Proteção de Dados Pessoais no Setor Financeiro: a *accountability* como ponte entre inovação, concorrência e proteção do consumidor

DOI: 10.58766/rpgbcb.v19i1.1250

Lorenzzo Antonini Itabaiana*
Eduardo Goulart Pimenta**

Recebido/Received: 29/10/2025
Aprovado/Approved: 11/12/2025

Resumo

O artigo examina a centralidade do princípio da *accountability* na Lei Geral de Proteção de Dados (LGPD) e sua função de salvaguarda da dignidade da pessoa humana no tratamento de dados no setor financeiro. Adota-se método dedutivo, com revisão bibliográfica nacional e estrangeira, relacionando os quatro standards propostos por Daniel Sarmento – valor intrínseco, autonomia, mínimo existencial e reconhecimento – às exigências materiais e procedimentais da LGPD. O estudo identifica a *accountability* como eixo operativo de governança que reduz assimetrias informacionais, disciplina incentivos econômicos e estrutura a transparência, especialmente no setor financeiro. Demonstra-se que instrumentos como registros das operações, Relatório de Impacto à Proteção de Dados (RIPD), testes de legítimo interesse e atuação do encarregado tornam auditáveis as escolhas técnicas e comerciais dos agentes de tratamento. O estudo demonstra que a *accountability* é o eixo central de governança da LGPD, especialmente diante da conclusão de que o direito fundamental à proteção de dados não é absoluto e admite flexibilização. Sustenta-se, por fim, que a convergência regulatória entre a Agência Nacional de Proteção de Dados (ANPD), Banco Central do Brasil (BC) e Conselho Administrativo de Defesa Econômica (Cade) deve reforçar a previsibilidade e a segurança jurídica, convertendo a dignidade em parâmetro operacionalizável para uma economia orientada a dados.

Palavras-chave: LGPD. *Accountability. Dignidade da pessoa humana. Concorrência. Consumidor. Sistema Financeiro Nacional.*

* Advogado. Mestre em Direito e Tecnologia pela Universidade Federal de Minas Gerais (UFMG). Especialista em Direito Digital, Gestão da Inovação e Propriedade Intelectual pela Pontifícia Universidade Católica de Minas Gerais (PUC/MG).

** Professor Associado de Direito Empresarial da Universidade Federal de Minas Gerais (UFMG). Professor Adjunto IV de Direito Empresarial na Pontifícia Universidade Católica de Minas Gerais (PUC/MG). Membro do corpo docente do Programa de Pós-Graduação em Direito da UFMG e da PUC/MG. Doutor e Mestre em Direito Empresarial pela Faculdade de Direito da UFMG. Procurador do Estado de Minas Gerais. Consultor e Árbitro societário.

Personal Data Protection in the Financial Sector: accountability as a bridge between innovation, competition, and consumer protection

Abstract

The paper examines the centrality of the accountability principle in Brazil's General Data Protection Law (LGPD) and its role in safeguarding human dignity. A deductive method is adopted, based on national and international literature review, relating the four standards proposed by Daniel Sarmento – intrinsic value, autonomy, existential minimum, and recognition – to the LGPD's material and procedural requirements. The study identifies accountability as an operational governance axis that reduces information asymmetries, disciplines economic incentives, and structures transparency, particularly in the financial sector. It demonstrates that instruments such as records of processing, DPIA, legitimate-interest tests, and the data protection officer's role make the technical and commercial choices of data controllers and processors auditable. The study concludes that accountability is the central governance axis of the LGPD, acting as a balancer that reduces information asymmetries, structures transparency, and disciplines economic incentives, especially in the financial sector. It is therefore argued that the fundamental right to data protection is not absolute and allows flexibility when a proper legal basis, proportionality, and accessible data-subject controls are ensured. Finally, it sustains that regulatory convergence among the National Data Protection Authority (ANPD), the Banco Central do Brasil (BCB), *and the Administrative Council for Economic Defense (Cade) reinforces predictability and legal certainty, converting dignity into an operational benchmark for a data-driven economy.*

Keywords: *LGPD. Accountability. Human dignity. Competition. Consumer. Brazilian National Financial System.*

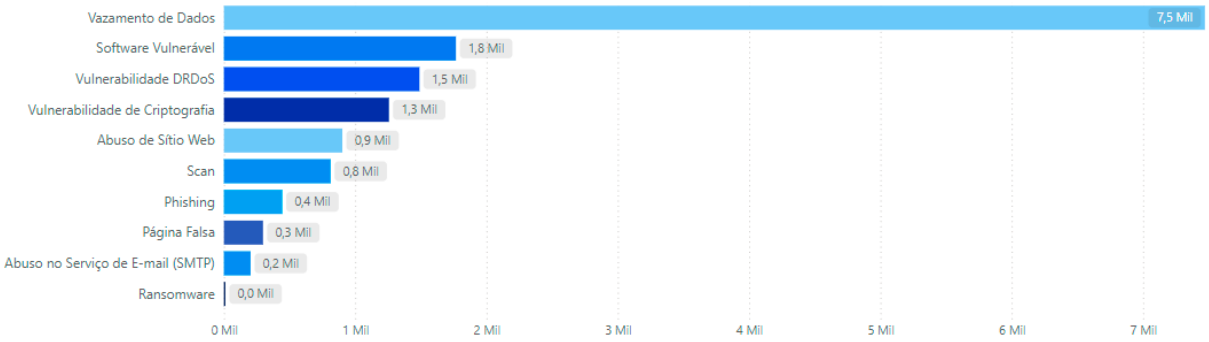
Introdução

Em 2024 foram reportados 14.654 riscos cibernéticos, dentre os quais se inserem incidentes de segurança da informação ou vulnerabilidades.[1] Segundo dados do CTIR Gov "Em Números",[2] a maior parte de tais riscos são relativos a vazamento de dados:

1 Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 6 jan. 2025.

2 O CTIR Gov "Em Números" é uma iniciativa criada com o objetivo de disponibilizar estatísticas gerais de interesse público relacionadas aos incidentes cibernéticos de governo, em um ambiente que simplifica o acesso e compreensão dos dados, utilizando-se de relatórios interativos e uma interface visual mais amigável. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 6 jan. 2025.

Figura 1 – Riscos cibernéticos em 2024



Fonte: CTIR Gov.

As ameaças, contudo, não se limitam a violações da confidencialidade dos dados pessoais. O tratamento irregular, em desacordo com a legislação, e, muitas vezes, de forma discriminatória, é um risco a direitos e garantias fundamentais que se coloca aos titulares, especialmente no setor financeiro. Esse risco deve ser gerenciado pelos agentes de tratamento, especialmente pelas organizações que dependam de autorização do BC. Nesse contexto, os direitos dos consumidores dos serviços ofertados por essas organizações, especialmente o direito fundamental à proteção de dados e à dignidade da pessoa humana, são ameaçados. A proteção a tais direitos, contudo, precisa ser balizada à luz dos demais interesses envolvidos no tratamento de dados pessoais.

