UNIVERSIDADE FEDERAL DE OURO PRETO
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

CEZAR GUILHERME DE PAIVA PETRILLO

PRIVACIDADE E REPERCUSSÃO DA *ACCOUNTABILITY* PARA OBRIGAÇÕES DO AGENTE DE TRATAMENTO DE MENOR PORTE RELACIONADAS AOS DIREITOS DO TITULAR DE DADOS

OURO PRETO
2025

Cezar Guilherme de Paiva Petrillo

PRIVACIDADE E REPERCUSSÃO DA *ACCOUNTABILITY* PARA OBRIGAÇÕES DO AGENTE DE TRATAMENTO DE MENOR PORTE RELACIONADAS AOS DIREITOS DO TITULAR DE DADOS

Trabalho de Conclusão de Curso apresentado ao Departamento de Direito da Universidade Federal de Ouro Preto como requisito parcial para obtenção de título de Bacharel em Direito

Orientador: Prof. Dr. Roberto Henrique Pôrto Nogueira

OURO PRETO
2025

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Cezar Guilherme de Paiva Petrillo

Privacidade e repercussão da accountability para obrigações do agente de tratamento de menor porte relacionadas aos direitos do titular de dados

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 03 de setembro de 2025.

Membros da banca:

Dr. Roberto Henrique Pôrto Nogueira – Orientador e Avaliador (Universidade Federal de Ouro Preto)
Dra. Juliana Evangelista de Almeida – Avaliadora (Universidade Federal de Ouro Preto)
Mestranda Maria Paula Correia Ramos – Avaliadora (Programa de Pós-Graduação em Direito - Mestrado Acadêmico – UFOP)

Dr. Roberto Henrique Pôrto Nogueira, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 04/09/2025.

Documento assinado eletronicamente por **Roberto Henrique Porto Nogueira**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 04/09/2025, às 20:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0973600** e o código CRC **83184841**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3559-1545 - www.ufop.br

AGRADECIMENTOS

Agradeço a Deus, por ter me amado primeiro, mostrando-me que os planos d'Ele são sempre maiores que os meus e por ter cuidado de mim durante toda essa jornada.

Agradeço aos meus pais, por me sustentarem não apenas materialmente, mas também com palavras de incentivo, pela preocupação que traduz amor e pelo cuidado que me acompanhou em cada passo desta caminhada.

Agradeço à Maria Clara, meu amor e companheira de jornada, minha gratidão por compartilhar comigo sonhos, medos, alegrias e preocupações, por me apoiar todos os dias e celebrar comigo cada conquista, sempre me lembrando que tudo era para Ele.

Agradeço à minha família, em especial a José Carvalho, José Carvalho Jr. e Vítor, por serem exemplos de caráter e dedicação, e por me acompanharem desde o início dessa jornada, me inspirando sempre a persistir.

Agradeço ao meu orientador Roberto, pela paciência, atenção e pela amizade construída ao longo dessa trajetória, sendo um exemplo que levarei para a vida, tanto no campo acadêmico quanto profissional.

Agradeço ao escritório Leroy e Freitas, em especial ao Lucas e ao Guilherme, pelo apoio, incentivo e confiança que fizeram toda a diferença nessa etapa.

Agradeço a todos os meus professores e professoras, que moldaram a minha formação acadêmica.

Por fim, agradeço de coração a todos os amigos que caminharam comigo, tornando essa jornada mais leve.

"*Se você deseja construir um navio, não reúna pessoas para coletar madeira nem lhes atribua tarefas ou trabalho, mas ensine-as a ansiar pela imensidão infinita do mar"*.

(Antoine de Saint-Exupéry)

RESUMO

É juridicamente possível reconhecer que, mesmo sob regime regulatório simplificado, as obrigações dos agentes de tratamento de pequeno porte, em relação aos direitos dos titulares, devam ser interpretadas como dinâmicas e interativas, por força da noção de privacidade como autodeterminação informativa e da incidência do princípio da *accountability*? A LGPD consagra o princípio da *accountability*, o qual parece determinar os desenhos dos deveres dos agentes de tratamento. A hipótese é a de que a simples disponibilização de canal de atendimento ao titular de dados não satisfaz, por si só, as exigências da LGPD, diante das repercussões do princípio em apreço e da privacidade marcada pela autodeterminação informativa. Portanto, o objetivo geral é investigar a possibilidade jurídica de se reconhecer a natureza dinâmica e interativa das obrigações dos agentes de tratamento de pequeno porte, relativas aos direitos dos titulares, como desdobramento do princípio da *accountability*, à luz da noção de privacidade como autodeterminação informativa. São objetivos específicos: analisar os fundamentos principiológicos da LGPD e os direitos dos titulares de dados; conceituar e delimitar o princípio da *accountability* no contexto da proteção de dados pessoais; estudar a redefinição da privacidade como autodeterminação informativa, conforme Stefano Rodotà; examinar o regime jurídico aplicável aos agentes de tratamento de pequeno porte; verificar a conformidade dos canais de comunicação com a exigência de efetividade e diálogo. A justificativa da pesquisa está na constatação de que a Resolução CD/ANPD nº 2/2022 estabelece flexibilizações específicas aos agentes de pequeno porte. Contudo, à luz da LGPD e da teoria da autodeterminação informativa, impõe-se apurar se essas flexibilizações permitem práticas meramente formais ou se exigem o cumprimento substancial e responsivo dos deveres, como expressão do princípio da *accountability*. A metodologia adotada é qualitativa, de natureza bibliográfica e documental, com abordagem hipotético-dedutiva. Parte-se da redefinição da privacidade conforme Rodotà (2008), articulada com a dogmática normativa da LGPD e com a Resolução CD/ANPD nº 02/2022. A pesquisa alcança o importante achado de que a efetividade e a natureza dialógica desse canal são imperativos jurídicos decorrentes da *accountability*, sobretudo quando se adota a privacidade como expressão de autodeterminação informativa.

Palavras-chave: *Accountability*; Agente de tratamento de menor porte; Autodeterminação informativa; LGPD; Privacidade.

ABSTRACT

Is it legally possible to recognize that, even under a simplified regulatory regime, the obligations of small-scale data controllers, in relation to data subjects' rights, must be interpreted as dynamic and interactive, by virtue of the notion of privacy as informational self-determination and the application of the principle of accountability? The LGPD enshrines the principle of accountability, which appears to shape the design of data controllers' duties. The underlying hypothesis is that the mere provision of a communication channel for data subjects does not, by itself, satisfy the LGPD's requirements, in light of the repercussions of the aforementioned principle and of privacy understood as informational self-determination. Therefore, the general objective is to investigate the legal possibility of recognizing the dynamic and interactive nature of the obligations of small-scale data controllers, regarding the rights of data subjects, as an outgrowth of the principle of accountability, in light of the notion of privacy as informational self-determination. The specific objectives are: to analyze the foundational principles of the LGPD and the rights of data subjects; to define and delimit the principle of accountability in the context of personal data protection; to study the redefinition of privacy as informational self-determination, according to Stefano Rodotà; to examine the legal regime applicable to small-scale data controllers; and to verify the compliance of communication channels with the requirement of effectiveness and dialogue. The justification for this research lies in the finding that ANPD Resolution CD/ANPD No. 2/2022 establishes specific flexibilizations for small-scale data controllers. However, in light of the LGPD and the theory of informational self-determination, it is necessary to determine whether these flexibilizations allow merely formal practices or require the substantial and responsive fulfillment of duties, as an expression of the principle of accountability. The methodology adopted is qualitative, bibliographical, and documentary in nature, with a hypothetical-deductive approach. It is based on the redefinition of privacy proposed by Rodotà (2008), articulated with the normative dogmatics of the LGPD and with Resolution CD/ANPD No. 02/2022. The research reaches the important finding that the effectiveness and dialogical nature of this channel are legal imperatives arising from accountability, especially when privacy is adopted as an expression of informational self-determination.

Keywords: Accountability; Small-Scale Data Controller; Informational Self-Determination; LGPD; Privacy.

SUMÁRIO

1 INTRODUÇÃO

A sociedade contemporânea é marcada pela incorporação das tecnologias da informação e da comunicação, que transformaram as formas de organização social, econômica e política. Vivencia-se, hoje, um cenário caracterizado por fluxos informacionais massivos, contínuos e velozes, os quais remodelaram a noção tradicional de espaço e tempo, e passam a ocupar papel central na dinâmica das relações sociais. Nesse novo ambiente informacional, a utilização de tecnologias baseadas em dados acentua a necessidade de redefinir os contornos jurídicos da proteção à privacidade.

Como efeito, despontam desafios inéditos à privacidade dos indivíduos, o que exige do Direito respostas mais específicas, proporcionais e coerentes com a complexidade do cenário informacional contemporâneo. Nesse contexto, ganha relevo a concepção de privacidade como autodeterminação informativa, formulada por Stefano Rodotà (2008), segundo a qual a pessoa deve exercer controle efetivo sobre o fluxo de informações que lhe dizem respeito, condição ao pleno exercício da liberdade e da dignidade humana.

Nesse sentido, o direito à privacidade é reformulado pela Lei Geral de Proteção de Dados Pessoais (LGPD), marco normativo que consolida o direito à proteção dos dados pessoais, posteriormente elevado ao patamar de direito fundamental por meio da Emenda Constitucional nº 115/2022. A LGPD adota uma lógica principiológica e estruturante, exigindo dos agentes de tratamento, de modo geral, não apenas o cumprimento formal de obrigações legais, mas a internalização de uma postura ativa, preventiva e transparente no trato com dados pessoais. É nesse arcabouço que se insere o princípio da *accountability*, traduzido no ordenamento brasileiro como “responsabilização e prestação de contas”, elemento central do modelo de governança regulatória adotado pela legislação.

A *accountability*, concebida no âmbito da Organização para Cooperação e Desenvolvimento Econômico (OCDE), assume caráter multifacetado e camaleônico, articulando aspectos éticos, normativos e procedimentais da responsabilidade em sentido lato. Na LGPD, ela opera como diretriz de governança e como mecanismo de conformidade por meio dos quais os agentes devem demonstrar a adoção de medidas proporcionais e auditáveis para assegurar a proteção dos dados pessoais. Trata-se, assim, de princípio que conecta a autodeterminação informativa ao dever contínuo de justificação de práticas organizacionais, comunicacionais e tecnológicas diante dos titulares e da Autoridade Nacional de Proteção de Dados (ANPD).

Contudo, não obstante os preceitos normativos trazidos pela LGPD, persistem lacunas interpretativas e operacionais que podem comprometer a efetividade da tutela conferida aos titulares de dados, especialmente quando se trata dos agentes de tratamento de menor porte. Esses agentes, por vezes alijados dos debates especializados e marcados por limitações técnicas, operacionais e econômicas, enfrentam obstáculos concretos para o cumprimento pleno das exigências legais.

Tendo como um dos escopos editar normas, orientações e procedimentos simplificados e diferenciados do cumprimento dos deveres atribuídos por lei a agentes de tratamento de menor porte, a Resolução CD/ANPD nº 2/2022 aprova o Regulamento de aplicação para esses sujeitos.

Diante dessa realidade regulatória simplificada, coloca-se uma indagação central que orienta a presente investigação: é possível, a partir da noção de privacidade marcada pela autodeterminação informativa e articulada em um movimento teórico-dogmático da normativa aplicada, reconhecer a interatividade e dinamicidade das obrigações do agente de tratamento de menor porte relacionadas aos direitos do titular como repercussão de *accountability*?

Neste trabalho, almeja-se testar a hipótese de que, a partir da noção de privacidade como autodeterminação informativa, é possível reconhecer a interatividade e a dinamicidade das obrigações dos agentes de tratamento de menor porte como repercussão do princípio da *accountability.* Para tanto, especial atenção é dedicada ao dever de disponibilização de canal de comunicação com o titular de dados. Considera-se que, mesmo com as flexibilizações normativas concedidas a esses agentes, as exigências de transparência, segurança e governança não devem ser esvaziadas, mas sim ajustadas em grau, sem prejuízo do seu núcleo essencial.

Assim, o objetivo geral desta pesquisa é investigar a partir da noção de privacidade marcada pela autodeterminação informativa e articulada em um movimento teórico-dogmático da normativa aplicada, a possibilidade jurídica de reconhecer a interatividade e dinamicidade das obrigações do agente de tratamento de menor porte relacionadas aos direitos do titular como repercussão de *accountability*. Como objetivo específico, busca-se avaliar a suficiência dos canais de comunicação disponibilizados por esses agentes como expressão concreta da *accountability*, considerando-os elemento essencial para a efetivação da transparência e da confiança entre titulares e controladores

São objetivos específicos: analisar os fundamentos principiológicos da LGPD e os direitos dos titulares de dados; conceituar e delimitar o princípio da *accountability* no contexto da proteção de dados pessoais; estudar a redefinição da privacidade como autodeterminação informativa, conforme Stefano Rodotà; examinar o regime jurídico aplicável aos agentes de tratamento de pequeno porte; verificar a conformidade dos canais de comunicação com a

exigência de efetividade e diálogo com o titular de dados, conforme abstração do conteúdo normativo da *accountability*.

A metodologia adotada é de natureza qualitativa, com enfoque bibliográfico e documental, orientada por uma abordagem hipotético-dedutiva. A escolha pela abordagem qualitativa justifica-se pela complexidade conceitual e normativa do objeto em análise, que imprescinde de interpretação sistemática das categorias jurídicas correlatas, especialmente a noção de privacidade e o princípio da *accountability*. A investigação hipotético-dedutiva se desenvolve a partir da formulação da premissa de que a *accountability* é transversal à LGPD e, nessa medida, repercute em seu regramento. Esforço de interpretação sistemática da Lei Geral de Proteção de Dados Pessoais (LGPD) e da Resolução CD/ANPD nº 2/2022 também é empreendido. Como referencial teórico-estrutural, a redefinição da privacidade como autodeterminação informativa, nos moldes cunhados por Stefano Rodotà (2008), há de contribuir para uma perspectiva que projeta os direitos do titular para além da proteção, conferindo-lhe o caráter de um direito de controle ativo e consciente sobre suas informações. Essa concepção serve de fundamento hermenêutico da dogmática em questão, especialmente no que concerne à articulação entre os direitos dos titulares e os deveres dos agentes de tratamento de menor porte.

Nessa linha, a pesquisa recorre à bibliografia especializada e à normativa de regência, para avaliar se as flexibilizações específicas podem ser calibradas pela *accountability*. Assim, em movimento teórico jurídico-dogmático, cabe explorar as dimensões tolhidas e as características reforçadas pela regulação específica sistematicamente contextualizada.

2 ESTRUTURA NORMATIVA DA LGPD: EVOLUÇÃO, PRINCÍPIOS E DIREITOS DO TITULAR DE DADOS

A Lei Geral de Proteção de Dados Pessoais (LGPD) surge como resposta à necessidade de estabelecer regras claras e seguras sobre o tratamento de dados pessoais no Brasil. Em um cenário pautado pela coleta, circulação e uso massivo de informações, cabe garantir segurança jurídica tanto para titulares dos dados quanto para agentes públicos e privados que os processam. A LGPD, nesse sentido, não apenas disciplina as condutas relacionadas ao uso de dados, como também promove um ambiente de previsibilidade e estabilidade normativa (BIONI, 2020, p.103).

Em vista disso, a LGPD consolida-se como um marco inovador no ordenamento jurídico brasileiro, o que reflete uma mudança significativa na forma de regulação adotada no país, nas palavras de Nelson Rosenvald e José Luiz de Moura Faleiros Júnior (2022):

> A Lei Geral de Proteção de Dados Pessoais é o exemplo mais recente de uma tendência que se nota com especial intensidade, no Brasil, ao longo da última década: a superação de modelos regulatórios herméticos e lastreados em estruturas de comando e controle vem abrindo largo espaço ao florescimento de normas pautadas em estruturas abertas, catalisadas pelo desejável *compliance*. (ROSENVALD; FALEIROS JÚNIOR *In* FRAZÃO; CUEVA, 2022).

Este capítulo tem como objetivo apresentar os principais aspectos da LGPD, seu histórico de construção normativa, princípios e os direitos dos titulares de dados. Conforme descreve Bioni (2020):

> [...] As leis de proteção de dados procuram conferir segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado sobre como deve se dar o fluxo desses dados. E, em última análise, assegurar confiança entre todos os atores desse ecossistema para que não haja paralisia nessas trocas econômicas. (BIONI, 2020, p.103).

Trata-se, portanto, de marco legal que redefine a forma como os dados pessoais devem ser tratados no país, que busca assegurar um fluxo informativo legítimo, inequívoco, seguro e compatível com os direitos fundamentais e o livre desenvolvimento da personalidade, que promove um ambiente de confiança e responsabilidade no tratamento de informações.

2.1 Histórico e mutações da LGPD

Historicamente, antes da aprovação da LGPD, o Brasil dispunha apenas de leis setoriais de proteção de dados, o que caracteriza, conforme disposto por Bioni (2020) uma “colcha de

retalhos" (BIONI, 2020, p. 103), à medida que havia lacunas significativas na proteção jurídica, bem como incertezas para os cidadãos, para o setor produtivo e para o poder público.

A Lei Geral de Proteção de Dados Pessoais (LGPD) é resultado de um processo de articulação legislativa e institucional que se estende por quase uma década, tendo suas discussões iniciadas em 2010, até ser finalmente sancionada como Medida Provisória 869/ 2018 e convertida em lei em 8 de julho de 2019, assim, foram mapeadas nove fases ao longo do processo (BIONI, 2022, p. 38).

Segundo o estudo de Bioni (2022), as nove fases são, a seguir, especificadas:

> **a) Fase 1 (novembro, 2010):** O Ministério da Justiça divulgou um anteprojeto de lei sobre proteção de dados pessoais na plataforma culturadigital.br/dados pessoais para consulta pública.
> **b) Fase 2 (janeiro, 2015):** Ao longo do primeiro semestre de 2015 um novo anteprojeto foi disponibilizado para consulta pública na plataforma "Pensando o Direito".
> **c) Fase 3 (maio, 2016):** Nas vésperas do seu afastamento, a então Presidenta Dilma Rousseff encaminhou o texto do anteprojeto à Câmara dos Deputados, que se transformaria no PL 5.276/2016.
> **d) Fase 4 (maio, 2018):** A Câmara dos Deputados aprovou, em junho de 2018, o PL 4.060/2012, na forma do substitutivo apresentado pelo deputado Orlando Silva (PCdoB/SP). O texto foi então enviado ao Senado, onde tramitou como PLC 53/2018.
> **e) Fase 5 (agosto, 2018):**
> Aprovado o projeto de lei no Congresso (Lei 13.709/2018), seguiu à sanção presidencial pelo então Presidente Michel Temer, com a imposição de vetos a alguns dispositivos.
> **f) Fase 6 – Emendas parlamentares à MP 869/2018 (fevereiro, 2019):** Após vetar os artigos referentes à ANPD no texto aprovado no Congresso, Temer comprometeu-se a instituir Medida Provisória buscando criar essa entidade.
> **g) Fase 7 (maio, 2019) – Projeto de Lei de Conversão 7, de 2019:** Apresentado projeto de conversão da MP 869 em lei no Congresso.
> **h) Fase 8 (julho, 2019 – Lei 13.853/2019):** A MP 869 é convertida em lei.
> **h) Fase 8 (julho, 2019 – Lei 13.853/2019):** A MP 869 é convertida em lei.
> **i) Fase 9 (julho, 2019) – Destaques da segunda rodada de vetos:** Vetos do então Presidente Bolsonaro ao Projeto de Lei de Conversão 7, de 2019. (BIONI, 2022, p. 38-39, grifo do autor).

