou-se que os pressupostos clássicos - dano, nexo causal, ilicitude e culpabilidade - foram redesenhados no contexto digital, especialmente pela adoção da responsabilidade objetiva em diversas hipótese, conforme previsto tanto pela LGPD quanto pelo Código de Defesa do Consumidor. No contexto de vazamento de dados, basta a comprovação das falhas na segurança ou a violação de deveres legais para que surja o dever de indenizar, independentemente de culpa. Isso decorre da adoção da responsabilidade civil objetiva, especialmente em relações de consumo e na aplicação da LGPD, que impõem aos controladores um dever legal de segurança e de prevenção. Assim, quando esses deveres não são cumpridos configura-se o chamado fortuito interno, ou seja, um risco inerente à própria atividade de tratamento de dados, afastando a necessidade de demonstrar culpa e reforçando o caráter protetivo e preventivo da norma.

As hipóteses legais de tratamento de dados, previstas nos Artigos 7º e 11 da LGPD, mostram-se essenciais para delimitar a atuação legítima das empresas em e evidenciar, simultaneamente, situações em que violações representam clara transgressão normativa. O trabalho demonstrou que o tratamento inadequado, o uso sem base legal ou a ausência de medidas de segurança configura ilicitude e ensejam responsabilização.

A seção final evidenciou, com base em jurisprudência atualizada e casos concretos amplamente divulgados, que a responsabilidade das empresas por

vazamento é uma realidade consolidada. Decisões recentes do STJ e dos Tribunais Estaduais têm reconhecido o dano moral presumido em situações que envolvam dados sensíveis, reforçando a obrigação de reparação. Além disso, incidentes envolvendo diversos setores - financeiro, saúde, varejo digital, serviços essenciais e administração pública - demonstram a transversalidade dos riscos e a necessidade de governança informacional sólida.

De igual modo, verificou-se o crescente protagonismo da ANPD, que, após regulamentar os critérios de sanções e dosimetria, passou a fiscalizar ativamente controladores e operadores, aplicando advertências, multas e obrigações de ajuste. A atuação sancionatória evidencia que o sistema normativo brasileiro caminha para maior maturidade e segurança jurídica.

À luz da problemática proposta, conclui-se que a LGPD assegura, de fato, mecanismos eficazes de responsabilização civil das empresas que descumprem suas determinações, seja por violação de princípios, ausência de base legal, falhas na segurança da informação ou omissão na comunicação de incidentes. As hipótese secundárias também se confirmam: a ANPD exerce papel fundamental na consolidação dessa proteção; a reputação das empresas é diretamente impactada por incidentes de dados pessoais. E ainda persistem desafios interpretativos e lacunas regulatórias que exigem aprimoramentos futuros, mas que já estão bem encaminhadas e demonstra-se uma evolução significativa desde a promulgação da lei.

Assim, o estudo demonstra que a LGPD não apenas reforça a tutela da privacidade e da dignidade humana, como também promove a construção de uma cultura nacional de proteção de dados, essencial para a confiança nas relações digitais e para o desenvolvimento socioeconômico sustentável no ambiente informacional contemporâneo.

REFERÊNCIAS

ALVES, Julia. **Suspeito por ataque hacker era funcionário da C&M Software e teria fornecido acessos aos criminosos.** Publicado em 5 jul. 2025. Disponível em: https://exame.com/invest/mercados/suspeito-por-ataque-hacker-era-funcionario-da-cm-software-e-teria-fornecido-acessos-aos-criminosos/. Acesso em: 11 jul. 2025.

ANDRADE,Walmar. **Decreto 8.771/2016 – Regulamenta o Marco Civil da Internet.** Disponível em: https://walmarandrade.com.br/decreto-8771-2016/#:~:text=O%20Decreto%20n%C2%BA%208.771%2C%20de,seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o%20na%20internet. Acesso em: 16 set.2025.

ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil - e suas consequências.** Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil. Acesso em: 03 nov.2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, Governo Federal. **Relatório do Ciclo de Monitoramento**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/2023-08-17-relatorio-do-ciclo-de-monitoramento-2022.pdf. Acesso em: 09 abr.2025.

BARROS, Bruno Mello Correa de; BARROS, Clarissa Teresinha Lovatto;OLIVEIRA, Rafael Santos de. **O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais.** Revista Videre, Dourados, MS, v. 9, n.17, 1. semestre de 2017 - ISSN 2177-7837. Disponível em: https://ojs.ufgd.edu.br/index.php/videre/article/view/6029/pdf_1. Acesso em: 01 fev.2025.

BELLI,Luca.**O maior vazamento de dados pessoais na história brasileira e quais lições devemos aprender.** Disponível em: https://portal.fgv.br/artigos/maior-vazamento-dados-pessoais-historia-brasileira-e-quais-licoes-devemos-aprender?utm_source=chatgpt.com. Acesso em: 06 mar.2025.