Utilizando o método eminentemente dedutivo, com base em literatura nacional e internacional,[3] o trabalho buscou responder à seguinte pergunta: **como o princípio da *accountability* na LGPD atua para conciliar a dignidade da pessoa humana com a inovação, a concorrência e a proteção do consumidor, especialmente no setor financeiro?**

Para tanto, no **primeiro tópico**, foi abordada a inclusão da proteção de dados pessoais no rol de direitos fundamentais pela Emenda Constitucional 115/2022 e o impacto dessa mudança nas dimensões subjetiva e objetiva desse direito. Discutiu-se, de igual maneira, a respeito das obrigações dos agentes de tratamento impostas pela LGPD, dentre as quais se insere a responsabilização e a prestação de contas (*accountability*).

No **segundo tópico**, examinou-se o tratamento de dados no setor financeiro sob a perspectiva da defesa da concorrência e da proteção do consumidor. Para tanto, analisou-se o tratamento de dados pessoais no âmbito do Sistema Financeiro Nacional (SFN) e, na sequência, a correlação entre os riscos decorrentes desse tratamento e os elementos centrais da dignidade da pessoa humana, com base nos quatro *standards* propostos pelo Professor Daniel Sarmento: valor intrínseco, autonomia, mínimo existencial e reconhecimento.

Ao fim, defendeu-se que, embora a dignidade da pessoa humana deva ser preservada, a disciplina da proteção de dados pessoais exige a ponderação de interesses econômicos lícitos, que devem ser respeitados de igual maneira. Nesse cenário, argumenta-se que o princípio da responsabilização e prestação de contas (*accountability*) é importante baliza para o balanceamento de tais interesses, a fim de garantir vantagens sociais como o desenvolvimento econômico e a inovação no setor financeiro, sem, contudo, violar direitos e garantias fundamentais, como a autodeterminação informativa e a proteção da dignidade da pessoa humana.

3 Aqui, será dada prioridade para a literatura europeia, em especial do Prof. Stefano Rodotà. Embora a disciplina da proteção de dados não seja discutida somente na Europa, as maiores discussões se iniciaram lá, culminando no *General Data Protection Regulation*, a Lei Geral de Proteção de Dados da Europa, que inspirou a criação da legislação brasileira. Portanto, é prudente buscar conceitos e percepções do velho continente.

1 Proteção de dados pessoais como direito fundamental e o princípio da *accountability*

A proteção de dados pessoais é um direito fundamental. Desde o julgamento das Ações Diretas de Inconstitucionalidade 6.388, 6.389, 6.390 e 6.391 pelo Supremo Tribunal Federal (STF), e da promulgação da Emenda Constitucional 115/2022, esse direito foi incluído no rol de direitos fundamentais do art. 5º da Constituição da República Federativa do Brasil de 1988 (CR/1988).

Como todo direito fundamental, a proteção de dados passou a ser dotada de dimensões subjetivas e objetivas.[4] Na dimensão subjetiva, houve o alargamento das pretensões do titular de dados pessoais para que fossem adotados determinados comportamentos sobre seus dados, obrigando os agentes de tratamento (controladores e operadores) a proteger os dados pessoais e os titulares.

Esses titulares passaram a ter o direito de exigir o cumprimento de ações concretas a preservar sua vida íntima, seja diretamente pela via administrativa, por meio de canais da ANPD que permitem tanto a denúncia quanto o peticionamento,[5] seja judicialmente. Tais direitos já existiam, por exemplo, para postulação em face do Poder Público para obter informações de seu interesse particular, ou de interesse coletivo ou geral, prestadas no prazo da Lei Federal 12.527/2011 (Lei de Acesso à Informação). A inovação reside no fato de que, agora, os direitos irradiam do reconhecimento do cidadão como titular de dados pessoais, que merece proteção, conforme art. 5º, LXXIX, da Constituição Federal, e é igualmente oponível frente aos agentes privados.

Na dimensão objetiva, houve a produção de consequências práticas, irradiando em todo ordenamento jurídico como um vetor a ser seguido pelo Poder Público e por particulares.[6] Como consequência dessa dimensão, a Lei Federal 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD),[7] passou a exigir que os agentes de tratamento de dados pessoais adotassem determinados comportamentos, se responsabilizando e prestando contas,[8] demonstrando a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados. Esse princípio foi acolhido pelo Regulamento Geral sobre a Proteção de Dados (RGPD),[9] legislação que inspirou a criação da LGPD,[10] e que, em seu art. 5º, 2, o define simplesmente como *accountability*. Na LGPD, esse princípio está disposto no art. 6º, X.

Embora não seja possível afirmar a existência de uma hierarquia de princípios infraconstitucionais, o princípio da *accountability* parece ter uma posição central. *Accountability* é "um processo ativo de criação de conhecimento cujo objetivo é escrutinar determinado agente para tornar uma avaliação mais viável"[11] (tradução livre). Devido à complexa e tecnológica natureza da sociedade atual, há uma profunda necessidade de que os agentes de tratamento prestem contas e tornem suas atividades escrutináveis.[12] No fundo, tal necessidade reflete a obrigação dos agentes de tratamento em fornecer

4 MENDES, Gilmar; GONET, Paulo. **Curso de direito constitucional**. 15. ed. São Paulo: Saraiva Educação, 2020, p. 218-219.

5 https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular. Acesso em: 28 out. 2025.

6 GONÇALVES, Bernardo. **Curso de Direito Constitucional**. 13. ed. Salvador: Ed. JusPodivm, 2021, p. 366.

7 Embora a LGPD tenha sido publicada em agosto de 2018, os dispositivos relativos à *accountability* entraram em vigor somente em agosto de 2020, conforme art. 65, II da LGPD, portanto após o julgamento das ADIns pelo STF.

8 BRASIL. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Brasília, DF: Diário Oficial da União, 2018. Art. 6º, X.

9 "A *accountability* é, portanto, um dos pilares do atual sistema comunitário europeu de proteção de dados pessoais12, claramente prevista no art. 5º, 2, e art. 24, 1, do GDPR, bem como no regramento jurídico de vários países fora do bloco europeu.13 Inclusive no Brasil, em que a LGPD acolheu esse princípio – e todo o raciocínio estrutural que dele decorre – no art. 6º, X, com o nome de "responsabilização e prestação de contas" (Parentoni, 2021, p. 5).

10 DE LUCCA, Newton; MACIEL, Renata Mota. A Lei 13.709, de 14 de agosto de 2018: a disciplina normativa que faltava. *In*: DE LUCCA *et al*. **Direito e Internet IV**. Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019, p. 38.