Esse processo legislativo complexo não apenas consolida o modelo normativo brasileiro de proteção de dados, como também permite o amadurecimento de debates técnicos e jurídicos centrais para sua conformação. Ainda de acordo com Bioni (2020), durante a construção da Lei Geral de Proteção de Dados Pessoais (LGPD), o consentimento do titular figurava, inicialmente, como a principal, e praticamente única, base legal para o tratamento de dados pessoais. Essa concepção, no entanto, transforma-se ao longo dos anos, à medida que o debate sobre a regulação da proteção de dados no Brasil amadurece. O avanço do processo legislativo, impulsionado pelas contribuições recebidas nas consultas públicas realizadas, trouxe à tona a necessidade de um modelo mais flexível e adaptável às diversas realidades do tratamento de dados (BIONI, 2020, p.127).

Como resultado, a versão final da LGPD passa a reconhecer o consentimento não mais como fundamento exclusivo, mas como uma entre várias bases legais previstas para legitimar o tratamento de dados pessoais. Essa alteração marca um avanço significativo na técnica legislativa, ao adotar uma organização que coloca uma estrutura legal horizontal, que evita atribuir ao consentimento um status de superioridade em relação às demais hipóteses legítimas previstas na norma (BIONI, 2020, p.127).

A chamada fase 4 do processo legislativo merece destaque especialmente no que se refere à incorporação do princípio da *accountability*, pois altera de forma substancial a lógica do regime de responsabilidade civil até então aplicado aos agentes de tratamento (BIONI, 2022, p. 41). Nesse contexto, Bruno Bioni (2022) indica:

> Espera-se que o agente de tratamento de dados pessoais seja capaz de fazer um juízo de valor em torno da sua gravidade, o que não só desencadeará a obrigação legal em torno da comunicação ao órgão regulador e ao titular, como também, o próprio conteúdo dessa comunicação inicial. (BIONI, 2022, p.58).

Assim, nota-se que a LGPD passa a atribuir progressivamente maior autonomia e responsabilidade decisória a esses agentes, isto é, a aposta no juízo de valor dos próprios agentes para definir, de forma proporcional e eficaz, as melhores medidas para assegurar a proteção dos dados pessoais.

2.2 Princípios da LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, tem como escopo a proteção dos direitos fundamentais de liberdade, de privacidade e do livre desenvolvimento da personalidade da pessoa natural. Como estabelece seu artigo 1º, trata-se de um marco normativo voltado à salvaguarda da dignidade da pessoa humana frente à crescente circulação e uso de dados pessoais, inclusive em meios digitais.

> (...) sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento de personalidade da pessoa natural (BRASIL, 2018).

Para concretizar essa proteção, a LGPD apresenta um conjunto de princípios fundamentais (art. 6º), que orientam todo o ciclo de vida do tratamento de dados pessoais. Tais princípios, demonstram preocupação com a participação ativa do indivíduo no controle de suas

informações pessoais, que reforça sua autonomia e autodeterminação informativa (BIONI. 2022, p. 128).

Nesse contexto, o titular dos dados não é mero objeto do tratamento, mas sim seu protagonista. É importante destacar que a legislação assegura que o fluxo de dados se dê de forma ética, transparente e alinhada à vontade informada do titular, que resguarda sua liberdade de decisão e sua integridade pessoal.

2.2.1 Princípio da finalidade

> 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; (BRASIL, 2018)

O princípio da finalidade determina a necessidade de especificar a razão pela qual o dado é coletado, utilizado ou armazenado, assegurada a transparência e previsibilidade ao titular, de forma a garantir que o cidadão foi devidamente informado para tomar iniciar um processo de tomada de uma decisão livre e autônoma (BIONI, 2020, p. 185).

Nesse sentido, os dados pessoais devem apresentar uma finalidade clara e objetiva, sem a admissão de equivocidade ou ambiguidade, a fim de impedir qualquer desvio de finalidade e garantir a proteção da autonomia do titular.

Além disso, o tratamento de dados deve apresentar propósitos legítimos, específicos e explícitos, sem possibilidade de tratamento posterior que desvirtue da finalidade previamente informada (OLIVEIRA & LOPES, 2019, *apud* NUZZI & FERNANDES, 2022, p. 6).

Caso a utilização do dado desvie da sua finalidade, a conduta assume caráter ilícito e a atividade se torna ineficaz, que gera a responsabilização do agente de tratamento e possibilitando a adoção dos meios de tutela aos direitos do titular (MIRAGEM, 2019, p.6).

Por fim, observa-se que o princípio da finalidade, além de delinear o objetivo final do tratamento de dados, confere ao titular previsibilidade quanto ao uso que será feito das informações, preservando a segurança jurídica e escopo protetivo ao titular.

2.2.2 Princípio da adequação

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; (BRASIL, 2018).

O princípio da adequação refere-se ao procedimento realizado para se chegar à finalidade pretendida. Ou seja, “o tratamento de dados deve corresponder às legítimas expectativas do seu titular" (BIONI, 2020, p. 128).

Acerca disso, compreende-se que o tratamento de dados deve ser fiel à finalidade especificada, sendo assegurado que as informações utilizadas sejam pertinentes, proporcionais e não excessivas. O princípio da adequação está intrinsecamente ligado ao da finalidade, uma vez que determina que os dados coletados para atingir determinado objetivo devem ser compatíveis com a destinação previamente informada. Assim, as informações tratadas não podem se mostrar inadequadas ou destoantes da finalidade a que se propõem (LIMA, 2021, *apud* NUZZI & FERNANDES, 2022, p.6).

A fim de esclarecimento, enquanto a finalidade se concentra no propósito declarado para o tratamento dos dados, a adequação se volta à compatibilidade entre os meios utilizados e a finalidade pretendida.

> A adequação está intimamente ligada ao princípio da finalidade, mas em um contexto mais objetivo. Observa-se o serviço prestado ou o produto fornecido e a necessidade de coleta dos dados. Somente se existir compatibilidade entre o serviço ou produto e o dado coletado, a exigência será legítima (FLUMIGNAN; FLUMIGNAN, 2020, *apud* NUZZI & FERNANDES, 2022, p. 6).

Dessa forma, o princípio da adequação atua como um filtro essencial para garantir que o tratamento de dados se mantenha alinhado à finalidade previamente informada, evitando coletas arbitrárias ou excessivas e assegurando que cada dado solicitado seja estritamente necessário ao contexto apresentado.

2.2.3 Princípio da necessidade

> 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; (BRASIL, 2018).

O princípio da necessidade estabelece que os dados coletados devem ser estritamente necessários e não excessivos para que estejam em conformidade com a finalidade informada (LIMA, 2021, *apud* NUZZI & FERNANDES, 2022, p.7). Conforme Silvano Flumignan (2020), “o princípio assumirá duas facetas: implicará aumento de responsabilidade para aquele que coleta os dados e impedirá a coleta não imprescindível” (FLUMIGNAN; FLUMIGNAN, 2020, apud NUZZI & FERNANDES, 2022, p. 7).

Nesse sentido, “os dados coletados são realmente aqueles necessários (minimização) para se atingir a finalidade pretendida. A reflexão a ser feita é se seria possível atingir o mesmo resultado por meio de uma quantidade menor de dados, sendo, em última análise, menos intrusivo e impactando menos o indivíduo” (BIONI, 2020, p. 243). Depreende-se, portanto, que o tratamento de dados pessoais deve se limitar ao mínimo necessário para o alcance das finalidades previamente estabelecidas.

2.2.4 Princípio do livre acesso

> 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; (BRASIL, 2018).

O princípio do livre acesso preconiza o direito do titular de requerer informações sobre seu tratamento (LIMA, 2021, *apud* NUZZI & FERNANDES, 2022, p. 7). Além disso, o titular pode consultar, a qualquer momento, como seus dados pessoais estão sob utilização controlador (VAINZOF, 2020, *apud* NUZZI & FERNANDES, 2022, p. 7). Diante disso, o titular, além de requerer as informações coletadas, pode solicitar a atualização ou exclusão de seus dados pessoais, conforme estipulado no artigo 9º da LGPD.[1]

Assim, o princípio do livre acesso consolida-se como instrumento fundamental para a transparência e o controle exercido pelo titular sobre seus próprios dados, o que permite que o titular acompanhe todo o ciclo de tratamento

2.2.5 Princípio da qualidade dos dados

> 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 (BRASIL, 2018).

O princípio da qualidade dos dados aborda que os dados “devem ser claros, exatos, relevantes e atualizados de acordo com a necessidade e a finalidade do tratamento” (MACIEL, 2019, p. 24).

Tal princípio impõe aos agentes de tratamento a obrigação de garantir que os dados sejam tratados com rigor, que corresponde fielmente à realidade do titular e à finalidade para a qual foram coletados. Além disso, recai sobre os agentes o dever de comunicar eventuais

[1] “Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso” (BRASIL, 2018).

correções ou atualizações aos demais com quem os dados tenham sido compartilhados, salvo em casos de comprovada impossibilidade ou esforço desproporcional (LIMA, 2021, p. 214). Essa articulação entre os diversos envolvidos no tratamento de dados é essencial para impedir a perpetuação de erros e evitar prejuízos ao titular, que assegura, assim, a fidedignidade das informações.

No mesmo sentido, os artigos 6º, inciso V, e 18, inciso III, da Lei Geral de Proteção de Dados (LGPD) garantem ao titular o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados, que reafirma o caráter dinâmico e responsável da gestão de informações pessoais. Conforme observa Bioni (2020):

> Ao lado do princípio da qualidade dos dados, o direito de correção é uma construção que deriva da perspectiva da identidade do sujeito e não do direito à privacidade. É o primeiro direito de personalidade que determina a necessidade de haver uma correspondência fidedigna entre a pessoa e seus dados pessoais. (BIONI, 2020, p. 58).

Dessa forma, a integridade dos dados deve ser constantemente mantida, uma vez que qualquer distorção pode comprometer não apenas direitos individuais, mas também a própria confiança no sistema de tratamento de dados. A qualidade, portanto, é condição indispensável para a proteção efetiva dos titulares e para a legitimidade das operações realizadas com seus dados pessoais.

2.2.6 Princípio da Transparência

> 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 (BRASIL, 2018).

O princípio da transparência determina a necessidade de clareza e de precisão durante todo o fluxo dos dados pessoais, bem como o fácil acesso à informação por parte dos titulares.

> A transparência restringe apenas no tocante a segredos comercial e industrial, mas ademais, obrigada o coletor ou tratador de dados a tornar todas as informações o mais, transparentes possíveis para os titulares" (MALLMANN, 2020, *apud* NUZZI & FERNANDES, 2022, p.11).

Essa exigência visa assegurar o respeito à legítima expectativa do titular, de modo que ele possa exercer de forma plena o controle sobre seus dados. Tal garantia abrange não apenas o conhecimento das informações efetivamente tratadas, mas também os critérios utilizados, os prazos envolvidos e os responsáveis pelo tratamento. A LGPD reflete essa preocupação em diversos dispositivos legais, como no artigo 9º, que reforça a necessidade de tornar acessível ao

titular o funcionamento do tratamento de seus dados, bem como os canais para exercer seus direitos.

2.2.7 Princípio da segurança

> 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 (BRASIL, 2018).

O Princípio da segurança prevê que os dados pessoais devem ser tratados de modo a assegurar a segurança e confidencialidade das informações, a fim de prevenir o acesso de não autorizados, bem como o uso indevido tanto das informações quanto dos sistemas utilizados em seu tratamento (LIMA, 2020, apud NUZZI & FERNANDES, 2022, p. 8).

Além de proteger contra ameaças externas, o princípio da segurança também busca assegurar que o tratamento dos dados esteja alinhado às normas legais vigentes, que promove um ambiente de conformidade e responsabilidade por parte dos agentes de tratamento. Dessa forma, cria-se um arcabouço normativo capaz de mitigar riscos inerentes à atividade de manipulação de dados pessoais, que garante a integridade e a confidencialidade das informações.

2.2.8 Princípio da prevenção

> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (BRASIL, 2018).

O princípio da prevenção, conforme prevê no artigo 6°, inciso VIII da LGPD, determina aos agentes de tratamento o dever de atuar de forma proativa para evitar a ocorrência de danos aos titulares. Trata-se de um comando que exige não apenas a correção de falhas após seu surgimento, mas, sobretudo, a antecipação de riscos que possam comprometer a segurança e a integridade dos dados pessoais. A lógica preventiva, portanto, deve estar presente em todas as fases do tratamento, desde a coleta até o eventual descarte dos dados.

Essa diretriz demanda uma postura contínua de vigilância e responsabilidade, que vá além do uso de tecnologias de proteção. A efetividade da prevenção depende também de uma gestão adequada de processos internos e de um ambiente organizacional comprometido com a cultura da proteção de dados. Para isso, é fundamental que haja políticas internas bem definidas, alinhadas com os princípios da LGPD, bem como o treinamento constante das equipes que

lidam com dados, de forma a garantir que saibam reconhecer e lidar com possíveis vulnerabilidades. (LIMA, 2020, apud NUZZI & FERNANDES, 2022, p. 8).

2.2.9 Princípio da não discriminação

> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; (BRASIL, 2018).

O Princípio da não discriminação tem como finalidade impedir que o tratamento de dados pessoais seja utilizado para fins discriminatórios, ilícitos ou abusivos. Essa diretriz protege os titulares contra práticas que possam gerar exclusão, restrição de direitos ou tratamento desigual com base em características pessoais, como origem, raça, gênero, religião, entre outras. (LIMA, 2020, apud NUZZI & FERNANDES, 2022, p. 8).

Ao se tratar de dados que revelam aspectos sensíveis da personalidade do indivíduo — como orientação sexual, convicções religiosas, posicionamentos políticos, origem racial, estado de saúde ou filiação sindical, a preocupação com o uso discriminatório dessas informações torna-se ainda mais evidente. Esses dados, por sua natureza, estão profundamente ligados à identidade e à dignidade da pessoa, e seu tratamento inadequado pode resultar em exclusões, preconceitos e até violações de direitos fundamentais (BIONI, 2020, p. 83). Diante disso, a LGPD dedica “um regime jurídico mais protetivo em relação a dados sensíveis com o intuito de frear práticas discriminatórias” (BIONI, 2020, p. 85).

2.2.10 Princípio da responsabilização e prestação de contas

> 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, 2018).

Finalmente, o princípio da responsabilização e prestação de contas estabelece que os agentes de tratamento de dados não devem apenas cumprir as normas legais, mas também ser capazes de demonstrar, de forma clara e documentada, que estão em conformidade com os princípios e diretrizes da legislação. Esse princípio introduz a lógica do *accountability*, que será discutido adiante, conforme Maciel indica, exige não só o cumprimento das normas, mas a capacidade de demonstrar essa conformidade perante a Autoridade Nacional de Proteção de Dados, a sociedade e os titulares (MACIEL, 2019, *apud* NUZZI & FERNANDES, 2022, p. 8). Como reforça Lima, não basta adotar boas práticas de forma abstrata; é necessário que sejam eficazes, documentadas e auditáveis (LIMA, 2020, *apud* NUZZI & FERNANDES, 2022, p. 8).

Acerca disso, mostram-se necessárias condutas transparentes, técnicas e responsáveis no tratamento de dados pessoais por parte dos controladores, pois a simples adoção de medidas de proteção não é suficiente; é necessário que tais medidas sejam eficazes e capazes de demonstrar sua real aplicação e aderência às regras estabelecidas (LIMA, 2020, *apud* NUZZI & FERNANDES, 2022, p. 8). Conclui-se, então, acerca dos princípios da LGPD que:

> (...)grande parte dos princípios tem todo o seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio dos quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais "modernos", como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquirido de acordo com a finalidade especificada para o tratamento dos dados, assegurando-se que os dados sejam pertinentes, proporcionais e não excessivos (minimização dos dados). (BIONI, 2020, p. 128).

Dito isso, os princípios basilares da Lei Geral de Proteção de Dados Pessoais (LGPD) refletem uma verdadeira mudança de paradigma na forma como os dados pessoais são tratados no ordenamento jurídico brasileiro. Ao colocar o titular no centro das decisões que envolvem suas informações, a LGPD promove o protagonismo do indivíduo e garante a efetivação da autodeterminação informativa. Cabe ressaltar que tais princípios também exigem dos agentes de tratamento de dados uma postura transparente, responsável e preventiva, que assegura que qualquer utilização de dados ocorra de forma livre, informada e consciente por parte do titular.

2.3 Direitos dos Titulares de Dados

Conforme o art. 5º, inciso V da LGPD, o titular de dados é "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". Além desse, destacam-se também o controlador de dados pessoais, caracterizado como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018, art. 5º, inciso VI), o operador de dados pessoais, definido como "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018, art. 5º, inciso VII), e o encarregado pelo tratamento de dados pessoais, descrito como "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (BRASIL, 2018, art. 5º, inciso VIII).

Diante disso, conforme destacam Feigelson e Siqueira (2019), a LGPD atribui direitos subjetivos aos titulares, que permite controlar o fluxo de seus dados pessoais. Para isso, o

Capítulo III da LGPD, que abrange os artigos 17 a 22, trata dos Direitos do Titular, os quais serão brevemente analisados a seguir. Cabe destacar que outros dispositivos também asseguram direitos aos titulares, como o artigo 1º, que estabelece que o tratamento de dados pessoais deve visar à proteção dos direitos fundamentais de liberdade e privacidade, e o artigo 2º, que apresenta fundamentos como o respeito à privacidade, autodeterminação informativa, liberdade de expressão e inviolabilidade da intimidade.

O artigo 17 assegura a titularidade dos dados pessoais a toda pessoa natural, com vistas à garantir os seus direitos fundamentais de liberdade, intimidade e privacidade.