BRASIL, **Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 24 out.2025.

BRASIL, **Código de Defesa do Consumidor.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 03 nov.2025.

BRASIL, **Código Penal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 16 set.2025.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.Acesso em: 03 fev.2025.

BRASIL. **RESOLUÇÃO CD/ANPD Nº4, DE 24 DE FEVEREIRO DE 2023**. Disponível em:https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 28 set.2025.

BRASIL. **RESOLUÇÃO DA DIRETORIA COLEGIADA - RDC Nº 44 - DE 17 DE AGOSTO DE 2009**.Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/anvisa/2009/rdc0044_17_08_2009.pdf. Acesso em: 09 set.2025.

BRASIL. **Superior Tribunal de Justiça.** Recurso Especial nº 2121904-SP (2024/0031292-7). Recorrente: Prudential do Brasil Seguros de Vida S.A. Recorrido: Pedro Henrique Camiloti. Relatora: Ministra Nancy Andrighi. Brasília, 11 de fevereiro de 2025. Disponíovel em: https://www.conjur.com.br/wp-content/uploads/2025/02/voto-Nancy-STJ-indenizacao-seguradora-vazamento-dados-sensiveis-segurado.pdf. Acesso em: 17 nov.2025

BRASIL. **Tribunal de Justiça do Rio Grande do Sul**. Recurso Inominado nº 50058266820238212001. Recorrente:Euro Factoring Financeira LTDA e outro. Recorrido:Leonel dos Santos Paula. Relatora: Patrícia Antunes Laydner.Rio Grande do Sul, 03 de setembro de 2024.Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa. Acesso em: 17 nov.2025

BRASIL. **Tribunal de Justiça do Rio Grande do Sul**. Recurso Inominado nº 51564618120228210001. Recorrente: Mercado Pago Instituição de Pagamento LTDA e outro. Recorrido: Macedo e Reichert LTDA. Relatora: Patrícia Antunes Laydner.Rio Grande do Sul, 02 de abril de 2024. Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa. Acesso em: 17 nov.2025

BRASIL. **Tribunal de Justiça do Rio Grande do Sul**. Recurso Inominado nº 50077392320218210072. Recorrente: Banco do Estado do Rio Grande do Sul - BANRISUL. Recorrido: Ana Lucia Stefani Leão. Relatora: Nara Cristina Neumann Cano Saraiva. Rio Grande do Sul, 06 de abril de 2023. Disponível em: https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa. Acesso em: 17 nov.2025

CAVALCANTE, Daniele. **Quantidade de ataques cibernéticos no Brasil aumentou (e muito) em 2014, segundo CERT.br**. Disponível em: https://www.tudocelular.com/seguranca/noticias/n52459/ataques-ciberneticos-aumentam-no-brasil-em-2014.html#:~:text=Essa%20t%C3%A9cnica%2C%20utilizando%20sites%20que,sempre%20evitar%20abrir%20links%20duvidosos.&text=%C3%A9%20impressionante%20como%20ainda%20n%C3%A3o,antivirus%20da%20psafe%20no%20computador. Acesso em: 16 set.2025.

COTS, M.; OLIVEIRA, R. **Lei Geral de Proteção de Dados Pessoais Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. Acesso em: 07 out.2025.

FMP.EDU. **Lei Carolina Dieckmmann: você sabe o que essa lei representa?**Disponível em:https://www.fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/#:~:text=Por%20que%20a%20lei%20recebeu,tratava%20especificamente%20sobre%20o%20assunto. Acesso em: 16 set.2025.

GARRIDO, Patrícia Peck. **Proteção de dados pessoais**: comentários a lei n 13.709/2018 (LGPD) ligada. 2. ed. São Paulo: Saraiva, 2020. 152 p. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555599480/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover.xhtml]!/4/2[cover]/2%4050:77. Acesso em: 03 jul.2025.

G1. **Como eram o Brasil e o mundo em 2010: Bieber revelação, coloridos, Crepúsculo e Adeus a Saramago.** Disponível em: https://g1.globo.com/pop-arte/noticia/2023/06/28/como-era-o-brasil-e-o-mundo-em-2010-bieber-revelacao-coloridos-crepusculo-e-adeus-a-saramago.ghtml. Acesso em: 09 set.2025.

G1. **ANPD notifica 20 empsas por descumprirem regra de proteção de dados**. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/12/13/anpd-notifica-20-empresas-por-descumprirem-regra-de-protecao-de-dados.ghtml#lista. Acesso em: 13 nov.2025.

HAIKAL, Beatriz. **Brasil avança para ser declarado "país adequado" pela União Europeia em proteção de dados.** Disponível em: https://tiinside.com.br/09/09/2025/brasil-avanca-para-ser-declarado-pais-adequado-pela-uniao-europeia-em-protecao-de-dados/. Acesso em: 13 out.2025.