11 Do original: *accountability is an active knowledge creation process aimed at being scrutinized to re-establish the agent-principal relationship by making assessment more feasible. In*: DE HERT, Paul; LAZCOZ, Guillermo. **When GDPR-Principles Blind Each Other:** *Accountability*, Not Transparency, at the Heart of Algorithmic Governance. European Data Protection Law Review. Berlin: Lexxion. v. 08, n. 01, p. 31-40, Apr. 2022, p. 4.

12 DE HERT, Paul; LAZCOZ, Guillermo. When GDPR-Principles Blind Each Other: *Accountability*, Not Transparency, at the Heart of Algorithmic Governance. European Data Protection Law Review. Berlin: Lexxion. v. 08, n. 01, p. 31-40, Apr. 2022, p. 5.

informações suficientes ao titular, para garantir o exercício de seus poderes individuais à limitação ou determinação das operações de tratamento.[13]

Para auxiliar em tal gestão, o art. 50 §2º, I, *d*, da LGPD define que o controlador poderá implementar Programa de Governança em Privacidade e Proteção de Dados que, no mínimo, estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade. Tal comando parece ser um incentivo para que os agentes de tratamento[14] determinem, com base em uma avaliação de risco, um sistema de controle e monitoramento, permitindo que o agente de tratamento assuma riscos de forma controlada.

A palavra "riscos" ocorre mais de onze vezes na LGPD, permitindo inferir, em conjunto com o art. 50 §2º, I, *d*, da LGPD, que essa avaliação é relevante para a LGPD. Ainda, a avaliação sistemática dos riscos permite que as instituições organizem as medidas a serem adotadas por ordem de prioridade, visando reduzir o impacto tanto nas atividades das organizações quanto na privacidade e na proteção dos dados pessoais dos titulares. Portanto, no contexto da proteção de dados, o risco deve ser encarado não como um entrave ético/moral, mas como uma realidade sobre a qual não se pode escapar, e que baliza a alocação correta dos recursos.

Mas de qual risco estamos falando? Certamente não se trata do risco do mero acesso às informações pessoais. A noção de privacidade, isoladamente, remonta, desde o célebre texto de Samuel D. Warren e Louis D. Brandeis, "*The Right to Privacy*",[15] à noção de uma negação do acesso, vinculando o uso da informação ao consentimento do titular. Se alguém tira, sem autorização, uma foto do quarto do leitor, viola a sua privacidade. Essa foto pode conter informações privadas sobre o gosto do leitor em decoração, o tamanho de sua cama ou o estilo do seu guarda-roupa, entre outros fatos que, embora pareçam irrelevantes a um primeiro olhar, são capazes de revelar aspectos íntimos. Tais aspectos íntimos, sem o consentimento do leitor, não deveriam ser revelados ao mundo, ou poderiam causar surpresa caso o fossem nesses termos. Por isso, é preciso negar acesso às informações a tais terceiros não autorizados, e somente divulgar mediante o consentimento do leitor.

A disciplina da proteção dos dados pessoais não necessariamente produz os mesmos efeitos. Na era capitalista e informacional,[16] o avanço das tecnologias e o uso maciço de dados pessoais para finalidades econômicas tornou impensável a busca do consentimento para todos os usos. Se o leitor fotografa seu quarto e a posta voluntariamente em uma rede social, como o Instagram, certamente a plataforma utilizará suas preferências para alimentar o sistema de leilões de anúncios (*ads)*.[17] Pela LGPD, poderá fazê-lo, inclusive, sem o seu consentimento, com base no legítimo interesse (art. 7º, IX, da LGPD), desde que haja legítima expectativa e os demais requisitos previstos pela Lei. Contudo, cabe à rede social fornecer informações suficientes para que o leitor possa, livremente, decidir se continuará postando fotos de seu quarto no Instagram, e quais as consequências de continuar a fazê-lo.

Essa alteração de paradigma foi traduzida por Stefano Rodotà como uma "passagem de uma enunciação negativa e passiva da proteção dos dados para uma positiva e dinâmica".[18] Assim, não é

13 MONTEIRO, Renato Leite. **Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil**. 2021. 383 f. Tese (Doutorado em Direito Comercial) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021, p. 86.

14 Embora a obrigação seja do controlador, entende-se que é recomendável que operadores também mantenham um programa de governança em proteção de dados, especialmente porque, em algum momento de suas atividades, tratarão dados pessoais na condição de controladores. Isso é o caso, por exemplo, de tratamento de dados de colaboradores. Neste caso, o agente de tratamento que atua como operador na sua atividade-fim atuará como controlador nas suas atividades-meio.

15 WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, v. 4, n. 5, p. 193–220, 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 23 dez. 2024.

16 PELT, Eder van. **Sujeito de direito digital**: a nova governamentalidade do sujeito na era digital. Rio de Janeiro: Telha, 2024, p. 29.

17 Conforme se extrai do *site* do Instagram Business: https://business.instagram.com/advertising?locale=pt_BR. Acesso em: 30 dez. 2024.

18 RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 60.

mais necessário verificar abuso ou violação dos dados para que ao titular seja garantido o direito de interferir nas etapas do tratamento dos seus dados pessoais.[19] Se o dado agora pode ser tratado sem o seu consentimento, ao titular também é dado o poder de interferir sobre tal tratamento.

Para que esse giro fosse possível, foi necessário também ampliar a participação do titular no processo de tratamento. Tal ampliação foi resumida pela *autodeterminação informativa*, fundamento da disciplina da proteção de dados que proporciona ao indivíduo o controle sobre suas informações.[20] O termo foi cunhado em 1983 pelo Tribunal Constitucional Federal alemão (*Bundesverfassungsgericht), no julgamento na histórica decisão "Volkszählungsurteil"*, que reconheceu o direito à autodeterminação informativa como um direito fundamental.[21] A decisão surgiu em resposta ao Censo de 1983 na Alemanha, que previa a coleta extensiva de dados pessoais. O Tribunal alemão reconheceu que, com o avanço da tecnologia, especialmente no processamento automático de dados, havia um risco significativo de criação de perfis detalhados dos indivíduos sem seu consentimento ou conhecimento. Isso poderia levar a uma vigilância excessiva e influenciar negativamente o comportamento das pessoas devido à pressão psicológica da possível exposição pública.

Fornecendo ao titular armas suficientes para gerenciar seus dados, a LGPD também conferiu aos agentes de tratamento um voto de confiança, presumindo sua boa-fé,[22] desde que prestem contas sobre suas atividades, por meio do atendimento dos princípios constantes nos incisos I a VIII e, caso gerem danos a terceiros (inciso IX), sejam responsabilizados. Em outras palavras, todos os princípios servem para orientar a prestação de contas dos agentes e a consequente responsabilização, contraponto essencial para o equilíbrio das forças. A *accountability* se torna, então, a força que equilibra a dinâmica entre a pessoa física, aquela à qual a Lei atribuiu o papel de titular (ultrapassando o conceito de proprietário), e o particular, o qual a Lei denominou agente de tratamento, e que trata os dados pessoais.