O artigo 18 apresenta um conjunto de direitos subjetivos que conferem ao titular o controle e a autodeterminação informativa sobre seus dados, desde a coleta até sua eventual exclusão. Nesse mesmo artigo, é apresentado um conjunto de direitos subjetivos que conferem ao titular o controle e a autodeterminação informativa sobre seus dados, desde a coleta até sua eventual exclusão. Os incisos I e II desse artigo tratam do direito à confirmação da existência de tratamento e ao acesso aos dados. Tais prerrogativas são descritas por Vieira (2023):

> Os direitos de confirmação e acesso aos dados pessoais constituem mecanismos aptos a garantir meios para que a cidadania possa jogar luz sobre o conjunto dos dados pessoais coletados e tratados, com amparo nos princípios da transparência e da prestação de contas. (VIEIRA, 2023, p. 5).

Com base nisso, informações como os dados coletados, a forma e duração do tratamento, e a identificação do controlador devem ser disponibilizadas ao titular. Esses direitos estão relacionados aos princípios da transparência e da prestação de contas, que confere legitimidade, responsabilidade e confiança ao tratamento de dados.

O inciso III refere-se à correção de dados incompletos, inexatos ou desatualizados, conforme destaca Vieira (2023):

> Quando cientes da incompletude, inexatidão ou da desatualização das suas informações pessoais em bancos de dados de pessoas jurídicas, seja mediante o exercício do direito da confirmação ou acesso, seja mediante outra forma de conhecimento dessas circunstâncias, os titulares poderão pleitear a correção dessa situação aos agentes de tratamento. (VIEIRA, 2023, p. 5).

Paralelamente, o princípio da qualidade dos dados pessoais, previsto no artigo 6º, inciso V, da LGPD, serve de base para esse direito, pois assegura que os dados dos titulares sejam tratados com exatidão, clareza, pertinência e estejam devidamente atualizados, conforme a finalidade do tratamento e a real necessidade de sua utilização. O inciso IV aborda o direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em

desconformidade com a LGPD. Para melhor compreensão desse direito, convém abordar as definições de anonimização, bloqueio e eliminação.

A LGPD define a anonimização como "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (art. 5º, inc. XI). Nesse sentido, essa prática visa proteger a identidade dos titulares, especialmente diante da crescente sofisticação tecnológica e das ameaças cibernéticas, uma vez que:

> (...) a grande questão cinge em torno do grau de segurança e confiança na irreversibilidade da anonimização. Isto porque inúmeros estudos vêm demonstrando como é fácil identificar pessoas a partir de alguns tributos, mesmo que os dados sejam públicos. O processamento de dados por algoritmos, por exemplo, permite a reidentificação de dados anonimizados como preferências de consumo, transações comerciais, etc. (FEIGELSON & SIQUEIRA, 2019, p. 123).

Bruno Miragem (2019) complementa que a anonimização é um dos principais recursos destinados a preservar a privacidade do titular de dados, em que consiste na modificação da forma original dos dados, de maneira que se torne impossível identificar a pessoa a quem eles se referem. Trata-se, portanto, mais de um resultado a ser alcançado do que do processo em si. No entanto, é importante destacar que, na prática, alcançar um anonimato completo no ambiente digital atual é algo praticamente inalcançável (MIRAGEM, 2019, p.22).

O bloqueio é definido como a "suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados" (art. 5º, inc. XIII); enquanto a eliminação caracteriza-se pela "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado" (art. 5º, inc. XIV). Conforme se observa Bruno Feigelson e Antonio Siqueira (2019) o bloqueio é uma medida temporária, enquanto a eliminação é uma medida definitiva que deve ser aplicada na circunstância do tratamento de dados ser ilícito ou no seu término, medida a ser aplicada na circunstância de o tratamento de dados ser ilícito ou quando ocorrer o seu término, em conformidade com o artigo 16, que autoriza a conservação dos dados apenas para as finalidades nele descritas. (FEIGELSON & SIQUEIRA, 2019, p. 123).

Tal direito relaciona-se aos princípios da finalidade, adequação e necessidade (art. 6º, incisos I, II e III), à medida que propõe que os dados coletados devem atingir a finalidade pretendida, sem excessos e de forma a afastar dados incompatíveis com o contexto e finalidade.

O inciso V trata sobre a portabilidade de dados, em que, o titular de dados pode solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto, mediante

requisição expressa, mas não se aplica em situações em que os dados já tenham sido anonimizados pelo controlador (FEIGELSON & SIQUEIRA, 2019, p. 124). Já no inciso VI, estabelece-se o direito à eliminação dos dados pessoais tratados com o consentimento do titular, sem que isso implique revogação do artigo 16 da LGPD, o qual determina que o controlador deve eliminar os dados após o término do tratamento.

É igualmente importante ressaltar que o agente de tratamento deve adotar, em tempo hábil, as providências necessárias diante da solicitação de eliminação, enquadrando-se tal obrigação na cláusula geral da boa-fé objetiva (FEIGELSON & SIQUEIRA, 2019, p. 124).

O inciso VII trata do direito à informação sobre as entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados pessoais. Tal prerrogativa decorre diretamente do princípio da transparência, conforme se destaca a seguir:

> (...) é uma decorrência direta do princípio da transparência, em que o titular de dados tem o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. (FEIGELSON & SIQUEIRA, 2019, p. 124).

De forma complementar, Lucas Vieira (2023) ressalta que, em tese, "o controlador deverá ter um inventário de todas as entidades com as quais compartilhou dados pessoais de todos os titulares para que consiga cumprir esse direito" (VIEIRA, 2023, p. 9). Ainda segundo o autor, essa prerrogativa reforça a transparência nas operações de tratamento e impõe ao controlador a obrigação de manter um controle estruturado sobre os fluxos de dados sob sua responsabilidade. Contudo, sua implementação prática impõe desafios significativos, especialmente para microempresas, empresas de pequeno porte e negócios de médio porte, que frequentemente carecem de recursos técnicos ou humanos para gerenciar esse mapeamento de forma contínua e eficaz.

Soma-se a isso a dificuldade de identificar todas as entidades envolvidas no tratamento de dados quando são utilizados cookies e serviços terceirizados, muitas vezes integrados aos sites corporativos por prestadores externos, o que pode comprometer o cumprimento integral desse direito (VIEIRA, 2023, p. 9). O direito à informação sobre a possibilidade de não fornecer consentimento, bem como sobre as consequências dessa negativa, está previsto no inciso VIII do artigo 18 da LGPD.

Essa prerrogativa reforça, o princípio da transparência e está intrinsecamente relacionada à autodeterminação informativa e ao livre desenvolvimento da personalidade, fundamentos expressos no artigo 2º da Lei. Garantir ao titular o conhecimento de que ele pode recusar o consentimento é essencial para preservar sua liberdade de escolha e evitar práticas

que possam constrangê-lo ou contrariar suas convicções pessoais. A ausência dessa informação compromete a legitimidade do consentimento, uma vez que este deve ser livre, informado e inequívoco (VIEIRA, 2023, p. 10).

Além disso, se o indivíduo não tem ciência das consequências de negar seu consentimento, torna-se incapaz de avaliar adequadamente os prós e contras e, assim, de tomar a melhor decisão quanto ao tratamento de seus dados pessoais (FEIGELSON & SIQUEIRA, 2019, p. 125).

Por fim, o inciso IX, reforça o § 5º do art. 8º da LGPD, o qual determina que a revogação do consentimento pode ser realizada a qualquer tempo, mediante a manifestação expressa do titular, por meio de um procedimento gratuito e de fácil acesso, mas é importante destacar que os tratamentos de dados realizados com base no consentimento antes da revogação permanecem válidos, exceto se houver solicitação para a eliminação desses dados. A revogação, como ato unilateral, impõe o encerramento do tratamento por parte dos agentes envolvidos, inclusive no que se refere a terceiros que eventualmente tenham recebido os dados. Ainda assim, conforme observa Lucas Vieira (2023), a complexidade dos fluxos informacionais na era digital especialmente em ambientes como aplicativos que compartilham dados com diversas empresas pode dificultar o pleno cumprimento desse direito, de forma a exigir das organizações esforços técnicos significativos, ainda que nem sempre suficientes para assegurar o encerramento completo do tratamento. Entretanto, a LGPD é clara ao exigir que os controladores implementem mecanismos eficazes de *compliance*, com a devida organização de bancos de dados, sistemas e registros de consentimento. (VIEIRA, 2023, p. 10).

O artigo 19 dispõe sobre o direito à requisição de informações pelo titular, de forma a facilitar para o usuário a obtenção de informações dos agentes de tratamento. Esse mesmo artigo, nos incisos I e II determina que as informações solicitadas em formato simplificado sejam entregues imediatamente e, solicitadas em declaração completa, devem ser providenciadas em até 15 (quinze) dias. É importante, porém, ressaltar, que esse prazo pequeno pode tornar-se, para os agentes de tratamento de dados, a obrigação inviável ou extremamente onerosa. Por esta razão, é disposto no § 4º que a autoridade nacional pode excepcionar o cumprimento do referido prazo, de forma a criar prazos factíveis. (FEIGELSON & SIQUEIRA, 2019, p. 126).

Vale destacar, com base no que é discutido por Bruno Feigelson e Antonio Siqueira (2019), resumidamente, que no parágrafo 1º destaca que os dados deverão ser armazenados de forma a permitir a legibilidade e a facilidade do titular de dados. O parágrafo 2° dispõe o direito do dado de solicitar as informações por meio eletrônico ou impresso. O parágrafo 3° destaca a

importância da disponibilização das informações que possibilite ao titular de dados utilizá-las em outra aplicação (FEIGELSON & SIQUEIRA, 2019, p. 126).

O artigo 20 dispõe sobre o direito à revisão de decisões automatizadas e garante ao titular a possibilidade de recusar a submissão a decisões tomadas exclusivamente por sistemas automatizados, caso tais decisões tenham impacto sobre seus direitos legais ou afetem de forma relevante a sua esfera pessoal (FEIGELSON & SIQUEIRA, 2019, p. 127). Finalmente, o fundamento da norma prevista no artigo 21 é garantir que o titular não sofra qualquer prejuízo por exercer os direitos assegurados no Capítulo III da LGPD, e o artigo 22 confere o direito do titular de exercer os seus direitos em juízo, de forma individual ou coletiva.

Assim, no cenário atual marcado pela crescente digitalização das relações sociais e econômicas, os direitos dos titulares de dados pessoais ocupam papel central na proteção da personalidade humana. Dessa forma, a Lei Geral de Proteção de Dados Pessoais (LGPD) consagra um conjunto de garantias que não se limitam à proteção da privacidade, mas que se estendem à autodeterminação informativa e à liberdade individual frente ao poder de coleta, análise e uso massivo de dados por agentes públicos e privados.

3 ACCOUNTABILITY: ORIGEM, DEFINIÇÕES E DESDOBRAMENTOS

Esta seção tem por finalidade aprofundar o estudo sobre o princípio da *accountability* no contexto da proteção de dados pessoais, em especial quanto à sua estrutura conceitual e histórica. Para tanto, inicia-se pela reconstrução de sua origem nas diretrizes da Organização para Cooperação e Desenvolvimento Econômico (OCDE), de forma a destacar o papel que a organização desempenhou na consolidação da *accountability*. Em seguida, analisa-se seu caráter multifacetado e adaptável, cuja flexibilidade permite diferentes interpretações e formas de operacionalização conforme o contexto regulatório.

Além disso, discute-se a sua dimensão temporal, especialmente perspectiva preventiva (*ex ante*) e repressiva (*ex post*) da *accountability*, de forma a ressaltar sua aplicação ao longo do tratamento de dados. Por fim, será explorada a aplicação da *accountability* no cenário da "metarregulação".

3.1 A origem da *accountability* no campo da proteção de dados e o seu conceito multiforme

Em primeiro lugar, cabe salientar a origem do princípio da *accountability* para que posteriormente, seja possível defini-lo. Desta feita, a *accountability*, enquanto princípio propriamente dito, parece ter sido enunciado pela primeira vez no processo de redação e aprovação das diretrizes sobre privacidade da Organização para Cooperação e Desenvolvimento Econômico (OCDE) (BIONI, 2022, p. 5).

A OCDE tem como sua precursora a Organização para a Cooperação Econômica Europeia (OEEC), criada para administrar a assistência americana e canadense, no âmbito do Plano Marshall, para a reconstrução da Europa após a Segunda Guerra Mundial. Posteriormente, em 1960, a OEEC é transformada na OCDE que vigora hodiernamente.[2]

Alicerçada no objetivo de promover um maior bem-estar em todo o mundo, com vistas à orientar inclusive os governos na formulação de políticas que favoreçam um crescimento resiliente, inclusivo e sustentável[3], a OCDE em 1980, emite as diretrizes para a "proteção da

[2] "The forerunner of the OECD was the Organisation for European Economic Co-operation (OEEC), which was formed to administer American and Canadian aid under the Marshall Plan for the reconstruction of Europe after World War II. The Convention transforming the OEEC into the OECD was signed at the Chateau de la Muette in Paris on 14 December 1960 and entered into force on 30 September 1961" Disponível em: https://www.oecd.org/en/about/history.html. Acesso em: 29/06/2025.

[3] "Since then, the OECD's vocation has been to deliver greater well-being worldwide by advising governments on policies that support resilient, inclusive and sustainable growth." Disponível em: https://www.oecd.org/en/about/history.html. Acesso em: 29/06/2025.

privacidade e fluxo transnacional de dados pessoais" (BIONI, 2022, p.19). Repisa-se que tais diretrizes pavimentaram o caminho para uma discussão voltada à uniformidade no tratamento de dados pessoais em diferentes jurisdições, "na medida em que são a espinha dorsal pela qual se constitui o corpo de normas de proteção de dados pessoais ao redor do mundo" (BIONI, 2022, p. 19).

Desta feita, nota-se que a OCDE - com foco nos seus objetivos elencados acima, especialmente para o favorecimento de um crescimento resiliente, inclusivo e sustentável, busca estabelecer de certa medida, parâmetros e medidas para a harmonização entre os países na implementação das normas de proteção de dados, e não propriamente a criação de um sistema uniforme (BIONI, 2022, p.22). Assim, o objetivo das diretrizes parece priorizar a uniformização da aplicação das normas, e não criação de um sistema, cria-se assim, abertura nesse contexto para o emprego da *accountability* em seu cerne.

Neste diapasão, surgem diferentes reflexões quanto à forma de aplicação do referido princípio, especialmente quanto à extensão da sua definição, o seu respectivo papel no sistema de proteção de dados como um todo e, principalmente, a quem a *accountability* deveria ser direcionada. A questão paira, então, sobre a incidência, ou seja, se a normativa deveria incidir sobre qualquer agente da cadeia de tratamento de dados ou somente sobre aquele responsável pelas decisões relativas ao tratamento de dados pessoais, o controlador (BIONI, 2022, p. 23).

Com a finalidade de definir de forma mais assertiva, a OECD define no memorando explanatório que a aplicação pode ser realizada tanto para o controlador, quanto para os demais agentes da cadeia de tratamento, conforme se observa:

> O controlador de dados decide sobre os dados e as atividades de processamento de dados. É em seu benefício que o processamento de dados é realizado. Assim, é essencial que, de acordo com a legislação nacional, a responsabilidade pelo cumprimento das regras e decisões de proteção de privacidade seja atribuída ao responsável pelo tratamento de dados, que não deve ser dispensado desta obrigação apenas porque o processamento de dados é realizado em seu nome por outra parte, tal como um serviço de bureau. Por outro lado, nada nas Diretrizes impede que o pessoal das agências de serviço, "usuários dependentes" (ver parágrafo 40) e outros também sejam responsabilizados. Por exemplo, as sanções contra violações das obrigações de confidencialidade podem ser dirigidas contra todas as partes encarregadas do tratamento de informações pessoais (cf. parágrafo 19 das Diretrizes). A prestação de contas sob o parágrafo 14 **refere-se à prestação de contas apoiada por sanções legais, bem como à prestação de contas estabelecida por códigos de conduta**, por exemplo, (OECD, *apud* BIONI, 2022, p. 27, grifo do autor)

Depreende-se que a OCDE adotou uma concepção ampla para a *accountability* que não se restringe ao controlador, mas se estende a todos os agentes envolvidos no tratamento de dados pessoais. Tal entendimento reforça a ideia de que a proteção de dados exige uma estrutura

de corresponsabilidade, na qual cada agente da cadeia de tratamento assume deveres proporcionais ao seu papel. Esse modelo está em consonância com a lógica da LGPD, especialmente no que tange aos princípios da prevenção, segurança e responsabilização, que impõem aos agentes de tratamento a adoção de medidas técnicas e organizacionais adequadas para garantir a conformidade.

Nesse mesmo sentido, Bruno Ricardo Bioni destaca que diante da concepção adotada pela OCDE, a *accountability* passa a ser entendida como um conceito "camaleão", conforme as suas palavras:

> Essa disputa em torno do princípio da *accountability* revela a decisão em adotar um conceito enxuto e, ao mesmo tempo, **camaleão que fosse capaz de se amoldar a estratégias distintas de implementação das normas de proteção de dados pessoais**. (BIONI, 2022, p. 27, grifo nosso)

Diante da assunção do caráter camaleônico, indicado anteriormente, é notório que a *accountability* é um conceito que se apresenta de maneira multifacetada e dinâmica. Tal característica permite que o princípio seja interpretado e operacionalizado de diferentes formas, a depender do contexto normativo e das estratégias regulatórias adotadas.

Brendan Van Alsenoy,[4] no contexto da General Data Protection Regulation (GDPR), a qual a LGPD, também observa que a *accountability* assume uma posição central na estrutura regulatória europeia, para ele:

> A *accountability* é um conceito com muitas dimensões. Tem sido caracterizada por estudiosos como um conceito 'elusivo' e até mesmo 'camaleônico', uma vez que pode significar coisas muito diferentes para pessoas distintas. Em seu significado essencial, *accountability* refere-se à existência de uma relação pela qual uma entidade tem a capacidade de convocar outra entidade e exigir uma explicação e/ou justificativa por sua conduta. Com o tempo, diferentes instrumentos de proteção de dados promoveram diferentes tipos de mecanismos de *accountability*. Na GDPR, o princípio da responsabilização é usado principalmente para indicar que os controladores não são apenas responsáveis por implementar medidas apropriadas para obedecer a GDPR, o regulamento, mas também devem ser capazes de demonstrar a conformidade a pedido das autoridades de supervisão. (VAN ALSENOY, 2019, p. 318, tradução nossa).[5]

[4] "Dr. Brendan Van Alsenoy is Deputy Head of Unit, Policy and Consultation at the European Data Protection Supervisor (EDPS). He previously worked as a Legal Advisor and Acting Head of Unit at the Belgian Data Protection Authority. Prior to that, he worked as a legal researcher at the KU Leuven Centre for IT & IP Law, with a focus on data protection and privacy, intermediary liability and trust services. In 2012, he worked at the Organisation for Economic Co-operation and Development (OECD) to assist in the revision of the 1980 OECD Privacy Guidelines." Disponível em: https://www.iicom.org/profile/brendan-van-alsenoy/. Acesso em 10/07/2025

[5] "Accountability is a concept with many dimensions. It has been characterized by scholars as being an 'elusive' and even 'chameleon-like' concept, because it can mean very different things to different people. In its core meaning, accountability refers to the existence of a relationship whereby one entity has the ability to call upon another entity and demand an explanation and/or justification for its conduct. Over time, different data protection instruments have advanced different types of accountability mechanisms. In the GDPR, the principle of accountability is mainly used to signal that controllers are not only responsible for implementing appropriate

Van Alsenoy (2019) destaca o caráter multifacetado da *accountability,* na busca de implementar medidas técnicas e organizacionais adequadas e na comprovação da comprovar sua efetividade quando solicitado, conferindo à *accountability* um papel operativo, além de um mero princípio declaratório. Tal característica introduz um elemento proativo de governança, no qual os agentes não apenas devem respeitar as normas, mas também construir um ecossistema que a *accountability* seja um mecanismo. Essa abordagem reflete uma mudança paradigmática, com foco da conformidade formal para uma conformidade demonstrável.

