PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS: FUNDAMENTOS, PRINCÍPIOS E DESAFIOS NA SOCIEDADE DA INFORMAÇÃO

PRIVACY, PERSONAL DATA PROTECTION, AND THE GENERAL DATA PROTECTION LAW: FOUNDATIONS, PRINCIPLES, AND CHALLENGES IN THE INFORMATION SOCIETY

PRIVACIDAD, PROTECCIÓN DE DATOS PERSONALES Y LEY GENERAL DE PROTECCIÓN DE DATOS: FUNDAMENTOS, PRINCIPIOS Y RETOS EN LA SOCIEDAD DE LA INFORMACIÓN

Rafael Pacheco Lanes Ribeiro[1]

DOI: 10.54899/dcs.v22i83.3701
Recibido: 29/09/2025 | Aceptado: 24/10/2025 | Publicación en línea: 31/10/2025.

RESUMO

A proeminência dos dados pessoais como ativo central na economia digital contemporânea impulsionou a necessidade de um arcabouço jurídico robusto para a sua proteção. A Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), emerge como o marco regulatório brasileiro, alinhando o país a um movimento global de tutela da privacidade e da autodeterminação informativa. Este artigo analisa os fundamentos, princípios e desafios da proteção de dados pessoais no Brasil sob a ótica da LGPD. O objetivo é investigar criticamente a estrutura da lei, desde seus conceitos basilares, como dados pessoais e dados pessoais sensíveis, até o regime de responsabilidade civil dos agentes de tratamento. A metodologia empregada consiste no método de abordagem dedutivo, com procedimento monográfico e técnica de pesquisa bibliográfica, fundamentada exclusivamente na doutrina e nos documentos de referência anexados. Os resultados apontam que a LGPD, inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) europeu, estabelece um sistema complexo baseado em princípios como finalidade, necessidade e não discriminação, e em um rol de bases legais que buscam equilibrar o desenvolvimento econômico e a proteção dos direitos fundamentais. Conclui-se que, apesar dos avanços, a efetiva implementação da lei enfrenta desafios significativos, como a consolidação da cultura de proteção de dados e a atuação da Autoridade Nacional de Proteção de Dados (ANPD).

Palavras-chave: Proteção de Dados. LGPD. Privacidade. Direitos Fundamentais. Sociedade da Informação.

[1] Doutor em Educação, Centro Universitário de Viçosa (UNIVIÇOSA), Viçosa, Minas Gerais, Brasil.
E-mail: pachecolanes@gmail.com Orcid: https://orcid.org/0000-0002-5152-1143

ABSTRACT

The prominence of personal data as a central asset in the contemporary digital economy has driven the need for a robust legal framework for its protection. Law No. 13,709/2018, the General Personal Data Protection Law (LGPD), emerges as the Brazilian regulatory milestone, aligning the country with a global movement to protect privacy and informational self-determination. This article analyzes the foundations, principles, and challenges of personal data protection in Brazil from the perspective of the LGPD. The objective is to critically investigate the law's structure, from its basic concepts, such as personal data and sensitive personal data, to the civil liability regime of processing agents. The methodology employed consists of the deductive approach method, with a monographic procedure and bibliographic research technique, based exclusively on the doctrine and attached reference documents. The results indicate that the LGPD, inspired by the European General Data Protection Regulation (GDPR), establishes a complex system based on principles such as purpose, necessity, and non-discrimination, and on a list of legal bases that seek to balance economic development and the protection of fundamental rights. It is concluded that, despite the advances, the effective implementation of the law faces significant challenges, such as the consolidation of a data protection culture and the role of the National Data Protection Authority (ANPD).

Keywords: Data Protection. LGPD. Privacy. Fundamental Rights. Information Society.