O choque entre essas duas forças é inevitável, pois a relação de interesses entre diversas partes envolvidas (*stakeholders*) configura uma relação de agência. Neste tipo de relação, uma parte (*agent*) promete algum tipo de performance perante outra parte (*principal*)[23]. Havendo conflitos sobre esses interesses, está-se diante de um conflito de agência, o que pode acarretar custos adicionais às partes (custos de agência). Por consequência, para mediar esses conflitos e gerenciar os custos envolvidos, tornou-se necessário prestar contas aos *stakeholders*, por exemplo, entre acionistas/quotistas, administradores, trabalhadores, para o caso de companhias privadas, e sociedade, para medidas que envolvem direitos difusos, como aqueles que envolvem o meio ambiente.

No campo da privacidade e da proteção de dados, os conflitos de interesse são materializados pela necessidade de se conciliar, simultaneamente, o direito fundamental à proteção de dados, à privacidade, dentre outros aspectos da personalidade, com o desenvolvimento econômico, tecnológico, científico e social. Essa preocupação não fugiu aos olhos do legislador, que introduziu, nos fundamentos da LGPD, tais disciplinas, que devem coexistir. Afinal, a boa interpretação da LGPD pressupõe a conciliação da observância dos direitos dos titulares de dados pessoais com o

19 RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 60.

20 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters. 2021, p. 173; RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 46.

21 Julgamento disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html Acesso em: 25 dez. 2024.

22 PARENTONI, Leonardo. Compartilhamento de Dados Pessoais e a Figura do Controlador (Personal Data Sharing and the Role of the Data Controller). 2021. Disponível em: https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller, p. 5. Acesso em: 30 dez. 2024.

23 ARMOUR, John; HANSMANN, Henry; KRAAKMAN, Reiner. Agency Problems and Legal Strategies. *In*: **The Anatomy of Corporate Law**. A comparative and Functional Approach. KRAAKMAN, Reiner *et al*.Oxford: Oxford, 2017, p. 29.

desenvolvimento econômico, tecnológico, e a inovação, conferindo segurança jurídica às partes envolvidas (*stakeholders*).[24]

O desafio posto é, então, o de permitir que instituições desenvolvam suas atividades sem violar direitos básicos dos titulares, ou que, em havendo potencial de violação, que sejam manejados os riscos de forma efetiva.

A inobservância dos princípios, e a possibilidade de violação dos direitos dos titulares se mostram, então, os principais riscos que, na sociedade de vigilância/capitalismo de vigilância,[25] os agentes de tratamento incorrem.[26] Como visto, não se trata somente de um risco à privacidade, no sentido de que tais dados nunca poderiam ter sido tratados, mas sim de uma ausência de controle efetivo e necessário a tais dados enquanto são utilizados para finalidades econômicas, impedindo que o titular exerça, de forma consciente, controle sobre suas informações. O risco se agrava na medida em que o tratamento em desacordo com os princípios pode levar a violações dos direitos e garantias fundamentais.

Temos, portanto, um direito fundamental à proteção de dados pessoais que, por meio do princípio da responsabilização e prestação de contas, visa proteger outros direitos fundamentais, como a não discriminação, a honra, e a vida privada (art. 5º, I e X, da Constituição Federal). Todos eles essenciais a uma vida digna. Violá-los, seria, então, violar a própria dignidade da pessoa humana.

O princípio da dignidade da pessoa humana é consagrado no art. 1º, III, da Constituição Federal de 1988 como um dos fundamentos da República Federativa do Brasil. Este modelo constitucional, inspirado nas constituições europeias pós-Segunda Guerra Mundial, prioriza os direitos e garantias fundamentais, que, no Brasil, foram elevados à condição de cláusulas pétreas (art. 60, §4º).

A Constituição Brasileira, nesse sentido, coloca a pessoa humana no centro do ordenamento jurídico, não sob uma perspectiva individualista, mas dentro de um contexto social e coletivo.[27] A dignidade da pessoa humana, portanto, é um valor que permeia todas as normas jurídicas, orientando sua interpretação e aplicação, e serve como critério para a criação ou reconhecimento de novos direitos fundamentais,[28] mesmo quando não expressamente previstos na Constituição. Exemplo disso foi o próprio julgamento que reconheceu o direito à proteção de dados como um direito fundamental, conforme a Emenda Constitucional 115/2022.

Para evitar interpretações abertas e vazias sobre o conteúdo da dignidade da pessoa humana, faz-se necessário fornecer balizas sobre o seu significado no contexto deste trabalho. Contudo, advertimos que definir a dignidade da pessoa humana não é objeto deste trabalho, nem poderíamos fazê-lo em tão apertado espaço. A proposta será somente adotar um *standard* para evitar um uso maleável[29] e amorfo da dignidade da pessoa humana.

Para tanto, será adotada a visão do Professor Daniel Sarmento,30 que, em sua obra *Dignidade da pessoa humana: conteúdo, trajetórias e metodologia*, decompõe a dignidade da pessoa humana em quatro elementos básicos:

24 PARENTONI, Leonardo. Compartilhamento de Dados Pessoais e a Figura do Controlador (Personal Data Sharing and the Role of the Data Controller). 2021, p. 3. "Busca-se, apenas, fornecer uma visão panorâmica do tema, seguida da posição jurídica do autor, de forma clara, fundamentada e com enfoque prático, tendo como premissa compatibilizar o respeito aos direitos do titular de dados pessoais com o desenvolvimento econômico, a inovação e o funcionamento do "mercado de dados", a fim de trazer segurança jurídica a todos os envolvidos".

25 Para ficarmos com os termos utilizados, respectivamente, por Stefano Rodotà e Shoshana Zuboff. *In*: RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008; ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Nova York: Perseus Books, 2019.

26 É certo que existem outros riscos, não ligados ao titular, como riscos coletivos, ou de danos à própria sociedade empresária, mas não fazem parte do objeto de estudo deste artigo, que tem como finalidade investigar o impacto de eventual tratamento na dignidade da pessoa humana.

27 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.

28 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 77.

29 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 16.

30 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.

- valor intrínseco da pessoa;
- autonomia;
- mínimo existencial; e
- reconhecimento.

A decomposição da dignidade da pessoa humana em *standards* objetivos permite deslocar o debate da mera retórica para parâmetros jurídicos verificáveis. Ao se adotar tais critérios como referencial interpretativo, o princípio da *accountability* deixa de ser apenas um comando abstrato da LGPD e passa a ser compreendido como instrumento de concretização da dignidade em suas diversas dimensões: resguardo do valor intrínseco da pessoa, garantia de autonomia decisória, proteção de um mínimo existencial informacional e promoção do reconhecimento social em contextos digitais.