Danielle Rached (2016), nesse mesmo entendimento, observa-se que o conceito de *accountability* é marcado por ambivalência e múltiplas dimensões que inviabilizam sua redução a uma noção unívoca. A autora afirma que:

> O conceito de accountability é ambivalente. Sua dualidade se expressa de três maneiras distintas que estão complexamente entrelaçadas entre si. O conceito pode: (i) apresentar um caráter descritivo ou normativo; (ii) abarcar uma relação política ou extrapolítica; e (iii) ser moldado por propriedades legais ou extralegais. Para obter uma compreensão satisfatória desse conceito, deve-se situar essas três dimensões paralelas em um contexto adequado e coerente. Caso alguma dessas três dimensões seja deixada de fora, a capacidade explicativa ou o apelo normativo do conceito diminuirão significativamente. Caso elas sejam inadvertidamente confundidas e suas conexões obscurecidas, a aplicação do conceito torna-se ambígua." (RACHED, 2016, p. 319, tradução nossa).[6]

Após as primeiras definições da *accountability*, a OCDE inicia em 2008 um processo de revisão das diretrizes estabelecidas anteriormente, baseada na percepção de que a *accountability* seria um instrumento para a mudança de foco da sua aplicabilidade, passando de um sistema que busca pela harmonização, para um sistema que busca pela interoperabilidade (BIONI, 2022, p. 31).

Com o intuito de examinar as discussões relativas às diretrizes da OCDE, Bruno Bioni (2022) identifica três marcos centrais na revisão do conceito de *accountability*: (i) o ciclo de conferências realizado em comemoração aos trinta anos das diretrizes — Paris 1, Jerusalém e

---

measures to comply with the GDPR, but must also be able to demonstrate compliance at the request of supervisory authorities". (VAN ALSENOY, 2019, p. 318).

[6] "The concept of accountability is Janus-faced. Its duality is expressed in three distinct ways that are complexly intertwined with each other. The concept can: (i) display a descriptive or normative character; (ii) capture a political or extra-political relationship; and (iii) be shaped by legal or extra-legal properties. In order to get a satisfactory grip on that concept, one should put these three parallel dimensions into an adequate and coherent context. Should any of these three dimensions be left out of the picture, the explanatory capacity or normative appeal of the concept will significantly recede. Should they get inadvertently conflated and their connections obscured, the application of the concept becomes equivocal.". (RACHED, 2016, p.319)

Paris 2;[7] (ii) o conjunto de documentos publicados entre 2008 e o início de 2013;[8] e (iii) as discussões sobre a transferência internacional de dados.[9]

Diante desses marcos, observa-se que a *accountability* deixou de ser um conceito mais tímido para se consolidar como um princípio normativo dotado de mecanismos concretos de implementação. As discussões no âmbito da OCDE, os desdobramentos nas conferências internacionais e a vinculação do princípio a mecanismos, como relatório de impacto à proteção de dados, código de boas condutas, programas de governança de dados, selos de certificação e *privacy enhancing technologies*, demonstram uma transição significativa: de uma definição tímida para um modelo orientado à demonstração de conformidade e à responsabilização efetiva dos agentes, inclusive em contextos como transferências internacionais de dados.

Portanto, o princípio da *accountability* passa a desempenhar, primeiramente, o papel de harmonizar diferentes abordagens regulatórias, com os resultados em detrimento dos meios na aplicação das normas de proteção de dados pessoais. Em segundo plano, assumiu a função de servir como uma válvula de escape para livre fluxo de informações, evita-se que agentes econômicos fossem prejudicados na situação de estarem localizados em países sem uma estrutura legal e institucional capaz de assegurar um nível adequado de proteção de dados, desde que suas próprias estruturas organizacionais pudessem suprir essa lacuna estatal (BIONI, 2022, p.35). Nas palavras de Danielle Rached (2016):

---

[7] "**a) no ciclo de conferências em comemoração ao aniversário de trinta anos – Paris 1, Jerusalém e Paris 2**, accountability foi um tema recorrente. Destacam-se as falas dos representantes dos Estados Unidos – Hugh Stevenson à época diretor de relações governamentais da Federal Trade Commission – e da União Europeia – Peter Hustinx à época Comissário Europeu de Proteção de Dados. O americano afirmou que tal princípio deveria mudar a dinâmica até então existente entre reguladores e regulados. Este foi secundado pelo garante europeu ao considerar que o sistema de notificações da então diretiva de proteção de dados deveria ser reconsiderado, devendo-se apostar e estimular a capacidade dos agentes de tratamento de dados para colocar a tecnologia a favor da proteção de dados (e.g., privacy by design e by default). São falas convergentes vindas de atores que representam os extremos de um sistema que privilegia autorregulação e outro que aposta mais no aparato estatal-legal (heterorregulação); a.1) vale destacar que, também nesse período, aconteceu a reunião anual global de autoridades supervisoras e comissários de privacidade em Madrid, quando é extraída uma resolução que enuncia e conceitua o princípio da *accountability* pela primeira vez em tal fórum. Ficou a cargo da Autoridade de Proteção de Dados espanhola organizá-la, tendo sido mais tarde uma das painelistas no ciclo de conferência de aniversário das guidelines;" (BIONI, 2022, p. 32-33, grifo do autor)

[8] "**b) todos os documentos de 2008 ao início de 2013**, faziam não só referência ao princípio da accountability, mas, sobretudo, apontavam quais instrumentos o materializariam. Utilizou-se a técnica de, ao listar mecanismos como relatório de impacto à proteção de dados, código de boas condutas, programas de governança de dados, selos de certificação e privacy enhancing technologies correlacioná-los ao referido princípio. Uma espécie de recapeamento do **buraco normativo** deixado por uma definição que não enunciava os elementos de exteriorização da accountability, isto é, uma definição normativamente tímida;" (BIONI, 2022, p.34 – 35, grifo do autor)

[9] "**c)Transferência internacional**: se os agentes de tratamento de dados conseguissem demonstrar maturidade organizacional em termos de proteção de dados pessoais, deveriam ser premiados com possibilidade de transferência internacional, mediante adesão das chamadas normas corporativas globais pelas quais a organização que é considerada como tendo um nível adequado de proteção de dados, e não o país onde ela – sede e subsidiárias – está localizada. Dessa forma, independe se o país destinatário tem um aparato estatal-legal, desde que o agente econômico demonstre a sua responsabilidade a esse respeito." (BIONI, 2022, p.35, grifo do autor)

> *Accountability* é anunciada, em outras palavras, como um objetivo digno de elogio a ser perseguido pelo direito e pela política, não importa onde ocorra, seja local, regional, nacional ou internacionalmente. Ela protegeria o responsável pela prestação de contas e, de várias maneiras, talvez de forma contraintuitiva, também pode beneficiar quem recebe essa prestação." (RACHED, 2016, p. 318, tradução nossa)[10].

Conforme destacado no segundo capítulo do presente trabalho, a LGPD passa por diferentes alterações e mutações no seu teor normativo. Em virtude disso, a lei gera espaço para que os agentes se auto-organizassem e passem a tratar os dados pessoais com maior discricionariedade na adoção de medidas de conformidade das suas atividades de tratamento de dados (BIONI, 2022, p.70).

Ademais, segundo Ricardo Bioni (2022), "o princípio da *accountability* na LGPD é o que melhor ilustra o processo de mutação pelo qual o texto da lei sofreu (...)" (BIONI, 2022, p. 70).

Em suma, o princípio da *accountability* não se limita ao mero cumprimento formal das normas, mas impõe uma postura ativa e transparente dos agentes no tratamento de dados pessoais. Para fins analíticos, Bioni (2022) sintetiza que:

> (...) ***accountability* é um termo histórico e intimamente ligado à filosofia regulatória estadunidense de menor intervenção estatal**. Além de forjar a sua significação desde o nascimento das leis de proteção de dados, foi a delegação norte-americana que venceu a disputa conceitual em torno da *accountability* enquanto um princípio nas diretrizes da OCDE. (BIONI, 2022, p. 72, grifo do autor).

Portanto, o caráter instrumentalista da *accountability*, é o que justifica a sua aplicação em diferentes cenários, para Rached (2016):

> Não existe uma "teoria pura" da accountability, no que diz respeito a uma prescrição carregada de valores. Ou seja, o apelo do chamado contemporâneo à prestação de contas não deriva da *accountability* em si. Esse apelo não é autossuficiente, mas sim acessório a um ideal externo, seja ele explicitamente articulado ou não. [...] A forma mais plausível de defender e justificar a accountability, nesse sentido, é instrumentalista. Em vez de ser um fim em si mesma, ela é um meio para um fim. Mais precisamente, é um meio para uma série de fins distintos e geralmente conflitantes que esses ideais externos articulam. Não existe um único fim autoevidente a ser promovido." (RACHED, 2016, p. 334, tradução nossa)[11]

---

[10] "Accountability is announced, in other words, as a praiseworthy goal to be pursued by law and politics no matter where it takes place, be it locally or regionally, nationally or internationally. It would protect the account-holder and, in several ways, perhaps counter-intuitively, it may benefit the accountee as well." (RACHED, 2016, p. 318)

[11] "There is no such thing as a 'pure theory' of accountability, as far as a value-laden prescription is concerned. That is, the appeal of the contemporary call for accountability does not stem from accountability tout court. Such call is not self-standing, but rather ancillary to an external ideal, be it explicitly articulated or not." (RACHED, 2016, p.334)

Para além, é necessário ressaltar que a *accountability*, não opera isoladamente. Isto é, se insere em um campo semântico mais amplo, que envolve ainda os termos da língua inglesa, como *liability, responsibility* e *answerability*. Todos esses termos, embora traduzidos para o português como "responsabilidade" possuem significados jurídicos e normativos distintos, especialmente no contexto da proteção de dados pessoais.

Em primeiro lugar, a *liability* representa o núcleo clássico da responsabilidade civil, isto é, o dever de reparar o dano culposo, após a ocorrência. Nesta seara, Nelson Rosenvald e José Luiz de Moura Faleiros Júnior (2022) destacam que a *liability* se apresenta como uma "última trincheira" (*last resort*) da proteção jurídica, com atuação na ocasião de outras esferas preventivas e regulatórias falharam. Assim, ela não constitui o epicentro da responsabilidade civil contemporânea, mas sim sua "epiderme", pois já não é suficiente para lidar com os desafios impostos pelo tratamento massivo e contínuo de dados pessoais.

> Metaforicamente, se poderia dizer que a **liability não é o epicentro da responsabilidade civil, mas apenas a sua epiderme**. Em verdade, trata-se apenas de um *last resort* para aquilo que se pretende extrair da responsabilidade civil no século XXI, destacadamente na tutela dos dados pessoais, uma vez que a definição de regramentos próprios não advém de uma observação ontológica (ser), mas de uma expectativa deontológica (dever-ser) da interação entre inovação e regulação em um ecossistema no qual o risco é inerente às atividades exploradas. (...) É indubitável que o potencial do Big Data ultrapassa as meras aplicações práticas, pois também torna possível a interpretação de comportamentos humanos. (...) **No apogeu da sociedade da informação, considerar a "responsabilidade" a partir de uma leitura conceitual simplista revela-se inconcebível** (ROSENVALD; FALEIROS JÚNIOR *In* FRAZÃO; CUEVA, 2022, grifo nosso).

Em contraste, a *accountability* amplia o escopo da responsabilidade ao incorporar uma dimensão que exige dos agentes de tratamento a demonstração ativa de conformidade. Na LGPD, isso se concretiza por meio de medidas preventivas como a implementação de programas de compliance, avaliação de impacto, regras de boas práticas e estruturas de governança, nos termos do artigo 50 da LGPD[12]. Assim, a *accountability* não apenas complementa, mas transcende a *liability*, oferece um modelo regulatório orientado à mitigação de riscos e à indução de comportamentos responsáveis. Inclusive, pode ser utilizada para a fixação das sanções de natureza unitiva e da quantificação das multas pela ANPD, nos termos do artigo 52 da LGPD (ROSENVALD, 2020).

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

Ainda nesse panorama, o termo *responsibility* é definido por Nelson Rosenvald como "o sentido moral de responsabilidade, voluntariamente aceito e jamais legalmente imposto" (ROSENVALD, 2022). Para Rosenvald (2020), no campo da proteção de dados, a *responsibility* assume duas frentes, quais sejam:

> No campo do tratamento dos dados pessoais, assume duas vertentes: para agentes de tratamentos, significa a inserção da ética no exercício de sua atividade; para os titulares dos dados, a educação digital, no sentido de "...capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania" (art. 26 MCI). Se uma pessoa não sabe o que acontece com os seus dados, não poderá se proteger. Conceitos como de "anonimização de dados", sequer são dominados por advogados, quanto mais pelo cidadão em geral. Por isto a educação digital não se confunde com o direito fundamental à inclusão digital (tratado neste espaço na coluna de 23/10 por Carlos Edison do Rêgo e Diana Loureiro). A educação digital extrapola a ideia de acesso à internet, alcançando o sentido de uma autodeterminação informativa, tal como delineado entre os fundamentos da LGPD (art. 2, II, lei 13.709/18) (ROSENVALD, 2020).

Para além da aplicabilidade aos agentes de tratamento, Rosenvald (2022) assinala que o titular de dados também precisa compreender os fluxos e os riscos inerentes ao tratamento de seus dados para exercer sua autonomia de forma plena — o que exige mais do que inclusão digital: exige capacitação.

Quanto à *answerability*, cuja tradução ao português seria "explicabilidade". Trata-se de uma dimensão da responsabilidade centrada justificação das decisões e "materializada no dever recíproco de construção da fidúcia a partir do imperativo da transparência " (ROSENVALD; FALEIROS JÚNIOR In FRAZÃO; CUEVA, 2022). No contexto da proteção de dados, a *answerability* se concretiza especialmente no artigo 20 da LGDP, que assegura ao titular o direito de solicitar a revisão de decisões automatizadas que afetem seus interesses. Nesse sentido a *answerability*, é aplicada na "*ability to appeal*, ou seja, quando é conferido ao titular dos dados o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses (...)" (ROSENVALD, 2022).

Em paralelo, para Elena Simina Tănăsescu (2011), *responsibility* corresponde a um preceito ético com status de princípio, como o da igualdade e da liberdade, que envolve o cuidado com as consequências das próprias ações e refere-se aos deveres do indivíduo perante a coletividade. A *liability*, por sua vez, é compreendida como responsabilidade legal, implementada na norma jurídica voltada à responsabilização individual. Já a *accountability*, apresentada pela autora apenas no ambiente público, relaciona-se ao dever de agentes públicos

prestarem contas de seus atos, em conformidade com normas e regulamentos, aproxima-se da responsabilidade administrativa (TĂNĂSESCU *apud* DOS SANTOS, 2023, p.142).

Assim, diante das perspectivas supracitadas, enquanto a *liability* se relaciona à responsabilização após a ocorrência do dano, e a *responsibility* e a *answerability* lidam com dimensões éticas e procedimentais do agir responsável, a *accountability* distingue-se como conceito normativo central, pois atua enquanto um mecanismo de governança de dados. Ela combina os aspectos preventivos e corretivos da responsabilidade, integra as exigências de conformidade com a necessidade de prestação de contas efetiva.

Dessa forma, a *accountability*, de forma distinta em relação aos demais conceitos, reside exatamente na sua capacidade de operar simultaneamente como diretriz regulatória e mecanismo de conformidade, ocupa um lugar central na arquitetura normativa da proteção de dados pessoais no Brasil.

3.2 A perspectiva *ex ante* e *ex post* sob a ótica da *accountability*

De forma a analisar a *accountability,* faz-se necessário considerar também o aspecto temporal da sua aplicabilidade, em especial, como se dão as perspectivas das racionalidades *ex ante* e *ex post* à luz das interações da *accountability.* Isto é, de forma repressiva (*ex post*) ou de forma preventiva (*ex ante*). Assim, a prestação de contas pelo agente de tratamento pode ocorrer em qualquer tempo, entretanto, o que sobrevém da aplicação no momento, pode gerar efeitos mais ou menos concretos (RACHED, 2016, p. 331).

De forma histórica, segundo Bioni (2022), a proteção de dados assumiu primordialmente uma racionalidade *ex ante* (BIONI, 2022, p. 222). Conforme ele destaca:

> Historicamente, proteção de dados sempre foi ritmada por uma racionalidade *ex ante*. Isto é, a padronização de comportamentos com contornos prestabelecidos em lei ou a partir de regulamentação administrativa, a serem observados antes do lançamento de uma atividade de tratamento de dados no meio ambiente. Em vez de apostar em uma lógica prioritariamente repressiva por meio da responsabilização civil e/ou penal do agente de tratamento de dados, caso este viesse causar dano a outrem. (BIONI, 2022, p. 223).

Assim, Rosenvald e Faleiros Júnior (2022), destacam que "no plano *ex ante,* a *accountability* é compreendida como um guia para controladores e operadores", em especial pela "inserção de regras de governança e boas práticas" (ROSENVALD; FALEIROS JÚNIOR *In* FRAZÃO; CUEVA, 2022). Nota-se, portanto, a primazia da aplicação da perspectiva preventiva da *accountability.*

Explica-se que tal primazia ocorre em virtude de três aspectos principais. Em primeiro lugar, a natureza do objeto regulado poder assumir diferentes usos, uma vez que está em constante movimento. Somado a isso, a alta carga de discricionariedade dos agentes de tratamento, em virtude do caráter aberto das normas. Por fim, o risco de que seja impossível retornar ao *status quo ante* em uma eventual violação de segurança (BIONI, 2022, p.223). Assim, conforme destaca Bioni:

> Não é por outra razão que o princípio da *accountability* é definido como a demonstração da eficácia dessas medidas. Isso implica, portanto, não apenas na adoção de medidas preventivas (*ex ante*), mas, sobretudo, que sejam potencialmente objeto de experiencias participativas. (BIONI, 2022, p.224).