HIGA, Carlos César. **Ditadura Militar Chilena.** Disponível em: https://mundoeducacao.uol.com.br/historia-america/ditadura-militar-chilena.htm#:~:text=A%20ditadura%20militar%20chilena%20come%C3%A7ou,julgados%20e%20condenados%20%C3%A0%20pris%C3%A3o. Acesso em: 03 set.2025.

INPD. **União Europeia avança em decisão de adequação que reconhece proteção de dados no Brasil.** Brasília, 6 set. 2024. Disponível em: https://www.inpd.com.br/post/uni%C3%A3o-europeia-avan%C3%A7a-em-decis%C3%A3o-de-adequa%C3%A7%C3%A3o-que-reconhece-prote%C3%A7%C3%A3o-de-dados-no-brasil. Acesso em: 07 out. 2025.

MÁXIMO, Wellton. **CNJ comunica vazamento de dados de chaves Pix de 11 milhões de pessoas**. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2025-07/cnj-comunica-vazamento-de-dados-de-chaves-pix-de-11-milhoes-de-pessoas. Acesso em: 03 nov.2025.

MERCEY, Jérôme de. **Lista de Países considerados adequados para transferências ao abrigo do RGPD [TABELA].** Disponível em: https://www.dastra.eu/en/article/the-list-of-countries-deemed-adequate-for-gdpr-transfers-table/59031?utm_source=chatgpt.com. Acesso em: 24 out.2025.

MENEZES, J. B. de; COLAÇO, H. S. **Quando a lei geral de proteção de dados não se aplica**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei

Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/97711725/Lei_Geral_de_Protecao_de_Dados_Pessoais_e_suas_Repercussoes_no_Direito.pdf?. Acesso em: 07 out.2025.

OLIVEIRA, Diogo Luís Manganelli De. **Proteção de dados pessoais na América Latina: é possível uma harmonização?** Disponível em: https://www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-pessoais-na-america-latina-e-possivel-uma-harmonizacao. Acesso em: 09 set.2025.

OPENAI. *ChatGPT*. Disponível em: https://chat.openai.com/. Acesso em: 03 jul. 2025.

SANTOS, L. **Princípios da Lei Geral de Proteção de Dados: fundamentos e aplicabilidade prática.** São Paulo: Atlas, 2019. Acesso em: 07 out.2025.

SESC. **Documentos da década de 1940 ajudam a entender contextos social, político, econômico e ideológico da criação do Sesc.** Disponível em: https://www.sescsp.org.br/editorial/documentos-da-decada-de-1940-ajudam-a-entender-contextos-social-politico-economico-e-ideologico-da-criacao-do-sesc/.Acesso em: 09 set.2025.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016. Acesso em: 29 set.2025.

SILVA, Daniel Neves. **"História da internet"; *Brasil Escola*.** Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em: 11 jul.2025.

SILVA, Júlio César Lázaro da. **"As Dificuldades Enfrentadas pela Economia da Argentina"**; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/geografia/as-dificuldades-enfrentadas-pela-economia-argentina.htm. Acesso em: 26 set.2025.

SILVA, Ana Paula Vasconcellos da. **Avanços e desafios sete anos após a promulgação da LGPD**. Disponível em: https://www.migalhas.com.br/amp/depeso/439117/avancos-e-desafios-sete-anos-apos-a-promulgacao-da-lgpd. Acesso em: 11 nov.2025.

SILVA, R. L.; SILVA, L. B. **A proteção jurídica de dados pessoais na internet: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil**. Direito e novas tecnologias. Florianópolis: FUNJAB, 2013. Disponível em: http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65. Acesso em: 07 out. 2025.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. **Tutela da pessoa humana na lei geral de proteção de dados pessoais:** entre a atribuição de direitos e a enunciação de remédios. Disponível em: https://ojs.unifor.br/rpen/article/view/9407. Acesso em: 23 mar.2025.

TEFFÉ, Chiara Spadaccini; VIOLA, Mario. **Tratamento de dados pessoais na LGPD**: estudo sobre as bases legais. Civilistica. Rio de Janeiro, p. 1-38. 10 dez. 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em: 03 fev. 2025.

TEIXEIRA, R. **Direito Digital e a Proteção de Dados no Brasil.** Rio de Janeiro: Forense, 2019. Acesso em: 07 out.2025.

TIMES, Global. **Uruguai superará crise sem recessão.** Disponível em:http://business.globaltimes.cn/world/2009-09/468924.html. Acesso em: 28 set.2025.

ZUP. **História da Privacidade de Dados e suas Legislações.**Disponível em: https://zup.com.br/blog/historia-da-privacidade-de-dados/. Acesso em: 03 jul.2025.