Essa perspectiva é particularmente relevante quando se analisam setores intensivos em dados, como o sistema financeiro nacional. Ali, o entrelaçamento entre proteção de dados pessoais, defesa da concorrência e tutela do consumidor evidencia que a *accountability* não é apenas um dever técnico de conformidade, mas um elemento estrutural de justiça econômica e social. É nesse cenário que se insere a análise a seguir, dedicada a examinar como tais princípios dialogam no ambiente regulatório das instituições financeiras, cooperativas de crédito, *fintechs* e demais atores que operam em um mercado profundamente orientado pela informação.

2 Tratamento de dados no setor financeiro: defesa da concorrência e direitos do consumidor

O sistema financeiro é, historicamente, um dos ambientes mais sensíveis em termos de tratamento de dados pessoais. Bancos, cooperativas de crédito, *fintechs*, seguradoras e instituições de meios de pagamento dependem intensamente da coleta e análise de informações sobre seus clientes para ofertar produtos e serviços. Dados cadastrais, transacionais, biométricos e de comportamento de consumo tornam-se ativos centrais para a estratégia de negócios, gerando inovações, mas também riscos jurídicos e éticos.

Nesse cenário, a proteção de dados pessoais não pode ser analisada isoladamente. O fluxo massivo de informações que circula entre instituições financeiras, consumidores e plataformas tecnológicas produz efeitos diretos na concorrência entre agentes econômicos e na tutela do consumidor. A própria Constituição Federal, ao mesmo tempo em que assegura a livre iniciativa e a livre concorrência (art. 170, *caput* e IV), protege os direitos do consumidor como princípio da ordem econômica (art. 170, V). Assim, o debate sobre proteção de dados encontra no setor financeiro um campo privilegiado para observar tensões entre eficiência econômica, competição justa e direitos fundamentais, materializando o conflito de agência que mencionamos no capítulo anterior.

2.1 Tratamento de dados pessoais no SFN

A informação é hoje um dos principais fatores de competitividade no setor financeiro. Embora a aplicação de técnicas matemáticas aos negócios não seja um fenômeno oriundo do século XXI, a quantidade de dados pessoais (*big data*), processados em larga escala por ferramentas inovadoras como o *machine learning*, impulsionados pela alta capacidade de processamento computacional,

abriu caminhos para inovação em diversos setores da sociedade, descobrindo-se padrões ocultos, antes não identificáveis à *razão humana. Nesse sentido, há tendência de as instituições do século XXI estarem orientadas a dados para maximizar sua produtividade,*[31] mantendo-se competitivas.

As vantagens de exploração dos dados puderam ser verificadas por meio de experiências feitas no setor bancário na década de 90, considerado como um *early adopter*[32] pela implementação precoce dos princípios da Ciência de Dados. Os americanos Richard Fairbanks e Nigel Morris compreenderam que a informática teria um potencial de gerar modelos preditivos mais sofisticados, que poderiam ser aplicados a serviços bancários, como a concessão de linhas de crédito, análise de taxas de pagamento, e até mesmo na análise de perda de clientes (*user churn*).[33] Para isso, contudo, era necessário obter dados de qualidade e de forma minimamente estruturados. Pensando nisso, Fairbanks e Morris sugeriram que fossem oferecidos serviços diversos aleatoriamente a clientes do banco *Signet*, do estado da Virgínia, nos Estados Unidos. Ainda que, inicialmente, a iniciativa tenha gerado um prejuízo ao banco, eventualmente a descoberta de padrões de consumo financeiro e a tomada de decisões baseada nesses padrões tornou a operação tão lucrativa que foi realizada uma cisão[34] na empresa, criando-se o Capital One, um importante banco dos Estados Unidos.

No Brasil, o tratamento de dados pessoais por meio do SFN é objeto de densa normatização infralegal, cuja observância é essencial para a efetividade do princípio da *accountability*. A atuação coordenada do BC e do Conselho Monetário Nacional (CMN) estrutura um regime regulatório que busca compatibilizar inovação, segurança e proteção de dados.

No plano normativo, destacam-se a Resolução CMN 4.893/2021, que trata da política de segurança cibernética, e a Resolução BCB 85/2021, que dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados em nuvem. Essas normas complementam o regime da LGPD ao impor deveres de governança e controles internos, exigindo que as instituições financeiras implementem políticas de proteção e monitoramento contínuo de riscos operacionais e de segurança da informação.

Já o Open Finance, regulamentado pela Resolução Conjunta 1/2020 (BC, CMN e CNSP), é exemplo paradigmático da aplicação do princípio da responsabilidade proativa. O modelo de compartilhamento padronizado de dados e serviços, mediante consentimento do cliente, reforça a transparência e a autodeterminação informativa, mas exige das instituições participantes mecanismos auditáveis de registro, autenticação e rastreabilidade, instrumentos típicos de *accountability*.

Além disso, o Manual de Supervisão do BC e o Guia de Boas Práticas de Cibersegurança evidenciam que a prestação de contas não é apenas documental: ela se concretiza no acompanhamento contínuo dos riscos e na capacidade das instituições de demonstrar que adotam medidas técnicas e organizacionais eficazes. A ausência de tais mecanismos pode ensejar medidas de supervisão ou sanções administrativas, conforme o art. 44 da LGPD. O princípio da *accountability*, portanto, conecta-se diretamente à função supervisora do BC, que, ao exigir evidências verificáveis de conformidade, internaliza o comando do art. 6º, X, da LGPD no regime prudencial do SFN.

Apesar da importância do tratamento dos dados pessoais às instituições, não se pode perder de vista que a exploração massiva de dados pode, ao mesmo tempo, ocasionar riscos à privacidade

31 PROVOST, Foster; FAWCETT, Tom. **Data Science for Business**: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013, p. 10.

32 PROVOST, Foster; FAWCETT, Tom. **Data Science for Business**: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013, p. 7.

33 PROVOST, Foster; FAWCETT, Tom. **Data Science for Business**: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013, p. 10.

34 Para o Direito brasileiro, e conforme o art. 229 da Lei 6.404/1976, a cisão é a operação pela qual a companhia transfere parcelas do seu patrimônio para uma ou mais sociedades.

e à proteção dos dados dos consumidores, bem como à concentração de mercado. A seguir trabalharemos, sob os quatro *standards* propostos pelo Professor Daniel Sarmento, como esses riscos à dignidade da pessoa humana podem se materializar no tratamento de dados dos agentes do SFN.

2.2 Quatro *standards* para a dignidade da pessoa humana: um tratamento ético para o SFN

2.2.1 Valor intrínseco da pessoa

O primeiro elemento, valor intrínseco da pessoa, busca compreender se existe uma qualidade natural, intrínseca ao ser humano. Para isso, é necessário colocar a dignidade à prova por meio de situações hipotéticas de "colisões entre direitos fundamentais do indivíduo e os interesses da maioria ou de alguma entidade abstrata, como o Estado, a Nação, o povo ou a raça".[35] A questão da tortura costuma ser um exemplo na discussão sobre este valor. É justo torturar uma pessoa para obter uma confissão que poderia salvar diversas vidas? Se não houver certeza sobre quantas ou quais vidas seriam salvas, a tortura segue sendo justa? Ou, ao contrário, existe uma "base moral, que transcende qualquer utilidade"[36] e que precisa ser observada em quaisquer casos?