Diante do exposto, é possível concluir que a aplicabilidade da *accountability* sob uma lógica predominantemente *ex ante*, prioriza a prevenção de danos em vez da mera repressão a condutas lesivas. Tal racionalidade se manifesta na exigência de que os agentes de tratamento internalizem padrões de conduta, desde o início do tratamento de dados pessoais.

No que se refere à sua dimensão repressiva, a *accountability* também apresenta relevância no plano *ex post*, como um referencial orientador para a atuação de magistrados e autoridades administrativas. Nesse sentido, serve de base para a apuração das responsabilidades decorrentes de condutas inadequadas no tratamento de dados, colabora tanto para a individualização dos sujeitos responsáveis quanto para a definição proporcional das sanções cabíveis, sendo considerada a gravidade da infração e o grau de conformidade prévio demonstrado pelo agente de tratamento (ROSENVALD; FALEIROS JÚNIOR *In* FRAZÃO; CUEVA, 2022).

Nessa toada, faz-se necessário frisar que para a melhor aplicabilidade da *accountability* a aplicação no tempo deve ocorrer de forma coalescente. Conforme ilustra Danielle Rached:

> Ocasionalmente, quando o detentor do poder antecipa as reações potenciais do prestador de contas e age de acordo com isso, a própria distinção pode em parte perder sua força. A distinção entre *ex ante* e *ex post*, portanto, captura uma ambivalência no fenômeno de "ser responsável": "*perceber-se responsável*" (e agir de acordo) e "*ser responsabilizado*" (e sofrer as consequências de seus atos anteriores) não são a mesma coisa. Ambas podem, de fato, coalescer em parte, ou mesmo na maior parte do tempo (...) (RACHED, 2016, p.331).[13]

[13] "Occasionally, when the power-holder anticipates the potential reactions of the account-holder and acts accordingly, the distinction itself may partially lose its grip. The distinction between *ex ante* and *ex post*, thus, captures an ambivalence in the phenomenon of 'being accountable': to 'perceive yourself accountable' (and acting accordingly) and to 'be held accountable' (and suffering the consequences of your previous acts) are not the same thing. Both may indeed coalesce part of, or even most of the time" (RACHED, 2016, p. 331).

Tal entendimento justifica-se na medida em que, por exemplo, a aplicação da *accountability* apenas na perspectiva *ex post,* possa ser infrutífera ou não útil, faz-se necessária a atuação preventiva também, nesse sentido entendem Collen Scott (2000), Thiago Sombra (2019) e Bruno Bioni (2022), conforme abaixo:

> À luz dessa análise, a distinção às vezes feita entre *accountability* e controle — sendo o controle entendido como um envolvimento *ex ante* em uma decisão, enquanto a *accountability* é restrita à supervisão *ex post* — não é particularmente útil. Essa distinção, frequentemente encontrada em relatos do direito público, parece negligenciar a observação de que está implícito, na capacidade de exigir prestação de contas, algum elemento da capacidade de controle. Parece melhor enxergar controle e *accountability* como conceitos interligados, operando em um contínuo. Se fôssemos redesenhar essa distinção, poderia ser em termos de que o controle gerencial se refere ao direito de envolvimento *ex ante* na tomada de decisões, enquanto o controle baseado na *accountability* se refere à supervisão *ex post* (SCOTT, 2008, *apud* BIONI, 2022, p. 229).

> Como em geral a atuação das autoridades de proteção de dados é mais focada num papel "*ex post*" em vez de "*ex ante*", *a accountability* pode ser um meio de também propiciar uma atuação prévia e educativa voltada à preservação da privacidade (SOMBRA, 2019, p. 192).

> A sua função é dar voz aos indivíduos afetados pelo tratamento de dados, bem como a entidades representativas dos seus direitos. Sua inclusão nos circuitos decisórios é o principal gargalo para se prevenir danos e violações à proteção de seus dados (regulação *ex ante*). Somente se este fórum for, de fato, constituído é que os agentes de tratamento de dados devem ser considerados *accountable* e, com isso, beneficiarem-se, eventualmente, de sanções mais brandas no caso de comportamentos ilícitos (regulação *ex post*) (BIONI, 2022, p. 230).

.

Portanto, constata-se que a dicotomia entre as abordagens *ex ante* e *ex post* não deve ser compreendida de excludente no campo da proteção de dados, especialmente quanto à concretização do princípio da *accountability*. Ao contrário, conforme demonstrado, a efetividade desse princípio repousa justamente em uma articulação dinâmica entre ambas as perpectivas. A atuação preventiva (*ex ante*), por meio da incorporação de padrões de governança, boas práticas e participação dos titulares no processo decisório, contribui para mitigar riscos e estruturar um ambiente de conformidade contínua. Já a atuação repressiva (*ex post*), por sua vez, complementa esse modelo ao assegurar mecanismos de responsabilização, que reforça a credibilidade do sistema regulatório e serve de incentivo à conformidade.

A convergência dessas dimensões, conforme apontado por Rached (2016), Scott (2000), Sombra (2019) e Bioni (2022), permite que a *accountability* opere como um instrumento regulatório mais completo e responsivo, que transcende a simples punição de condutas inadequadas e avança no sentido de promover uma cultura institucional de responsabilidade proativa.

3.3 Aplicabilidade da *accountability* no contexto da "metarregulação"

A emergência de novos arranjos regulatórios, especialmente diante da complexificação das relações sociais e da velocidade das inovações tecnológicas, impôs alterações modelos tradicionais de regulação estatal. Nesse cenário, de forma distinta da autorregulação em que é confiado que o agente de tratamento terá capacidade plena para uma autocontenção de sua atividade (BIONI, 2022, p. 85), a metarregulação parte do pressuposto que o "mandato regulatório é colaborativo e não privativo" (BIONI, 2022, p.86).

Isto é, apesar do entendimento de que o agente de tratamento executa uma atividade que precisa ser regulada, o processo de governança não cabe de forma exclusiva a ele. Bruno Bioni (2022), acerca da temática da metarregulação aponta que:

> (...) os objetivos desse processo são fruto de deliberação exógena e, por conseguinte, mais porosa. Nesse sentido, decompondo a palavra metarregulação, as metas são estabelecidas pela lei e/ou por agentes externos e, por outro lado, há discricionariedade por quem, desempenha a atividade regulada, em definir os meios para atingi-las, que, por fim, ainda que com algum tipo de supervisão. (BIONI, 2022, p. 86).

Depreende-se que a metarregulação pode ser compreendida como uma forma intermediária entre a autorregulação e os tradicionais modelos de comando e controle, na medida em que há compartilhamento de responsabilidades entre os próprios regulados e agentes externos no processo de governança.

No que concerne a aplicabilidade da *accountability,* diante da realidade das leis de proteção de dados que tem como característica uma "moldura normativa mais indireta" (BLACK, *apud* BIONI, 2022, p. 86), a *accountability* surge como um conceito orientativo das condutas dos agentes de tratamento e da ANPD, enquanto figura de regulação.

Assim, é preciso ter em vista que a ANPD, enquanto agente regulador pode ser capturável. Ou seja, caso a ANPD passe a atuar de forma parcial, sobressaindo os interesses de algum particular, é dito que houve a captura do agente regulador. O interesse, pode ocorrer devido a influências políticas, econômicas, empresariais, dentre outras, com o objetivo de beneficiamento pessoal. A Teoria da Captura, teoria que versa sobre o assunto, "pressupõe que a ação do regulador tende a defender os interesses de determinado grupo, ou seja, a sua ação é capturada pela indústria regulada" (Bernstein, 1955 apud Barbosa, 2017, p.19).

Nesta toada, segundo Claudia Quelle (2018):

> (...) “mudança de paradigma” ao colocar mais responsabilidade nos controladores corporativos, afastando-se do controle do titular dos dados [...]. Mas é pertinente perguntar: é a [...] evidência de uma ideologia liberal, de mercado livre ou de legislaturas fracas sofrendo com a captura regulatória? (QUELLE, 2018 apud BIONI, 2022, p. 95).

Diante dessa realidade, a *accountability* deve ser operacionalizada como uma forma de “vacina para a patologia da metarregulação” (BIONI, 2022, p. 96). Para além, uma “espécie de contrapeso para que tal discricionariedade não transmude em arbitrariedade e não se desvie dos objetivos programados” (BIONI, 2022, p. 96).

Conclui-se que, para a efetividade da aplicação da *accountability,* não basta que esta seja concebida como um princípio estático, a ser invocado de forma meramente retórica ou circunstancial. É imprescindível que seja colocada em movimento, como um verdadeiro mecanismo dinâmico de prestação de contas, capaz de produzir consequências concretas (BIONI, 2022, p. 97). Nesse sentido, a *accountability* deve desembocar em processos decisórios informados e transparentes. Trata-se, assim, de uma prática orientada não apenas à resposta formal, mas à responsabilização substantiva, como parte de um ciclo virtuoso de governança e de cultura organizacional. Conforme a expressão delimitada por Bruno Bioni, a *accountability* deve ser um “termo mecanismo e não apenas uma virtude” (BIONI, 2022, p. 98).

4 A PRIVACIDADE E SUA REDEFINIÇÃO PARA A AUTODETERMINAÇÃO INFORMATIVA

Esta seção se dedica à análise da redefinição do direito à privacidade no contexto da Sociedade da Informação, com o objetivo de demonstrar como esse direito, diante das transformações tecnológicas e informacionais, passou a ser compreendido sob a lógica da autodeterminação informativa. Para tanto, inicialmente, vale apresentar o advento da Sociedade da Informação e os seus impactos. Em seguida, explora-se a concepção de privacidade proposta por Stefano Rodotà, referencial teórico deste trabalho, com destaque à sua vinculação com a noção de controle individual sobre os próprios dados pessoais e os paradoxos que emergem dessa reconfiguração. Por fim, a ideia de codeliberação informativa é introduzida como uma ampliação ao alcance da autodeterminação.

4.1 O Advento da Sociedade da Informação

É preciso considerar a sociedade passa por diferentes formas e fases de organização ao longo do tempo. Em especial, pode-se considerar três momentos bem definidos. Em primeiro lugar, a sociedade agrícola, marcada pela revolução agrícola, em que houve a inserção do homem no sistema produtivo, marcada pelo aumento quantitativo da mão de obra e dos recursos naturais (em particular a terra) no processo produtivo (SIQUEIRA JR., 2019, p. 266-267). Em seguida, a sociedade industrial, marcada pela revolução industrial, na qual a principal fonte e produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e circulação (SIQUEIRA JR., 2019, p. 267-268). Por fim, em seu atual estágio, a sociedade informacional.

A Sociedade Informacional, surge especificamente no último quartil do século XX, marcada uma intensa transformação da sociedade, denominada como revolução tecnológica (SIQUEIRA JR., 2019, p. 265). Nas palavras de Manuel Castells: “Uma revolução tecnológica concentrada nas tecnologias da informação começou a remodelar a base material da sociedade em ritmo acelerado” (CASTELLS, 2002, p. 39).

Segundo Paulo Hamilton Siqueira Jr. (2019):

> A sociedade da informação é constituída em tecnologias de informação e comunicação que envolve a aquisição, o armazenamento, o processamento e a distribuição da informação por meios eletrônicos, como rádio, televisão, telefone e computadores, entre outros. Essas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, econômicos e políticos,

> criando uma nova estrutura social, que tem reflexos na sociedade local e global, surgindo assim a sociedade da informação. (SIQUEIRA JR., 2019, p. 264).

Desta feita, a Sociedade da Informação, ao se estabelecer como resultado direto do avanço das tecnologias de informação e comunicação, não apenas redefine os meios de produção e circulação de conhecimento, como também altera as relações sociais e econômicas. Nesse contexto, a informação torna-se um recurso estratégico, comparável em relevância aos recursos naturais na sociedade agrícola ou à energia na sociedade industrial, passa a desempenhar papel central no desenvolvimento e na competitividade entre indivíduos, organizações e nações.

Além disso, a conectividade global e a instantaneidade no acesso às informações transformaram profundamente a dinâmica social. Assim, a Sociedade da Informação não pode ser compreendida apenas sob o viés tecnológico, mas também a partir das mudanças culturais, políticas e econômicas que ela desencadeia, estabelece novos paradigmas de interação e produção de conhecimento. Conforme ilustra Rodrigo da Cunha Lima Freire (2006):

> Nas últimas décadas o mundo vem experimentando notáveis transformações em função da aceleração dos mecanismos de difusão das informações, proporcionada, especialmente, pelo desenvolvimento tecnológico das telecomunicações e da microeletrônica. A facilitação do acesso à informação pelos diversos meios de comunicação, como o rádio, a televisão, os telefones e os computadores – especialmente com o advento de novas tecnologias como a internet, o satélite, a telefonia celular e a rede de fibra óptica mundial – modificou – e vem modificando – substancialmente as relações sociais, econômicas e jurídicas, razão pela qual se pode dizer que a sociedade contemporânea é da informação (FREIRE, 2006, p. 247).

Nesse sentido, evidencia-se que a principal força motriz da sociedade contemporânea é a informação, que assume o papel de elemento estruturante da organização social, assim como a terra, as máquinas a vapor e a eletricidade desempenharam essa função em períodos anteriores (BIONI, 2020, p.5). Ainda que o protagonismo da informação como fator gerador de riqueza tenha se consolidado na atualidade, sua relevância já se esboçava desde a sociedade industrial, especialmente com o advento do Taylorismo[14], que surge no contexto do próprio processo de

[14] "Frederick Taylor (1856-1915) foi um engenheiro mecânico norte-americano que escreveu os princípios da Administração Científica, nos quais defendeu uma abordagem metódica e mais racional aos desafios administrativos para alcançar a produtividade. Taylor é considerado um dos responsáveis pelo desenvolvimento da Teoria Geral da Administração. Os conceitos desenvolvidos por Taylor preconizam a racionalização do trabalho, mas, para chegar até aí, vários itens do ambiente laboral foram pesquisados academicamente, sendo que, anteriormente, as estratégias de trabalho eram realizadas de forma empírica. Porém, tais formulações acadêmicas tinham o mesmo objetivo de aumento da produtividade ao menor custo, tanto que Taylor criou várias metodologias que repercutem no ambiente organizacional até hoje, como a adoção do controle de tempo nas atividades do trabalhador." (LACERDA, 2021, p.16)

produção passar a ser objeto de estudo para o aumento da produtividade com menores custos (BIONI, 2020, p. 9).

Contudo, como pontua Bioni (2020), não se trata apenas de uma economia da informação, mas, necessariamente, uma economia do conhecimento. Isto é, a informação, por si só, não garante eficiência na atividade empresarial, e sim o seu processamento, organização e transformação em conhecimento aplicável que gera vantagem competitiva (BIONI, 2020, p.10). Um exemplo paradigmático é o da Zara, que reprojeta seus produtos de acordo com a resposta do mercado consumidor, que transforma os dados extraídos das vendas em um conhecimento estratégico que orienta sua produção e inovação (BIONI, 2020, p. 11).

Sob essa perspectiva, João Ferreira do Amaral reforça a mesma linha de pensamento ao afirmar que:

> O que faz a empresa ganhar dinheiro não é receber a informação em si própria. É transformar essa informação em conhecimento que depois é aplicado. Falta-nos por isso introduzir a questão da transformação da informação em conhecimento (AMARAL, *apud* BIONI, 2020, p. 11).

Dessa forma, as informações como a resposta do consumidor, bem como outros dados pessoais relacionados, tornam-se ativos fundamentais para empreender com maior eficácia (BOULDING, 1971, p.24). Tais informações geram vantagens desde o aprimoramento na concepção e segmentação de produtos e serviços até uma abordagem publicitária mais direcionada.

Por isso, a matéria-prima de uma economia redimensionada pelos avanços das tecnologias da informação e comunicação, com foco nos dados pessoais dos cidadãos que passaram a ditar na sociedade da informação, uma lógica de acumulação de capital para a geração de riquezas (BIONI, 2020, p. 11).

Nesse cenário, a mineração de dados surge como uma das principais ferramentas na transformação de informação em conhecimento, uma vez que consiste em um conjunto de técnicas e processos voltados à identificação de padrões, correlações e tendências a partir de grandes volumes de dados, a chamada Big Data. Mais do que simplesmente coletar dados, a mineração atua na etapa de interpretação, extrai-se valor do que, à primeira vista, são apenas registros dispersos e desestruturados.

Segundo Jonas Lerman (2013), advogado consultor do gabinete jurídico do departamento de Estado dos EUA:

> A Big data, apesar de toda a sua complexidade técnica, surge de uma ideia simples: reunir detalhes suficientes sobre o passado, aplicar as ferramentas analíticas corretas

> e, assim, encontrar conexões e correlações inesperadas que podem ajudar a fazer previsões incomumente precisas sobre o futuro — como os consumidores escolhem entre produtos, como terroristas operam, como as doenças se espalham. As previsões baseadas em big data já orientam decisões dos setores público e privado diariamente em todo o mundo (LERMAN, 2012, p. 57, tradução nossa).[15]

Portanto, a *Big Data* "não se preocupa com a causalidade de um evento, mas, tão somente, com a probabilidade de sua ocorrência" (BIONI, 2020, p. 36). Devido à sua aptidão para fornecer previsões por meio de probabilidades, tais recursos têm o poder de gerar benefícios significativos à sociedade. Por exemplo, existe a ferramenta *Google Flu Trends* que se baseia em dados sobre a quantidade de buscas de determinadas palavras-chave no *Google*. Utilizadas essas informações, é possível prever precisamente a quantidade de pessoas com gripe em diferentes regiões do mundo (CRUZ, IZBICKI, 2017, p. 513).

O desafio contemporâneo está baseado exatamente no limiar do o uso indiscriminado dessas informações. De forma a relacionar com o capítulo do presente trabalho que versa sobre a *accountability*, é nesse contexto que urge a importância dos os agentes adotarem práticas mais *accountable*.

O tratamento massivo de dados, aliado a técnicas de mineração e análise preditiva, pode colocar em risco a privacidade individual dos titulares de dados. A possibilidade de traçar perfis comportamentais, prever preferências e influenciar escolhas transforma os dados em instrumentos de poder e controle, pode levar a situações de discriminação algorítmica. Como explica Bioni:

> Ainda que, assim como um dado anônimo pode se tornar um dado pessoal, um dado "trivial" pode também se transmudar em um dado sensível; particularmente, quando se têm disponíveis tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos (BIONI, 2020, p. 84).

Somado a isso, vale destacar que a discriminação algorítmica tem raízes históricas que remontam desde a Alemanha da década de 1930. Naquela época, trabalhadores do censo coletavam informações como nacionalidade, língua materna, religião e profissão dos moradores. Esses dados eram processados por máquinas que foram utilizadas não apenas para identificar indivíduos judeus, mas também para auxiliar na logística de transporte para os campos de concentração (WAXMAN, 2018).

---

[15] "Big data, for all its technical complexity, springs from a simple idea: gather enough details about the past, apply the right analytical tools, and you can find unexpected connections and correlations, which can help you make unusually accurate predictions about the future—how shoppers decide between products,how terrorists operate, how diseases spread. Predictions based on big data already inform public- and private-sector decisions every day around the globe" (LERMAN, 2012, p. 57)

Assim, o advento da Sociedade da Informação não apenas consolidou a informação como principal ativo estratégico da economia contemporânea, mas também inaugurou um cenário em que com o emprego da *Big Data*, torna-se necessária a aplicabilidade de mecanismos efetivos para a salvaguarda dos direitos fundamentais, garante que o progresso tecnológico não se converta em instrumento de discriminação ou exclusão.

Danilo Doneda problematiza essa relação, afirma que:

> "o verdadeiro problema não é saber sobre o que o direito deve atuar, mas sim de como interpretar a tecnologia e suas possibilidades em relação aos valores no ordenamento jurídico, mesmo que isso signifique uma mudança nos paradigmas do instrumental jurídico utilizado, mesmo que isso signifique uma mudança nos paradigmas do instrumental jurídico utilizado" (DONEDA, 2020, p. 54).

Além disso, é relevante observar que a Sociedade da Informação redefine as relações de poder, uma vez que aqueles que detêm grandes volumes de dados e capacidade analítica, como *big techs*, passam a exercer uma influência significativa sobre os fluxos econômicos, políticos e sociais. A utilização de dados em larga escala requer em certa medida uma atuação regulatória eficaz, que busque equilibrar o desenvolvimento tecnológico com a proteção dos direitos dos titulares. Conforme descreve Bruno Bioni (2020):

> Qualquer perspectiva regulatória para a proteção dos dados pessoais deve levar em consideração o quadro acima descrito, a existência de uma economia de vigilância. Tal diagnóstico deságua em estratégias regulatórias complementares que são, por um lado, o empoderamento do indivíduo para exercer um controle significativo sobre seus dados pessoais, e, por outro lado, a consideração de que o próprio fluxo das informações pessoais não se deve submeter, tão somente, à lógica desses interesses econômicos em jogo (BIONI, 2020, p. 43).

Afinal, a emergência das leis de proteção de dados decorreu do receio de que o Estado, na qualidade de fiduciário de uma vasta quantidade de informações pessoais destinadas à execução de políticas de bem-estar social, pudesse utilizar os dados pessoais dos cidadãos de forma contrária aos interesses e direitos do cidadão (BIONI, 2022, p. 83)

4.2 A Privacidade como Autodeterminação Informativa segundo Stefano Rodotà

Após a breve digressão acerca da Sociedade da Informação, faz-se importante destacar no contexto destacado, os estudos do professor e jurista italiano Stefano Rodotà (2008), referencial teórico do presente trabalho.

Diante da realidade do compartilhamento massivo de dados pessoais na sociedade da informação, Rodotà analisa que:

> A sociedade da informação se especifica, portanto, como "sociedade dos serviços", com elevada padronização e crescentes vínculos internacionais. Disso decorrem duas consequências: quanto mais os serviços são tecnologicamente sofisticados, mais o indivíduo deixa nas mãos do fornecedor do serviço uma cota relevante de informações pessoais; quanto mais a rede de serviços se alarga, mais crescem as possibilidades de interconexões entre bancos de dados e de disseminação internacional das informações coletadas (RODOTÀ, 2008, p. 100).

Nesse cenário, diante do fornecimento de "uma cota relevante de informações pessoais", conforme descrito por Rodotà, torna-se preciso analisar a privacidade. Com o seu nascimento, associado à desagregação da sociedade feudal (RODOTÀ, 2008, p. 26), a Privacidade analisada, muito mais do que um direito previsto constitucionalmente[16], ela deve ser compreendida como um direito fundamental ativo, que confere ao indivíduo a capacidade de controlar suas próprias informações, conforme será exposto. Para Rodotà (2008), diante da influência da tecnologia dos computadores, a privacidade muito mais do que a definição tradicional como "direito a ser deixado só", conforme Louis Brandeis e Samuel Warren (1890) defendiam, passa-se ao "direito a controlar o uso que os outros façam das informações que me digam respeito" (RODOTÀ, 2008, p. 75)

Para mais, diante do posicionamento tradicional de privacidade, Rodotà também entende que:

> Uma definição de privacidade como "direito de ser deixado só" perdeu há muito tempo seu valor genérico, ainda que continue a abranger um aspecto essencial do problema e possa (deva) ser aplicada a situações específicas. Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. Assim, a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações. (RODOTÀ, 2008, p. 92).

Por decorrência da nova definição de privacidade, como um direito de manter o controle sobre as próprias informações, o privado também se ressignifica para Rodotá. Agora, o "privado passa a significar pessoal, e não necessariamente secreto"(RODOTÀ, 2008, p. 93).

Em outras palavras, a privacidade torna-se a sequência "pessoa-informação-circulação-controle" – supera-se assim a definição tradicional que restringia em "pessoa-informação-sigilo" – em que "o titular do direito à privacidade pode exigir formas de "circulação

[16] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:(...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;" (BRASIL, 1988)

controlada", e não somente interromper o fluxo das informações que lhe digam respeito" (RODOTÀ, 2008, p.93)

Diante da tutela do direito à privacidade de um modo dinâmico e plural, Rodotà (2008) apresenta três paradoxos oriundos da ampliação do direito à privacidade, usados "para indicar uma situação na qual a tensão relativa à privacidade entra (aparentemente) em contradição consigo mesma ou produz consequências (aparentemente) inesperadas" (RODOTÀ, 2008, p.95).

O primeiro paradoxo para Rodotà (2008), fundamenta-se a partir da premissa de que apesar do "Núcleo Duro" da privacidade ser fundamentado em uma necessidade de sigilo (como informações relacionadas à saúde ou hábitos sexuais), cada vez mais surgiram outras categorias de informações, protegidas sobretudo para evitar que pela sua circulação possam nascer situações de discriminação (RODOTÀ, 2008, p.95).[17]

Em seguida, o segundo paradoxo decorre do tratamento conferido a determinados dados sensíveis, como opiniões políticas, convicções religiosas, filiação sindical ou questões raciais. Tais informações, por um lado, são fundamentais para a construção da identidade "pública" do indivíduo em sociedades democráticas, já que permitem a livre manifestação de convicções e posicionamentos no espaço social. Por outro lado, esses mesmos dados são extremamente vulneráveis a usos discriminatórios, motivo pelo qual recebem proteção reforçada, com restrições à sua coleta e circulação, sobretudo realizadas por sujeitos como empregadores ou instituições privadas. Assim, estabelece-se uma tensão: para que a vida democrática seja plena, esses dados devem poder circular, mas, para proteger o indivíduo contra discriminações, eles devem ser cercados de limitações, caracteriza, assim, o segundo paradoxo da privacidade (RODOTÀ, 2008, p. 96).

Por fim, o terceiro paradoxo, é fundamentado na privacidade como um direito fundamental, sobretudo à luz da necessidade de o titular acompanhar suas informações pessoais, mesmo que já se encontrem sob controle de terceiros. Segundo o autor, esse reconhecimento acentua o papel do direito de acesso, que passa a ser a regra básica para disciplinar as relações entre sujeitos potencialmente em conflito informacional, substitui-se o critério formal da posse pela prevalência do direito da pessoa à qual os dados se referem. Esse deslocamento confere nova feição à privacidade, que deixa de ser um simples direito ao sigilo e assume função ativa: garantir a transparência e o controle das esferas informacionais alheias. É nesse sentido que

[17] "Do exame de textos relevantes nessa matéria, percebe-se claramente que o "núcleo duro" da privacidade é ainda hoje constituído por informações que refletem tradicional necessidade de sigilo (por exemplo, aquelas relacionadas saúde ou aos hábitos sexuais): internamente, porém, assumiram cada vez maior relevância outras categorias de informações, protegidas sobretudo para evitar que pela sua circulação possam nascer" (RODOTÀ, 2008, p.95)

Rodotà (2008) afirma que o fortalecimento da privacidade individual se converte em instrumento para tornar mais transparentes e controláveis os outros sujeitos. Assim, o "terceiro paradoxo da privacidade" reside justamente no fato de que, para garantir sua proteção, a privacidade deve se abrir à circulação, não no sentido de exposição irrestrita, mas por meio do direito de acesso e da visibilidade controlada, inclusive sobre informações normalmente públicas, mas que podem conter dados privados (RODOTÀ, 2008, p.97).[18]

Diante dos paradoxos trazidos por Rodotà, é mister salientar que em um ambiente em que os dados circulam em larga escala e de forma opaca, mesmo "as coletâneas de dados anônimos podem ser manipuladas de forma gravemente lesiva aos direitos dos indivíduos" (RODOTÀ, 2008, p. 32), demonstra que a mera desidentificação não é suficiente para afastar os riscos à dignidade e à liberdade pessoal.

Nesta toada, Rodotà (2008) alerta que "quanto mais os serviços são tecnologicamente sofisticados, mais o indivíduo entrega ao fornecedor uma parcela significativa de suas informações pessoais" (RODOTÀ, 2008, p. 100); e quanto mais se amplia a rede de serviços digitais, "maiores são as possibilidades de interconexão entre bancos de dados e de disseminação internacional das informações coletadas" (RODOTÀ, 2008, p. 100).

Esse cenário expõe o sujeito a uma vigilância constante, centrada não apenas na proteção passiva, mas na "efetiva capacidade do titular de acompanhar, controlar e limitar o uso de seus dados" (RODOTÀ, 2008, p. 100), em cada etapa do tratamento. A autodeterminação informativa, assim, surge como reação normativa à complexidade dos fluxos informacionais modernos, reafirma o protagonismo do indivíduo em face dos sistemas automatizados e das arquiteturas digitais de poder.

A autodeterminação informativa constitui uma garantia fundamental própria, emergente das transformações na concepção contemporânea de privacidade. Em vez de ser compreendida apenas como proteção contra interferências indevidas, a privacidade, sob a ótica de Stefano Rodotà, adquire uma dimensão ativa e relacional, que abrange a faculdade de o indivíduo

[18] "O reconhecimento da condição de direito fundamental à privacidade, do ponto de vista de poder "acompanhar" as informações pessoais mesmo quando se tornaram objeto da disponibilidade de um outro sujeito, deu relevo especial ao direito de acesso, que se tornou a regra básica para regular as relações entre sujeitos potencialmente em conflito, superando o critério formal da posse das informações. Acima, o critério proprietário, fundado na legitimidade da coleta e do tratamento de informações relativas a outras pessoas, prevalece o direito, fundamental da pessoa à qual se referem as informações. O fortalecimento do direito individual à privacidade converte-se assim em instrumento para tornar mais transparentes e controláveis as esferas de outros sujeitos. Não por acaso, o desenvolvimento da legislação sobre a tutela dos dados pessoais foi acompanhado pela difusão de leis sobre o acesso às informações (normalmente públicas, mas em certos casos também privadas). Chamo esse de "o terceiro paradoxo da privacidade" (mesmo se histórica e conceitualmente, pela forma como veio gradativamente se transformando o direito de acesso (...)" (RODOTÁ, 2008, p. 97).

exercer poder efetivo sobre os dados que o representam no ambiente social e digital. Para o jurista italiano:

> A presença de riscos conexos ao uso das informações coletadas, e não uma natural vocação ao sigilo de certos dados pessoais, foi o que levou ao reconhecimento de um "direito à autodeterminação informativa" como direito fundamental do cidadão. Este reconhecimento enquadra-se na tendência de atribuir a condição de direitos fundamentais a uma série de posições individuais e coletivas relevantes no âmbito da informação (RODOTÀ, 2008, p. 96).

Nesse panorama, extrai-se que o direito à autodeterminação informativa se revela como um mecanismo jurídico específico de controle sobre o fluxo de informações pessoais, centrado na figura do titular como agente ativo. Diferentemente da concepção tradicional de privacidade, que abarca valores mais amplos ligados à construção da intimidade e da subjetividade, a autodeterminação informativa constitui uma ferramenta central de defesa do sujeito frente aos riscos da sociedade informacional.

Desse modo, conforme exposto anteriormente, é preciso que seja adotado um meio dinâmico para a proteção da privacidade, uma vez que “os dados pessoais são o petróleo, insumo ou uma commodity, estando para a economia da informação como a destruição do meio ambiente estava para a economia industrial” (BIONI, 2020, p.102). Ao passo que as informações passaram a se tornar um ativo, a cessão de dados passa a ser muito mais do que uma troca, criam uma espécie de posse permanente do titular de dados. Conforme disserta Rodotà:

> Tudo isso é apresentado como um preço compulsório para fruir das crescentes oportunidades oferecidas pela sociedade da informação. Concretamente, isso significa que a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações. Nessa troca, então, não é mais somente o patrimônio de uma pessoa que está envolvido. A pessoa é obrigada a expor seu próprio eu, sua própria persona, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito (RODOTÀ, 2008, p.113).

Portanto, o direito à autodeterminação informativa, entendido como a prerrogativa de o indivíduo manter o controle efetivo sobre seus próprios dados, deve ser efetivado por meio de mecanismos concretos, capazes de garantir sua operacionalização no ambiente informacional contemporâneo. Mais do que isso, “é assegurar que o fluxo informacional atenda às suas legítimas expectativas, e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade” (BIONI, 2020, p. 105).

4.3 Codeliberação informativa: uma nova definição para as decisões compartilhadas sobre dados pessoais

Toma-se por base a construção conceitual de Rodotà (2008) acerca da privacidade como expressão da autodeterminação informativa, é possível avançar para uma compreensão mais contemporânea e relacional desse direito, especialmente à luz das contribuições de Bruno Bioni (2022). Nesse sentido, o autor propõe o conceito de codeliberação informativa, por meio do qual se busca redefinir a dinâmica entre titular e agente de tratamento, promove-se uma corresponsabilidade na tomada de decisões que envolvem dados pessoais. Trata-se de um aprofundamento da ideia de autodeterminação, agora concebida não apenas como manifestação individual de vontade, mas como um processo dialógico e colaborativo, no qual a prestação de contas (*accountability*) e a transparência são pilares essenciais para o exercício efetivo da liberdade informacional.

Em especial uma vez que seja versado um dever de proteção que independe da concordância e da manifestação do titular, haveria de fato um interesse público. Portanto, os agentes de tratamento devem ser parte principal para um sistema de freio e contrapesos (BIONI, 2022, p. 234).

Conforme indicado no capítulo destinado ao princípio da *accountability e* à luz de Bioni (2022), a prestação de contas deve ser enxergada como um mecanismo operacionalizado por diferentes agentes, em outras palavras, é “um processo que reúne múltiplos atores que se alternam no polo ativo e passivo” (BIONI, 2022, p. 240).

Portanto, para a ressignificação do direito à proteção de dados, como um direito que não seja simplório, deve-se levar em conta a codeliberação informacional junto com a autodeterminação informação, como objetivo de “experimentar um processo de codeliberação e não de dominação informacional” (BIONI, 2022, p. 245).

5 A ANPD E OS AGENTES DE TRATAMENTO DE MENOR PORTE

Esta seção tem por objetivo analisar a natureza jurídica da Autoridade Nacional de Proteção de Dados (ANPD), sua origem normativa e a legalidade dos atos infralegais por ela editados. Em seguida, será explorada a Resolução CD/ANPD nº 02/2022, que instauram um regime regulatório diferenciado para agentes de tratamento de pequeno porte.

5.1 Legalidade dos atos normativos infralegais da ANPD

Inicialmente, é necessário examinar a natureza jurídica, a origem e os fundamentos legais da Autoridade Nacional de Proteção de Dados (ANPD). A instituição da ANPD ocorreu por meio da Medida Provisória nº 869, de 27 de dezembro de 2018, posteriormente convertida na Lei nº 13.853, de 14 de agosto de 2019.

Contudo, o percurso para sua criação não foi linear. Ainda durante o processo legislativo da Lei Geral de Proteção de Dados, o então presidente da República, Michel Temer, vetou a criação da ANPD sob a justificativa de que a criação da ANPD implicaria em uma inconstitucionalidade do processo legislativo por trazer um vício de iniciativa, uma vez que a ao seu ver, a criação deveria ter partido pelo Executivo Federal (SENADO FEDERAL, 2018).

Tal alegação à época gerou uma controvérsia, na época foi afirmado que:

> Ainda, como bem se sabe, eventual veto à criação da ANPD pode pautar-se por motivos outros que não a sua (falta de) base constitucional. A grave crise financeiro-orçamentária pode derrubar a medida. O debate político sobre a alocação das competências recém-aprovadas, desejada por diferentes órgãos no governo, também (...) Quanto ao lastro jurídico, tem-se uma autoridade desenhada, ao fim e ao cabo, por projeto de lei de iniciativa parlamentar. Ainda, como bem se sabe, eventual veto à criação da ANPD pode pautar-se por motivos outros que não a sua (falta de) base constitucional. (DE PAULA & NAEFELE, 2018).

Apesar da controvérsia, forma, o próprio poder executivo apresentou a Medida Provisória n. 869, de 27 de dezembro de 2018, que incluiu a ANPD na estrutura da Presidência da República, com a ressalva do caráter transitório de sua natureza jurídica. Portanto, a referida autoridade passou a integrar a Administração Direta, "que é um modelo mais fraco em termos de autonomia funcional e financeira" (BIONI, 2022, p. 62).

Segundo Marçal Justen Filho, a administração direta "consiste no ente político que, por determinação constitucional, é o titular da função administrativa. A Administração direta compreende a União, os Estados, o Distrito Federal e os Municípios" (JUSTEN FILHO, 2025, p. 115).