No campo da proteção de dados pessoais, é necessário questionar se existe um direito absoluto à proteção dos dados pessoais, ou se é possível que, em determinados casos, fundamentos como a privacidade deem espaço para o desenvolvimento tecnológico e a inovação. Essa pergunta demandaria um espaço próprio para aprofundamento, mas é possível descrever, pela própria sistemática da LGPD que expressamos acima, que, em diversos casos, existe uma abertura da legislação para que o desenvolvimento econômico se sobreponha. Por exemplo, ao permitir o uso das suas informações para treinamento de algoritmos de redes sociais com base no legítimo interesse (art. 7º, IX, da LGPD),[37] a legislação está permitindo que, em nome de interesses econômicos, o direito à intimidade, à privacidade, e ao uso da imagem sejam colocados em segundo plano. Contudo, não há propriamente uma violação de tais direitos, pois a plataforma não pretende (ou não deveria fazê-lo), utilizar a imagem em prejuízo do titular, mas tão somente, treinar o seu algoritmo de inteligência artificial.

Seria possível argumentar que tal uso poderia gerar riscos de discriminação ao titular, o que é uma verdade. Como já visto, o risco é uma consequência natural do tratamento de dados, mas deve ser cuidadosamente manejado. Caso a discriminação a que se teme seja concretizada, haverá violação à dignidade da pessoa humana por não haver um respeito ao valor intrínseco da pessoa. Ou seja, a utilidade econômica somente será justificável quando não prevalecerem direitos e liberdades fundamentais, pois, conforme a fórmula Kantiana,[38] o ser humano é fim em si mesmo. Essa é, inclusive, a limitação literal posta pela LGPD no artigo que define o legítimo interesse,[39] mas aparece também em outras passagens, como na limitação ao uso da base legal da garantia da

35 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 102.

36 SANDEL, Michael J. **Justiça**: o que é fazer a coisa certa. Tradução de Heloísa Matias e Maria Alice Máximo. 40. ed. Rio de Janeiro: Civilização Brasileira, 2024, p. 53.

37 Aqui não se está fazendo uma defesa desta base legal, tão somente utilizando-a hipoteticamente para testar o standard da autonomia sob o aspecto da proteção de dados pessoais.

38 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.

39 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, **exceto no caso de prevalecerem direitos e liberdades fundamentais do titular** que exijam a proteção dos dados pessoais.

prevenção à fraude (art. 11, II, *g*, da LGPD), ou da obrigatoriedade da elaboração de Relatório de Impacto à Proteção de Dados – RIPD (art. 38) quando o tratamento gerar riscos às liberdades civis e aos direitos fundamentais (art. 5º, XVII, da LGPD).

No campo da defesa da concorrência, esse parâmetro contrapõe a redução do indivíduo a mero insumo econômico em mercados digitais. A concentração de dados por grandes instituições financeiras ou plataformas de pagamento pode justificar-se pelo ganho de eficiência, mas deve respeitar a condição do ser humano como fim em si mesmo. Já no âmbito dos direitos do consumidor, essa mesma lógica se aplica contra cláusulas abusivas que impõem autorizações genéricas de uso de dados (Termos de Uso e Políticas de Privacidade), ou práticas que exploram vulnerabilidades informacionais. Na linha da transversalidade da LGPD (art. 45 da LGPD) e da aplicação conjunta de outras normas, o Código de Defesa do Consumidor (CDC) atua como contrapeso à instrumentalização excessiva da pessoa, ao vedar práticas abusivas e reconhecer a dignidade como valor central (art. 4º, *caput*, do CDC).

Portanto, sob o ponto de vista do valor intrínseco da pessoa, admite-se, até certo grau, a instrumentalização dos dados do titular para fins econômicos, desde que não violem outros direitos e garantias fundamentais.

Embora o valor intrínseco da pessoa seja parâmetro de extrema relevância, é necessário compreender, dentro do novo paradigma da disciplina da proteção de dados já exposto anteriormente, como o titular pode, de forma autônoma, influenciar sobre o tratamento dos dados pessoais.

2.2.2 Autonomia

O segundo elemento da dignidade da pessoa humana também coincide, portanto, com essencial elemento para o correto tratamento dos dados pessoais – a possibilidade de se decidir livremente sobre os aspectos ligados à sua vida íntima. Esse elemento pretende compreender até que ponto estamos, de fato, no comando das nossas próprias decisões, e quais os limites dessa liberdade privada. Essa autonomia privada "corresponde à faculdade do indivíduo de fazer e implementar escolhas concernentes à sua própria vida", capaz de decidir o que é bom e o que é ruim para si mesmo.[40] A dignidade da pessoa humana exige, portanto, que o indivíduo possa decidir por si mesmo, sendo plenamente autônomo.

Nesse sentido, é possível falar em autonomia do consumidor no âmbito das relações com dados pessoais? Autoriza com autonomia um cliente que "abre mão" de parte de sua intimidade em troca do uso das suas informações por uma rede social? São prestadas informações suficientes para que o consumidor possa decidir livremente se aceita ou não os termos desse acordo? Essas perguntas retomam, invariavelmente, a discussão da autodeterminação informativa. Esse fundamento, já introduzido anteriormente neste trabalho, exige que sejam prestadas informações suficientes para que o titular possa definir sua conduta frente às políticas de uso das instituições, corrigindo a assimetria informacional na relação entre instituições e consumidores.

Essa assimetria gera um problema de concorrência que repercute diretamente na autonomia do consumidor. A ausência de autonomia e a concentração de dados pelas instituições financeiras também podem levar a barreiras de entrada para novos concorrentes, levando o titular a depender das poucas instituições que se destacam no mercado. A experiência do *open finance*, liderada pelo Banco Central, ilustra uma tentativa de correção dessa distorção: ao possibilitar a portabilidade

40 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 140.

de dados financeiros mediante consentimento do titular, busca-se restituir-lhe controle sobre suas informações e, ao mesmo tempo, fomentar a competição no setor.