Nos ditames expressos na redação da Medida Provisória, foi assegurada a autonomia técnica à ANPD, além de ter-lhe sido atribuída a competência para fiscalizar, editar normas e aplicar sanções, reserva-se, contudo, todo o poder decisório à Presidência da República. Em função dessa estruturação, surgiu a preocupação relativa à falta de autonomia técnica que, afinal, por estar subordinada ao poder executivo, poderia sofrer pressões e interferências políticas, principalmente em uma fiscalização do poder público. Nesse sentido, o Deputado Orlando Silva explanou:

> Para finalizar neste tópico da estrutura da ANPD, após ouvir posicionamentos públicos de representantes do governo nesta comissão, e posicionamento dos colegas integrantes deste colegiado, assim como o setor produtivo e o terceiro setor, resta aqui a nossa declaração de que um órgão da administração indireta terá que ser prontamente criado pelo Poder Executivo como única forma para o exercício pleno dos princípios, direitos, garantias e deveres previstos na LGPD. Nesse sentido, incluímos novos parágrafos ao art. 55-K indicando expressamente que a natureza jurídica da ANPD terá que ser transformada em autarquia no prazo de dois anos da aprovação de sua estrutura regimental, bem como a tempo de ser incluída nas Leis Orçamentárias. (SENADO FEDERAL *apud* BIONI, 2022, p. 63).

Em 13 de junho de 2022, com a edição da Medida Provisória nº 1.124, que, posteriormente, foi convertida na Lei 14.460/22, foi promovida uma alteração substancial na natureza jurídica da ANPD, que passa a ser formalmente instituída como autarquia de natureza especial. Essa mudança eliminou o caráter transitório anteriormente conferido à entidade, atribuindo-lhe personalidade jurídica própria, autonomia técnica e decisória, bem como patrimônio próprio. A ANPD, desde então, passa a integrar a Administração Pública Indireta, vinculada ao Ministério da Justiça e Segurança Pública, sendo incumbida das funções de zelar pela proteção de dados pessoais, editar regulamentos e fiscalizar o cumprimento da legislação aplicável à matéria.

Sob a ótica do Direito Administrativo, a qualificação como autarquia de natureza especial implica a submissão da entidade a um regime jurídico diferenciado em relação às autarquias comuns. Conforme destaca Justen Filho (2025, p. 121), tais entidades gozam de "graus mais intensos de autonomia", o que se traduz em menor interferência política sobre suas atividades institucionais. Com isso, busca-se assegurar maior tecnicidade, agilidade e imparcialidade na atuação regulatória. Nesse sentido, Maria Sylvia Zanella Di Pietro (2025) esclarece que:

> […] o regime especial vem definido nas respectivas leis instituidoras, dizendo respeito, em regra, (a) à maior autonomia em relação à Administração Direta, (b) à estabilidade de seus dirigentes (...) e ao caráter final de suas decisões, que não são

> passíveis de apreciação por outros órgãos ou entidades da Administração Pública (DI PIETRO, *apud* JUSTEN FILHO, 2025, pág.121).

Em virtude da autonomia técnica conferida à ANPD pela alteração legislativa, é possível indicar que ela passa a exercer diferentes poderes, especialmente organizados como poder normativo-fiscalizatório. Bruno Bioni (2022), relaciona diferentes eixos que foram acrescidos na lei, conforme se verifica:

> **c.2.1) auditoria:** o poder de auditoria é eliminado no processo de sanção e veto do governo Temer – fase 5, vindo a retornar somente na fase 7 após um número bastante expressivo de emendas parlamentares (fase 6, art. 55-J, XVI);
> **c.2.2) relatório de impacto à proteção de dados pessoais:** o poder de regulamentação do instrumento de relatório de impacto à proteção de dados pessoais (previsto na fase 4) é arrancado no processo de veto e sanção do governo Temer – fase 5. Novamente, é recolocado durante a discussão da MP 869/2018 (fase 7, art. 55-J, XIII);
> **c.2.3) acordos administrativos:** somente na fase 7 é que se atribuiu o poder da ANPD de "celebrar compromissos" para "eliminar irregularidade, incerteza jurídica ou situação contenciosa" (fase 7, art. 55-J, XVII). É um salto que abre espaço para o órgão regulador compor com o regulado por meio de soluções que substituem sanções, o que vai à linha das recentes modificações da LINDB;
> **c.2.4) normas simplificadas para empresas nascentes de tecnologia de micro ou pequeno porte:** é, também, somente na fase 7, que se atribuiu o poder da ANPD de calibrar o peso da regulação de acordo com as particularidades e realidades de determinados atores regulados (fase 7, art. 55-J, XVIII). Parte-se do pressuposto que nem todos os agentes econômicos teriam a mesma capacidade para adotar e prestar contas acerca da eficácia de medidas para o cumprimento da lei (BIONI, 2022, p. 66-67, grifo do autor).

Portanto, é possível considerar diante da evolução e maturação do texto da LGPD para a criação e modificação da natureza da ANPD, que as delegações realizadas à ANPD buscam conferir-lhe um caráter institucional mais robusto e responsivo, amplia-se seus instrumentos normativos, fiscalizatórios e sancionatórios. A partir da chamada fase 7, segundo Bioni (2022), nota-se que não apenas foram restabelecidas prerrogativas eliminadas em fases anteriores, como também inaugura novas competências voltadas à governança regulatória (BIONI, 2022, p. 66-67).

Repisa-se, que apesar de possuir atributos e funções que são similares às de uma agência reguladora, não é possível o seu enquadramento à lei 13.848/19, que dispõe sobre gestão, a organização, o processo decisório e o controle social das agências reguladoras, bem como a lei 9.986/00. Entende nesse sentido Maria Sylvia Zanella Di Pietro:

> [...] para os fins da Lei nº 13.848/19 e da Lei nº 9.986, de 18-7-00 (que dispõe sobre a gestão de recursos humanos das agências reguladoras), somente são consideradas como tal as referidas no artigo 2º da Lei nº 13.848/19. (...) Assim sendo, embora outras entidades exerçam função reguladora semelhante à atribuída as agências reguladoras, as duas leis citadas somente se aplicam às entidades criadas com essa denominação (DI PIETRO, 2025, p. 521).

De toda sorte, diante das discussões acerca da natureza jurídica na seara do direito administrativo, é certo que, embora não esteja submetida ao regime da Lei n. 13.844/2019, a ANPD exerce atividade regulatória, nos termos do artigo 55-J da Lei Geral de Proteção de Dados Pessoais. Portanto, por competência a ANPD pode:

> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
> XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (BRASIL, 2018).

Dessa forma, evidencia-se que a ANPD possui legitimidade normativa para editar atos infralegais. Assim, a referida autarquia deve exercer tais competências nos limites da própria legislação da LGPD, uma vez que não se submete ao regime jurídico típico das autarquias sob da Lei n. 13.844/2019.

5.2 A Resolução CD/ANPD nº 02/2022

Diante da legitimidade da ANPD para editar normativas infralegais, adota-se, como enfoque do presente trabalho, o tratamento de dados realizado por agentes de tratamento de menor porte, especialmente em razão da competência da ANPD para "editar normas, orientações e procedimentos simplificados e diferenciados" (BRASIL, 2018), para as particularidades e realidades desses agentes, nos termos do art. 55-J, XVIII, da LGPD. Tais prerrogativas normativas encontram expressão concreta na Resolução CD/ANPD nº 02/2022.

As discussões acerca do texto da Resolução CD/ANPD nº 2, remontam desde fevereiro de 2021, na ocasião o diretor-presidente da ANPD enviou diferentes comunicações para mais de cinquenta pessoas, ocupantes de diferentes cargos na administração pública, com indicações de que foi iniciada a "Tomada de subsídios para regulamentação da aplicação da LGPD para microempresas de pequeno porte"[19]. O objetivo das comunicações, foi convidar os entes a contribuir no âmbito da tomada de subsídios. Dessa forma, todo o processo de elaboração da norma durou um pouco menos de um ano, com publicação definitiva em 27 de janeiro de 2022.

[19]O formulário de envio das contribuições para a tomada de subsídios deveria ser realizado no site: https://www.gov.br/anpd/pt-br/assuntos/noticias/ainda-na-semana-internacional-da-protecao-de-dados-anpd-inicia-tomada-de-subsidios-sobre-microempresa.

Em primeiro lugar, é preciso destacar que a aplicabilidade da referida resolução se restringe aos agentes de tratamento de pequeno porte. Conforme disposto no inciso I do artigo 2º da Resolução CD/ANPD nº 02/2022:

> Art. 2º Para efeitos deste regulamento são adotadas as seguintes definições: I - agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador; (BRASIL, 2022).

Depreende-se, portanto, que a expressão "pequeno porte", conferida a esses agentes, não se refere exclusivamente ao critério econômico, mas abarca uma variedade de organizações e pessoas físicas que, embora distintas em natureza jurídica e finalidade, compartilham limitações estruturais e operacionais. A definição é propositalmente abrangente, a fim de permitir uma adequação mais realista e inclusiva da LGPD, alinhada aos princípios da proporcionalidade e da razoabilidade. Nesse sentido, mesmo que na ótica de uma atividade empresarial quanto às empresas de pequeno porte, é preciso que seja compatibilizado "o volume de recursos movimentado por estes, isto é, não se pode exigir dos pequenos e médios empresários o mesmo que se exige de uma grande companhia." (TOMAZETTE, 2022, p. 677).

A partir desse entendimento, observa-se que a Resolução CD/ANPD nº 02/2022, é composta por quatorze artigos e estabelece critérios para aplicação das normas, hipóteses de flexibilização regulatória e medidas específicas de adaptação, compatibiliza-se os deveres legais à realidade concreta de agentes de menor porte. A norma permite, por exemplo, nos termos do art. 14, prazo diferenciado (em dobro) aos agentes de tratamento para atendimento de solicitações de titulares, na comunicação à ANPD e ao titular na ocorrência de incidente de segurança.

Bruno Bioni (2022) sintetiza, que:

> Por exemplo, à semelhança com o que está prescrito na GDPR, recentemente a ANPD editou Resolução CD 2, de 27 de janeiro de 2022 para agentes de pequeno porte em que há o relaxamento e, até mesmo, a dispensa de algumas obrigações como de: i) nomeação de encarregado; ii) registro das atividades de tratamento de dados; iii) mecanismos de segurança da informação; e iv) prazo para o atendimento à requisição dos titulares. No entanto, essas e outras obrigações legais dependem do cruzamento dos dois critérios acima mencionados e que são cumulativos – porte econômico do agente e risco da atividade de tratamento de dados – para se procedimentalizar – pesos distintos do plexo obrigacional das leis de proteção de dados. (BIONI, 2022, p. 166-167).

Desse modo, é preciso destacar primordialmente o artigo 11 e seus parágrafos, para ir ao encontro da operacionalização da *accountability* no tratamento de dados pessoais realizado por agentes de menor porte. Assim, conforme dispõe o artigo:

> Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.
> § 1º O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I da LGPD.
> § 2º A indicação de encarregado por parte dos agentes de tratamento de pequeno porte será considerada política de boas práticas e governança para fins do disposto no art. 52, §1º, IX da LGPD. (BRASIL, 2022)

A desnecessidade da indicação de um encarregado, "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (BRASIL, 2018), foi discutida durante a elaboração final do texto da resolução, registrada opiniões diversas sobre a sua aplicabilidade, conforme indicado pela Nota Técnica 35/2021/CGN/ANPD:

> Tiveram contribuições que abordaram a exclusão do dispositivo, visto que reconhecem a atribuição essencial para o desenvolvimento da atividade de proteção de dados desempenhada por profissional altamente qualificado sobre o assunto. Outras reforçam o fato de que a nomeação de um encarregado é uma boa prática que deve ser observada, argumentando, ainda, que a dispensa do encarregado dos dados fere o direito dos titulares. Houve contribuições sobre o parágrafo único quanto à necessidade de se delimitar como será o canal de comunicação, a inclusão de outras pessoas com conhecimento sobre o assunto, mesmo sem formação como encarregado para que atue em contato com a ANPD. (BRASIL, 2021).

Assim, é possível analisar que pluralidade de opiniões também demonstra que, embora o encarregado não seja juridicamente obrigatório nesses casos, seu papel segue considerado relevante sob a ótica da boa governança e da transparência institucional. Portanto, a equipe do projeto responsável pela redação da norma, definiu que:

> A equipe de projeto, considerando a análise apresentada no item 3.2.2.2 do relatório de Análise de Impacto Regulatório (SEI nº 2811023) para a dispensa da obrigação do encarregado, entende ser necessária a manutenção desta dispensa. Evidenciou-se naquele relatório que obrigar essa indicação aos agentes de tratamento de pequeno porte pode causar impactos negativos nas condições econômicas das empresas. Ademais, experiências internacionais, como a União Europeia, dispensam esta obrigação para grupo de pequenas empresas. No entanto, de forma a estimular a prática de indicação do encarregado, incluiu-se o §2º no art. 12 para considerar a indicação como uma política de boas práticas e governança para fins do disposto no art. 52, §1º, IX da LGPD, ou seja, aplicação de atenuantes caso o agente seja sancionado. (BRASIL, 2021, p. 87-88).

Desse modo, evidencia-se que a manutenção da dispensa da obrigatoriedade de indicação de encarregado para agentes de tratamento de pequeno porte reflete uma preocupação

legítima com a isonomia para o tratamento de dados pessoais entre organizações de diferentes tamanhos. Tal medida busca assegurar que o cumprimento da legislação não se torne inviável ou excessivamente oneroso para agentes de tratamento de menor porte. Conforme indica Guilherme Pinheiro, consultor legislativo na tramitação da LGPD na Câmara dos Deputados:

> (...) a previsão de um tratamento diferenciado para microempresas e startups está diretamente relacionada à disparidade dos recursos humanos e financeiros que estas têm à sua disposição para se adequar à lei diante dos conglomerados econômicos de médio e grande porte. O racional seria aliviar ou facilitar o processo de aderência às obrigações legais até para que novos entrantes desafiassem a posição de agentes econômicos dominantes. (BIONI, 2022, p.165).

Conclui-se que a Resolução CD/ANPD nº 02/2022 materializa o exercício da competência normativa da ANPD, ao adaptar as exigências da LGPD à realidade dos agentes de tratamento de pequeno porte. A flexibilização de obrigações visa não onerar excessivamente os agentes de tratamento de pequeno porte, permite-lhes alcançar conformidade com a LGPD de forma proporcional à sua capacidade operacional. Ao mesmo tempo, deve-se observar a aplicação da *accountability* como mecanismo para prestação de contas.

6 CANAIS DE COMUNICAÇÃO COM O TITULAR DE DADOS

Essa seção tem por objetivo aferir a suficiência do canal de comunicação disponibilizado por agentes de tratamento de menor porte, considera-os instrumentos essenciais à efetivação dos direitos dos titulares de dados pessoais. Busca-se verificar especialmente se a partir da noção de privacidade como autodeterminação informativa, a possibilidade de reconhecer a interatividade e a dinamicidade das obrigações atribuídas ao agente de tratamento, como repercussão de *accountability.*

6.1 Avaliação da suficiência dos canais de comunicação dos agentes de tratamento de menor porte

À luz do que foi desenvolvido no capítulo anterior, em especial quanto à flexibilização regulatória que dispensa a nomeação do encarregado pelo tratamento de dados pessoais para agentes de tratamento de menor porte, ganha relevo a análise do canal de comunicação que deve ser, obrigatoriamente, disponibilizado pelos agentes de tratamento de pequeno porte.

Desse modo, tendo em vista o § 1º, art. 11 da Resolução CD/ANPD nº 02/2022, apesar da não estipulação de um encarregado pelo tratamento de dados pessoais, o agente de tratamento de menor porte deverá, nos termos do art. 41, § 2º, inciso I da LGPD, "aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências" (BRASIL, 2018), como se encarregado fosse[20].

Faz-se necessário destacar que a manutenção dessa obrigação decorre da compreensão externada pela equipe do projeto responsável pela redação da resolução. De acordo com a justificativa constante do Nota Técnica 35/2021/CGN/ANPD, entendeu-se que a criação de critérios normativos mais rígidos para disciplinar o canal de atendimento poderia gerar elevação de custos ao agente de tratamento, consequentemente, compromete-se a viabilidade de conformidade sua conformidade à LGPD. Assim, conforme consignado expressamente no documento técnico:

> **Por fim, ressalta-se que o canal de atendimento tem propósito de disponibilizar ao titular de dados um meio de atendimento de suas reclamações, não**

[20] Nos termos do art. 41, § 2º, I, da LGPD, compete ao encarregado "aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências". Assim, ainda que o agente de tratamento de menor porte esteja dispensado da nomeação formal de um encarregado, ele permanece responsável por desempenhar essas funções, assumindo, na prática, as atribuições que seriam conferidas àquela figura.

> **necessitando, no entendimento da equipe de projeto, de definição de critérios para regular este dispositivo**, tendo em vista a possibilidade de elevação dos custos aos agentes de tratamento de pequeno porte. (BRASIL, 2021, p. 88, grifo nosso).

A partir desse entendimento da ANPD, acerca da desnecessidade da definição de critérios para regular o canal de comunicação, deixou-se livre ao agente de tratamento de menor porte a escolha da forma pela qual será estruturado esse canal, desde que seja capaz de cumprir com sua finalidade essencial aceitar reclamações e comunicações dos titulares, além de prestar esclarecimentos e adotar providências.

Essa opção regulatória, embora vise à redução de encargos operacionais e à promoção da proporcionalidade, pode gerar um desafio concreto à efetividade da comunicação entre titulares e agentes de tratamento de pequeno porte. Em outras palavras, a depender do meio escolhido, o acesso pode ser pouco intuitivo, burocráticos ou pouco transparente.

Em paralelo à outras obrigações, previstas na LGPD, mas flexibilizadas pela Resolução CD/ANPD nº 02/2022, como o próprio registro das operações de tratamento de dados pessoais. Embora o art. 37 da LGPD estabeleça tal registro como uma obrigação geral, a obrigação foi simplificada e foi fornecido um modelo de registro simplificado, intitulado “Modelo de Registro das Operações de Tratamento de Dados Pessoais para Agentes de Tratamento de Pequeno Porte (ATPP)”. Esse modelo, serve como referência para fins de conformidade mínima, demonstra-se a expectativa de que tais agentes documentem as operações de tratamento.

Portanto, diante do direito à autodeterminação informativa (RODOTÀ, 2008, p. 96), como um direito fundamental autônomo que surge da ampliação do direito à privacidade, impõe-se que os agentes de tratamento, ainda que de pequeno porte, observem mecanismos mínimos de garantia à participação ativa do titular no processo de tratamento de seus dados. A disponibilização de um canal de comunicação eficaz não se traduz apenas em cumprimento formal da legislação, mas em verdadeira condição de possibilidade para o exercício autônomo e consciente dos direitos informacionais por parte do titular.

Assim, diante da perspectiva "pessoa–informação–circulação–controle” elaborada por Stefano Rodotà (2008), o canal de comunicação deve ser operacionalizado de modo a fazer da privacidade uma expressão concreta da autodeterminação informativa do titular de dados. Desse modo, para que o canal de comunicação cumpra efetivamente sua finalidade e se revele suficiente enquanto obrigação atribuída ao agente de tratamento de menor porte, exige-se que sua estrutura contemple os elementos da interatividade e da dinamicidade.