Apesar do reconhecimento do direito à autonomia, como todo direito fundamental, a autodeterminação informativa não é absoluta. No próprio julgamento da decisão *Volkszählungsurteil*, que reconheceu o direito à autodeterminação informativa como um direito fundamental,[41] o Tribunal Constitucional Alemão reconhece também a sua limitação, considerando que outros interesses podem se sobrepor a ele:[42]

> ***b) The right to 'informational self-determination' is not, however, guaranteed without limitation.*** *It does not afford the individual absolute or unlimited control over 'their' personal data; rather, the individual develops their personality within the social community, and is dependent on communication with others. Any information, including personal data, mirrors social reality and thus cannot be attributed exclusively to the person concerned.* ***As repeatedly emphasised in the Court's case-law, the Basic Law resolves the tension between the individual and the community by endorsing the notion that the individual is connected to and bound by the community*** *(BVerfGE 4, 7 <15>; 8, 274 <329>; 27, 1 <7>; 27, 344 <351 and 352>; 33, 303 <334>; 50, 290 <353>; 56, 37 <49>). The individual must therefore accept that the right to informational self-determination is, in principle, subject to restrictions serving overriding public interests.* ***(grifo nosso).***

Para o Tribunal Constitucional Alemão, a individualidade não se sobrepõe à coletividade, essencial para a formação do indivíduo, e local onde ele está inserido. Essa visão parece coincidir com as limitações que a LGPD pôs a si mesma. A exemplo, a LGPD não se aplica para segurança pública e defesa nacional.[43] Alguém que tenha cometido um crime certamente não decide autonomamente sobre como a Polícia irá tratar seus dados. Não poderá, de igual maneira, exercer o direito à exclusão dos seus dados das bases policiais. Nesses casos, sobressaem interesses públicos, que limitam a autodeterminação do titular.

Dessa forma, a concessão de informações aos consumidores parece ser a regra: somente estarão dispensados desta obrigação os agentes de tratamento que, comprovadamente, possuírem direitos que se sobreponham aos direitos à informação. Podemos tomar como exemplo o direito à propriedade intelectual, cuja proteção, como já trabalhado, pode ser óbice à ampla informação concedida aos titulares de dados pessoais, ou outros direitos coletivos cuja proteção sobressaia à proteção individual.

2.2.3 Mínimo existencial

O mínimo existencial parte da compreensão de que "o Estado e a sociedade devem prover as condições materiais básicas para os necessitados, que não tenham condições de se sustentar",[44] ideia que foi recepcionada pela Constituição de 1988.[45] Somente perante o básico da subsistência, como

41 Julgamento disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Acesso em: 25 dez. 2024.

42 *Ibidem*, tradução original para o inglês.

43 As hipóteses de não aplicação da LGPD estão dispostas no art. 4º da LGPD: "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II – realizado para fins exclusivamente: *a*) jornalístico e artísticos; ou *b*) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III – realizado para fins exclusivos de: *a*) segurança pública; *b*) defesa nacional; *c*) segurança do Estado; ou *d*) atividades de investigação e repressão de infrações penais; ou IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei".

44 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 190.

45 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 193.

alimentação, educação, saúde, pode um indivíduo exercer plenamente sua autonomia. Embora de aplicação limitada aos propósitos deste trabalho, a noção de mínimo existencial possui interessante correlação com o tema da liberdade.[46]

De igual maneira, e com as limitações naturais da comparação, somente um indivíduo suficientemente informado poderá assumir as rédeas dos seus dados pessoais, compreendendo, inclusive, os riscos em que incorre quando consente com o tratamento de seus dados, ou quando, mesmo sem consentir, decide prosseguir com o uso de determinado produto/serviço. Portanto, no plano da defesa ao consumidor, a noção de mínimo existencial aparece na transparência: sem informações mínimas e adequadas, o consumidor não pode exercer escolhas conscientes sobre crédito, seguros ou uso de biometria. Aqui, a informação funciona como insumo essencial para a liberdade, tornando-se verdadeiro direito fundamental do consumidor.

No plano concorrencial, o mínimo existencial se traduz na obrigação de garantia, para além de informações para uma tomada de decisão informada, ao próprio acesso inclusivo e não discriminatório a serviços financeiros digitais. A exclusão de determinados perfis por critérios algorítmicos opacos pode comprometer a própria cidadania econômica.

2.2.4 Reconhecimento

O reconhecimento, assim como o mínimo existencial, tem aplicação reduzida no âmbito do presente artigo. Contudo, também fornece *insights* interessantes para a compreensão do âmbito de aplicação da dignidade da pessoa humana. Reconhecimento é a "valorização da pessoa reconhecida, em atitude que lhe expressa o devido respeito", cuja falta "oprime, instaura hierarquias, frustra a autonomia e causa sofrimento".[47] É a necessidade, portanto, de ser aceito pelo outro em sua plenitude. O pilar do reconhecimento atinge temas como a orientação sexual, a origem étnica ou racial, religião, dentre outros temas cuja moralidade costuma ser fruto de debates intensos na arena pública.

Essas características do indivíduo têm como ponto comum a possibilidade de, uma vez reveladas de forma indevida, causar discriminação ao titular. Os dados pessoais considerados como sensíveis pela LGPD guardam a mesma semelhança e, por isso, recebem especial proteção da lei, especialmente ao restringir as hipóteses que autorizam o tratamento (bases legais). Esse aspecto também guarda íntima correlação com a autodeterminação informativa, pois, embora seja reconhecida a necessidade de os indivíduos poderem se expressar livremente – e serem reconhecidos e tratados com igual consideração – cabe a cada um definir quando ou como isso será feito. Dessa forma, alguém que deseje expressar ao mundo sua orientação sexual, deve fazê-lo de acordo com seu próprio contexto, considerando os riscos individuais que serão incorridos. Por isso, é relevante que receba informações suficientes de instituições financeiras que podem, potencialmente, tratar este dado pessoal, para que decida se deseja ou não seguir em frente. O tratamento irregular desses dados por instituições financeiras, portanto, afetará profundamente direitos e garantias fundamentais, sendo um risco que os agentes de tratamento deverão avaliar.

Assim, haverá violação ao princípio da dignidade humana quando o tratamento de dados pessoais violar o direito ao reconhecimento, não só pelo direito individual de revelar ao mundo suas características sem represálias e com igual consideração, mas também pelo direito de controlar como fazê-lo.

46 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 197.
47 SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 242.

Conclusão

O presente trabalho buscou compreender como o princípio da *accountability* na LGPD atua para conciliar a dignidade da pessoa humana com a inovação, a concorrência e a proteção do consumidor, especialmente no setor financeiro. Trabalhou-se com a hipótese de que há especial relevância para o princípio da *accountability* no contexto do tratamento de dados no setor financeiro.

A análise da relevância da *accountability* permitiu confirmar a hipótese, demonstrando que esse princípio ocupa posição axial no regime brasileiro de proteção de dados, funcionando como critério operativo para compatibilizar inovação econômica e tutela de direitos fundamentais. Ao tomar os quatro *standards* de dignidade da pessoa humana propostos por Daniel Sarmento – valor intrínseco, autonomia, mínimo existencial e reconhecimento – como balizas normativas, evidencia-se que a LGPD exige dos agentes de tratamento não apenas conformidade formal, mas a capacidade contínua de justificar decisões, medir riscos e demonstrar resultados de proteção efetiva.