Esses elementos decorrem diretamente da compreensão de que os direitos do titular não são estáticos. Assim, mesmo os agentes de menor porte, embora beneficiados por flexibilizações regulatórias, devem estruturar seu canal de comunicação de forma que este seja capaz de atender aos princípios da transparência e da boa-fé.

Nessa lógica, é plenamente possível reconhecer, a partir da noção de privacidade como autodeterminação informativa, que as obrigações impostas aos agentes de tratamento de pequeno porte, precisam assumir caráter interativo e dinâmico, justamente porque se desdobram como expressão prática do princípio da *accountability*.

Conforme ilustra Bioni (2022):

> O jogo da regulação não se limita ao aparato estatal (...), essa divisão de trabalho com entidades de interesse público é ainda mais essencial. É a programada virtude da *accountability* na direção da constituição e consolidação de um sistema nacional de proteção de dados." (BIONI, 2022, p. 237).

Portanto, a manutenção de um canal de comunicação ativo e funcional representa, no contexto dos agentes de pequeno porte, não apenas um cumprimento mínimo de conformidade legal, mas a própria expressão da *accountability*. Conforme indicado anteriormente a *accountability* deve ser colocada em movimento, como um verdadeiro mecanismo dinâmico de prestação de contas, capaz de produzir consequências concretas (BIONI, 2022, p. 97).

7 CONSIDERAÇÕES FINAIS

Tendo em vista a meta de perquirir a possibilidade jurídica de reconhecer a interatividade e dinamicidade das obrigações do agente de tratamento de menor porte relacionadas aos direitos do titular como repercussão de *accountability*, na teia da articulação entre os construtos técnicos de privacidade e de autodeterminação, parece ser viável afirmar que a LGPD representa uma mudança de paradigma na regulação da proteção de dados no Brasil. Afinal, adota uma lógica principiológica que impõe aos agentes de tratamento o dever de atuar com transparência, boa-fé e responsabilidade ativa, podendo assumir tanto uma *perspectiva ex ante e ex post*.

Assim, ao longo do estudo, *accountability* desponta como dotada de natureza relacional, exigindo a presença e a participação dinâmica, facilitada e cíclica entre titular e agente de tratamento, mediante a implementação de práticas auditáveis.

A rigor, a operacionalização da *accountability* na tessitura da normativa protetiva dos dados pessoais pressupõe a sua correlação com as compreensões de *answerability, responsibility* e *liability*, na composição de um sistema plástico, aberto à realidade e interdependente. Significa que é aos agentes de tratamento é atribuído o dever contínuo de justificação e demonstração de conformidade.

A interpretação sistemática da LGPD, conjugada com a concepção de privacidade como autodeterminação informativa, conduz à conclusão de que a efetividade da proteção de dados não decorre apenas da existência de políticas ou protocolos documentais, mas da materialidade de prerrogativa de protagonizar a expressão informativa subjetiva por parte do titular.

A Resolução CD/ANPD nº 2/2022 reconhece as especificidades desses agentes, mas reafirma a vinculação aos princípios da LGPD. O art. 6º do documento infralegal explicita que a flexibilização de deveres. Entretanto, não se afasta o cumprimento das bases legais, dos princípios e dos direitos dos titulares. Verifica-se, portanto, que a responsabilidade permanece como elemento estruturante, mesmo diante de regimes diferenciados, em dimensões próprias de *accountability*.

Instrumentalmente, investiga-se a repercussão da *accountability*, como norma plástica, multifacetada e incentivadora de adoção de preceitos ético-jurídicos, no âmbito desse regime simplificado. A esse propósito, o canal de comunicação deve ser funcional, responsivo e estruturado de modo a viabilizar a participação ativa dos titulares na gestão de seus próprios dados.

Nessa acepção, *accountability* constitui-se vetor diretivo e fundamento de governança, capaz de compatibilizar flexibilidade regulatória e efetividade protetiva, bem como de estruturar um ecossistema de dados transparente, orgânico e codeliberativo. Interatividade e a dinamicidade das obrigações dos agentes de tratamento de menor porte são, nessa medida, decorrências da *accountability* que é transversal à LGPD.

REFERÊNCIAS

BARBOSA, Marco Aurélio Gomes. **Muito além da convergência**: a construção e os interesses nos argumentos de criação da Lei N° 11.638/2007 sob a ótica da análise do discurso**.** 2017. 103 f. Tese (Doutorado) - Programa de Pós-Graduação em Ciências Contábeis, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2017. Disponível em: http://repositorio.jesuita.org.br/bitstream/handle/UNISINOS/6429/Marco%20Aur%c3%a9lio%20Gomes%20Barbosa_.pdf?sequence=1&isAllowed=y. Acesso em: 30 jul. 2025.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo. **Regulamentação e Proteção de Dados Pessoais:** O Princípio da Accountability. Rio de Janeiro: Forense, 2022.

BOULDING, Kenneth E. The economics of knowledge and the knowledge of economics. **The American Economic Review**. V. 56, No. 1 / 2, p. 1-13. 1966. Disponível em: https://cooperative-individualism.org/boulding-kenneth_the-economics-of-knowledge-and-the-knowledge-of-economics-1966-mar.pdf. Acesso em: 18 jul. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Ainda na semana internacional da proteção de dados, ANPD inicia tomada de subsídios sobre microempresa**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/ainda-na-semana-internacional-da-protecao-de-dados-anpd-inicia-tomada-de-subsidios-sobre-microempresa. Acesso em: 30 jul. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Normatização. **Análise das contribuições da consulta pública referente à proposta regulamento de aplicação da LGPD para microempresas e empresas de pequeno porte**. Nota Técnica nº 35/2021/CGN/ANPD. 16 dez. 2023. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/8813. Acesso em: 31 Jul. 2025.

BRASIL. Senado Federal. Agência Senado. Sancionada com vetos lei geral de proteção de dados pessoais. **Senado Notícias**, Sítio eletrônico, ago. 2018. Disponível em: https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 30 Jul. 2025.

BRASIL. **Emenda Constitucional n° 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Casa Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 28 jun. 2025.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Secretaria-Geral. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 jun. 2025.

BRASIL. Presidência da república/ANPD. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. **Diário Oficial da União**: seção 1, Brasília, DF, 28 jan. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 31 jul. de 2025

CASTELLS, Manuel. **A era da informação:** a sociedade em rede. 6ª ed. São Paulo: Paz e Terra, 2002.

CRUZ, Letícia Octaviano; IZBICKI, Rafael. Monitoramento Online da Dengue: Usando o Google para Predizer Epidemias. **Brazilian Journal of Biometrics**. V. 36, n. 3, 2018. Disponível em: https://doi.org/10.28951/rbb.v36i3.227. Acesso em: 25 jul. 2025

DE PAULA, Felipe; NAEGELE, Vitor Rabelo. Há vício de iniciativa na criação da Autoridade Nacional de Proteção de Dados? **Jota.** Disponível em: https://www.jota.info/tributos-e-empresas/regulacao/ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados. Acesso em: 30 jul. 2025.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 38 Ed. Rio de Janeiro: Forense, 2025. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649440. Acesso em: 31 jul. 2025

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados, 2ª ed. São Paulo: Thomson Reuters Brasil, 2020.

DOS SANTOS, Romualdo Batista. *Responsibility*, *liability*, *accountability* e *answerability*: sistema articulado de responsabilidade civil em face das tecnologias digitais. **Revista de Direito da Responsabilidade**, p. 138-159, fev. 2023. Disponível em: https://revistadireitoresponsabilidade.pt/2023/responsibility-liability-accountability-e-answerability-sistema-articulado-de-responsabilidade-civil-em-face-das-tecnologias-digitais-romualdo-baptista-dos-santos/. Acesso em: 29 jul. 2025

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. **Comentário à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Thomson Reuters, 2019.

FERNANDES, Marcelo Eloy; NUZZI, Ana Paula Eloy. Fundamentos da Lei Geral de Proteção de Dados (LGPD): Uma revisão narrativa. **Research, Society and Development**. 2022. Disponível em: https://www.researchgate.net/publication/363588627_Fundamentos_da_Lei_Geral_de_Protecao_de_Dados_LGPD_Uma_revisao_narrativa. Acesso em: 20 jul. 2025.

FILHO, Marçal Justen. **Curso de Direito Administrativo**. 16ª Edição 2025, Rio de Janeiro: Forens, 2025. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788530996345/. Acesso em: 9 ago. 2025.

ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. Accountability e Mitigação da Responsabilidade Civil na Lei Geral de Proteção de Dados *In* FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e Políticas de Proteção de Dados**. São Paulo:

Thomsom Reuters, 2022, cap. 32. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/32-accountability-e-mitigacao-da-responsabilidade-civil-na-lei-geral-de-protecao-de-dados-pessoais-compliance-e-politicas-de-protecao-de-dados/1506551422. Acesso em: 15 jul. 2025

FREIRE, Rodrigo da Cunha Lima. O processo civil na sociedade da informação: estudo de um caso. **Revista do Instituto dos Advogados de São Paulo**. São Paulo: Revista dos Tribunais, 2006.

JÚNIOR SIQUEIRA, Paulo Hamilton. **Teoria do direito**. 5ª ed. Rio de Janeiro: Saraiva Jur, 2019. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553609192/. Acesso em: 20 jul. 2025.

LACERDA, Francisco Rogério de Jesus; BARBOSA, Rildo Pereira. **Psicologia no trabalho**. São Paulo: Expressa, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786558110248 Acesso em: 20 jul. 2025

LERMAN, Jonas. Big data and its exclusions. **Stanford Law Review Online.** 2013. Disponível em: http://ssrn.com/abstract=2293765. Acesso em: 10 jul. 2025.

MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor**. São Paulo: Revista dos Tribunais, 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 27 jul. 2025.

OECD. **Our history:** Better policies for better lives since 1960**.** Disponível em: https://www.oecd.org/en/about/history.html. Acesso em: 29 jun. 2025

RACHED, Danielle Hanna. The concept(s) of Accountability: Form in Search of Substance. **Leiden Journal of International Law**, 2016. Disponível em: https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/abs/concepts-of-accountability-form-in-search-of-substance/8E481D883DC5B5E9752C3CCA9BE39884. Acesso em: 05 jul. 2025

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson. A polissemia da responsabilidade civil na LGPD. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/336002/a-polissemia-da-responsabilidade-civil-na-lgpd. Acesso em: 15 jul. 025.

SOMBRA, Thiago Luís Santos. **Direito à privacidade e proteção de dados no ciberespaço:** A Accountability como fundamento da Lex Privacy. 2019. 219 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de Brasília, Brasília, 2019.

TOMAZETTE, Marlon. **Curso de direito empresarial**: Teoria geral e direito societário*,* 13. ed., São Paulo: SaraivaJur, 2022.

VAN ALSENOY, Brendan. **Data protection law in the EU:** roles, responsibilities and liability. Cambridge: Intersentia, 2019.

VIEIRA, Lucas Pacheco. **Direitos do titular de dados pessoais no ordenamento jurídico brasileiro**. Revista dos Tribunais, v. 1058, p. 119-140, dez. 2023. São Paulo: Revista dos Tribunais, 2023. Disponível em: https://www.researchgate.net/profile/Lucas-Vieira-12/publication/377075909_DIREITOS_DO_TITULAR_DE_DADOS_PESSOAIS_NO_ORDENAMENTO_JURIDICO_BRASILEIRO/links/65942e212468df72d3f5297e/DIREITOS-DO-TITULAR-DE-DADOS-PESSOAIS-NO-ORDENAMENTO-JURIDICO-BRASILEIRO.pdf. Acesso em: 27 jul. 2025.

WAXMAN, Olivia B. **The GDPR is just the latest example of Europe's caution on Privacy Rights that Outlook has a disturbing history.** Disponível em: https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/. Acesso em: 20 jul. 2025.

ANEXO A – RESOLUÇÃO CD/ANPD Nº 02 DE 27 DE JANEIRO DE 2022

DIÁRIO OFICIAL DA UNIÃO
Publicado em: 28/01/2022 | Edição: 20 | Seção: 1 | Página: 6
Órgão: Presidência da República/Autoridade Nacional de Proteção de Dados

RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022

Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), com base nas competências previstas no art. 55-J, inciso XVIII, da Lei nº 13.709, de 14 de agosto de 2018, no art. 2º, inciso XVIII, do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I do Regimento Interno da ANPD, tendo em vista a deliberação tomada no Circuito Deliberativo nº 04/2022, e pelo que consta no processo 00261.000054/2021-37, resolve:

Art. 1º Aprovar o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

WALDEMAR GONÇALVES ORTUNHO JUNIOR
Diretor-Presidente

ANEXO I

REGULAMENTO DE APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018,

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD), PARA AGENTES

DE TRATAMENTO DE PEQUENO PORTE

TÍTULO I

DISPOSIÇÕES GERAIS

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Este regulamento tem por objetivo regulamentar a aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte, com base nas competências previstas no art. 55-J, inciso XVIII, da referida Lei.

Parágrafo único. Este regulamento não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, bem como nas demais hipóteses previstas no art. 4º da LGPD.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 2º Para efeitos deste regulamento são adotadas as seguintes definições:

I - agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte,*startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;

II - microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, sociedade limitada unipessoal, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e 18-A, §1º da Lei Complementar nº 123, de 14 de dezembro de 2006;

III -*startups*: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no Capítulo II da Lei Complementar nº 182, de 1º de junho de 2021; e

IV - zonas acessíveis ao público: espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus, de metrô e de trem, aeroportos, portos, bibliotecas públicas, dentre outros.

Art. 3º Não poderão se beneficiar do tratamento jurídico diferenciado previsto neste Regulamento os agentes de tratamento de pequeno porte que:

I - realizem tratamento de alto risco para os titulares, ressalvada a hipótese prevista no art. 8º;

II - aufiram receita bruta superior ao limite estabelecido no art. 3º, II, da Lei Complementar nº 123, de 2006 ou, no caso de startups, no art. 4º, § 1º, I, da Lei Complementar nº 182, de 2021; ou

III - pertençam a grupo econômico de fato ou de direito, cuja receita global ultrapasse os limites referidos no inciso II, conforme o caso.

CAPÍTULO III

DO TRATAMENTO DE ALTO RISCO

Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:

I - critérios gerais:

a) tratamento de dados pessoais em larga escala; ou

b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;

II - critérios específicos:

a) uso de tecnologias emergentes ou inovadoras;

b) vigilância ou controle de zonas acessíveis ao público;

c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou

d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

§ 1º O tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

§ 2º O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

§ 3º A ANPD poderá disponibilizar guias e orientações com o objetivo de auxiliar os agentes de tratamento de pequeno porte na avaliação do tratamento de alto risco.

Art. 5º Caberá ao agente de tratamento de pequeno porte, quando solicitado pela ANPD, comprovar que se enquadra nas disposições do art. 2º e do art. 3º deste regulamento em até quinze dias.

TÍTULO II

DO TRATAMENTO DE DADOS PESSOAIS PELOS AGENTES DE TRATAMENTO

DE PEQUENO PORTE

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 6º A dispensa ou flexibilização das obrigações dispostas neste regulamento não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD, inclusive das bases legais e dos princípios, de outras disposições legais, regulamentares e contratuais relativas à proteção de dados pessoais, bem como direitos dos titulares.

CAPÍTULO II

DAS OBRIGAÇÕES DO AGENTE DE TRATAMENTO DE PEQUENO PORTE

Seção I

Das obrigações relacionadas aos direitos do titular

Art. 7º Os agentes de tratamento de pequeno porte devem disponibilizar informações sobre o tratamento de dados pessoais e atender às requisições dos titulares em conformidade com o disposto nos arts. 9º e 18 da LGPD, por meio:

I - eletrônico;

II - impresso; ou

III - qualquer outro que assegure os direitos previstos na LGPD e o acesso facilitado às informações pelos titulares.

Art. 8º Fica facultado aos agentes de tratamento de pequeno porte, inclusive àqueles que realizem tratamento de alto risco, organizarem-se por meio de entidades de representação da atividade empresarial, por pessoas jurídicas ou por pessoas naturais para fins de negociação, mediação e conciliação de reclamações apresentadas por titulares de dados.

Seção II

Do Registro das Atividades de Tratamento

Art. 9º Os agentes de tratamento de pequeno porte podem cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do art. 37 da LGPD, de forma simplificada.

Parágrafo único. A ANPD fornecerá modelo para o registro simplificado de que trata o caput.

Seção III

Das Comunicações dos Incidentes de Segurança

Art. 10. A ANPD disporá sobre flexibilização ou procedimento simplificado de comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da regulamentação específica.

Seção IV

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.

§ 1º O agente de tratamento de pequeno porte que não indicar um encarregado deve disponibilizar um canal de comunicação com o titular de dados para atender o disposto no art. 41, § 2º, I da LGPD.

§ 2º A indicação de encarregado por parte dos agentes de tratamento de pequeno porte será considerada política de boas práticas e governança para fins do disposto no art. 52, §1º, IX da LGPD.

Seção V

Da Segurança e das Boas Práticas

Art. 12. Os agentes de tratamento de pequeno porte devem adotar medidas administrativas e técnicas essenciais e necessárias, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.

Parágrafo único. O atendimento às recomendações e às boas práticas de prevenção e segurança divulgadas pela ANPD, inclusive por meio de guias orientativos, será considerado como observância ao disposto no art. 52, §1º, VIII da LGPD.

Art. 13. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los 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 política simplificada de segurança da informação deve levar em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte.

§ 2º A ANPD considerará a existência de política simplificada de segurança da informação para fins do disposto no art. 6º, X e no art. 52, §1º, VIII e IX da LGPD.

TÍTULO III

DOS PRAZOS DIFERENCIADOS

Art. 14. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro:

I - no atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, §§ 3º e 5º da LGPD, nos termos de regulamentação específica;

II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos de regulamentação específica, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada regulamentação;

III - no fornecimento de declaração clara e completa, prevista no art. 19, II da LGPD;

IV - em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento.

Parágrafo único. Os prazos não dispostos neste regulamento para agentes de tratamento de pequeno porte serão determinados por regulamentação específica.

Art. 15. Os agentes de tratamento de pequeno porte podem fornecer a declaração simplificada de que trata o art. 19, I, da LGPD no prazo de até quinze dias, contados da data do requerimento do titular.

TÍTULO IV

DISPOSIÇÕES FINAIS

Art. 16. A ANPD poderá determinar ao agente de tratamento de pequeno porte o cumprimento das obrigações dispensadas ou flexibilizadas neste regulamento, considerando as circunstâncias relevantes da situação, tais como a natureza ou o volume das operações, bem como os riscos para os titulares.