Em termos práticos, o princípio da *accountability* projeta-se sobre a regulação bancária como regime complementar de supervisão e governança. No contexto do Banco Central do Brasil, isso significa exigir que as instituições demonstrem, de forma contínua e auditável, a efetividade de seus programas de privacidade e proteção de dados, integrando-os aos sistemas de controles internos e de gestão de riscos operacionais de acordo com as normas específicas do SFN. Portanto, a convergência entre LGPD, Resoluções do CMN/BCB e diretrizes da ANPD configura um regime de governança regulatória integrada, no qual a *accountability* funciona como elo entre inovação tecnológica, estabilidade financeira e proteção do consumidor. Tal integração reforça a função do BC como agente garantidor de um mercado financeiro competitivo, ético e centrado na dignidade da pessoa humana.

A dignidade da pessoa humana, compreendida nesses quatro eixos, não confere um veto absoluto ao tratamento, mas impõe limites materiais e procedimentais: i) vedação à instrumentalização do titular quando houver danos ou riscos relevantes ao tratamento dos dados financeiros; ii) informação suficiente para escolhas livres e reversíveis; iii) salvaguardas mínimas para o exercício real de direitos; e iv) barreiras contra discriminação e estigmatização, viabilizando o acesso ao sistema bancário pelos titulares/consumidores. Nessa moldura, a flexibilidade do tratamento é admissível em hipóteses específicas, desde que lastreada em base legal adequada, proporcionalidade, medidas técnicas e organizacionais verificáveis e mecanismos de controle acessíveis ao titular.

No setor financeiro, cujo tratamento de dados é intenso, a *accountability* cumpre papel estruturante adicional. Ela reduz assimetrias informacionais ao conceder ao titular e ao mercado informações sobre o tratamento de dados, disciplina incentivos econômicos ao prever sanções administrativas e judiciais em caso de inobservância, e viabiliza a concorrência e a defesa do consumidor, ao nivelar as exigências entre diferentes mercados.[48]

Essa nova sistemática implica deslocar o foco de uma visão meramente proibitiva (negação de acesso, por exemplo) para uma governança positiva e dinâmica (controle, transparência e mitigação), com documentação auditável, tais como Registros de Operações (art. 37), RIPDs (art. 38), e Testes de Legítimo Interesse (art. 10). Esses documentos representam a materialização da avaliação de riscos conduzida pelos agentes de tratamento como condição *sine qua non* para o exercício de suas atividades.

48 Considerando que a LGPD possui aplicação em todos os setores da economia, com as exceções à aplicação e as aplicações especiais para agentes de tratamento de pequeno porte.

Por fim, a convergência regulatória entre ANPD, BC e Cade deve ser entendida como extensão institucional da *accountability*: o diálogo coordenado entre as autoridades aumenta a segurança jurídica, ao prever regras e padrões claros aos *stakeholders*, eleva o padrão de governança, e reduz custos de agência entre *stakeholders*.[49]

O caminho prático, portanto, é o da governança viva: para garantir uma *accountability* efetiva, é necessário que os agentes de tratamento do Sistema Financeiro Nacional estabeleçam Programas de Governança em Privacidade e Proteção de Dados com métricas, auditorias periódicas, gestão de terceiros, explicabilidade proporcional e testes de impacto concorrencial e consumerista quando apropriado. É essa arquitetura prática, e não apenas documentos abstratos, como políticas de privacidade genéricas, que torna a dignidade operacionalizável e sustentável em uma economia orientada a dados.

Referências

ALEMANHA. Tribunal Constitucional Federal. **Volkszählungsurteil – Census Act case – Judgment of 15 December 1983** – 1 BvR 209/83.

ARMOUR, John; HANSMANN, Henry; KRAAKMAN, Reiner. Agency Problems and Legal Strategies. *In*: **The Anatomy of Corporate Law.** A comparative and Functional Approach. *KRAAKMAN, Reiner et al*.Oxford: Oxford, 2017.

BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD 18, de 16 de julho de 2024**. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 17 jul. 2024.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 18 jan. 2025.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília, DF: Diário Oficial da União, 2018.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **CTIR-Gov em números**. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 18 jan. 2025.

COSTA, Rafael Viana de Figueiredo. **ANPD, BC e CVM**: reflexões sobre mecanismos de coordenação regulatória. Revista da Procuradoria-Geral do Banco Central, v. 18, n. 1, p. 93-107, jun. 2024.

DE HERT, Paul; LAZCOZ, Guillermo. **When GDPR-Principles Blind Each Other**: Accountability, Not Transparency, at the Heart of Algorithmic Governance. European Data Protection Law Review. Berlin: Lexxion. v. 08, n. 01, p. 31-40, Apr. 2022.

49 Para aprofundamento na interseção entre ANPD, BC e CVM, v. COSTA, Rafael Viana de Figueiredo. ANPD, BC e CVM: reflexões sobre mecanismos de coordenação regulatória. *Revista da Procuradoria-Geral do Banco Central*, v. 18, n. 1, p. 93-107, jun. 2024.

DE LUCCA, Newton; MACIEL, Renata Mota. A Lei 13.709, de 14 de agosto de 2018: A disciplina normativa que faltava. *In*: DE LUCCA *et al*. **Direito e Internet IV. Sistema de Proteção de Dados Pessoais**. São Paulo: Quartier Latin, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3ª Ed. São Paulo: Thomson Reuters. 2021.

GONÇALVES, Bernardo. **Curso de Direito Constitucional**. 13. ed. Salvador: JusPodivm, 2021.

MENDES, Gilmar; GONET, Paulo. **Curso de direito constitucional**. 15. ed. São Paulo: Saraiva Educação, 2020.

MONTEIRO, Renato Leite. **Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil**. 2021. 383 f. Tese (Doutorado em Direito Comercial) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

PARENTONI, Leonardo. **Compartilhamento de Dados Pessoais e a Figura do Controlador (Personal Data Sharing and the Role of the Data Controller)**. 2021. Disponível em: https://www.researchgate.net/publication/351073596_Compartilhamento_de_Dados_Pessoais_e_a_Figura_do_Controlador_Personal_Data_Sharing_and_the_Role_of_the_Data_Controller. Acesso em: 24 dez. 2024.

PELT, Eder van. **Sujeito de direito digital**: a nova governamentalidade do sujeito na era digital. Rio de Janeiro: Telha, 2024.

PROVOST, Foster; FAWCETT, Tom. **Data Science for Business**: What You Need to Know About Data Mining and Data-Analytic Thinking. Sebastopol: O'Reilly, 2013.

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

SANDEL, Michael. **Justiça**: o que é fazer a coisa certa. Tradução de Heloísa Matias e Maria Alice Máximo. 40. ed. Rio de Janeiro: Civilização Brasileira, 2024.

SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, v. 4, n. 5, p. 193–220, 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 23 dez. 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Nova York: Perseus Books, 2019.