RESUMEN

La importancia de los datos personales como activo central en la economía digital contemporánea ha impulsado la necesidad de un marco legal sólido para su protección. La Ley n.º 13.709/2018, Ley General de Protección de Datos Personales (LGPD), se ha consolidado como el marco regulatorio brasileño, integrando al país en un movimiento global de protección de la privacidad y la autodeterminación informativa. Este artículo analiza los fundamentos, principios y desafíos de la protección de datos personales en Brasil desde la perspectiva de la LGPD. El objetivo es investigar críticamente la estructura de la ley, desde sus conceptos fundamentales, como datos personales y datos personales sensibles, hasta el régimen de responsabilidad civil de los agentes del tratamiento de datos. La metodología empleada consiste en un enfoque deductivo, con un procedimiento monográfico y una técnica de investigación bibliográfica, basada exclusivamente en la doctrina jurídica y los documentos de referencia adjuntos. Los resultados indican que la LGPD, inspirada en el Reglamento General de Protección de Datos (RGPD) europeo, establece un sistema complejo basado en principios como la finalidad, la necesidad y la no discriminación, así como en diversos marcos jurídicos que buscan equilibrar el desarrollo económico y la protección de los derechos fundamentales. La conclusión es que, a pesar de los avances, la aplicación efectiva de la ley se enfrenta a importantes desafíos, como la consolidación de una cultura de protección de datos y el papel de la Autoridad Nacional de Protección de Datos (ANPD).

Palabras clave: Protección de Datos. LGPD. Privacidad. Derechos Fundamentales. Sociedad de la Información.

INTRODUÇÃO

A sociedade contemporânea, frequentemente denominada Sociedade da Informação, caracteriza-se por um fluxo incessante e massivo de dados. Nesse cenário, os dados pessoais converteram-se em um ativo de valor inestimável, o "novo petróleo" da economia digital (Souza; Viola; Padrão, 2019). A capacidade de coletar, processar, analisar e utilizar informações sobre indivíduos em larga escala transformou modelos de negócio, relações sociais e a própria atuação do Estado. Contudo, essa mesma capacidade trouxe consigo riscos significativos à privacidade, à liberdade e a outros direitos fundamentais. O tratamento indiscriminado de dados pessoais pode levar à vigilância, à manipulação de comportamento, à discriminação e à perda do controle individual sobre as próprias informações, um conceito encapsulado no direito à autodeterminação informativa (Mendes, 2018).

É nesse contexto de tensão entre o desenvolvimento tecnológico-econômico e a salvaguarda dos direitos da pessoa humana que o Direito é chamado a intervir. Globalmente, observa-se um movimento de positivação de normas específicas para a proteção de dados pessoais, com destaque para o *General Data Protection Regulation* (GDPR) na União Europeia, que estabeleceu um novo paradigma regulatório. No Brasil, após anos de debates e um processo legislativo complexo (Bioni, 2021), a resposta a essa demanda materializou-se na Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

O problema de pesquisa que orienta este trabalho é: de que forma a Lei Geral de Proteção de Dados Pessoais estrutura a proteção da privacidade e dos dados pessoais no ordenamento jurídico brasileiro e quais são os seus principais desafios de implementação? A relevância desta análise reside na centralidade que a LGPD ocupa na conformação da sociedade digital no Brasil. A lei não apenas estabelece um conjunto de regras para o tratamento de dados por entidades públicas e privadas, mas também promove uma mudança cultural, exigindo uma nova postura de governança de dados e de respeito aos direitos dos titulares.

O objetivo geral deste artigo é analisar criticamente o arcabouço normativo da proteção de dados pessoais instituído pela LGPD, com base na produção acadêmica de referência. Como objetivos específicos, busca-se: (i) explorar os fundamentos do direito à proteção de dados como um direito fundamental autônomo; (ii) examinar os princípios e as bases legais que orientam o tratamento de dados pessoais; (iii) diferenciar o regime de proteção de dados pessoais comuns e

de dados pessoais sensíveis; e (iv) discutir o sistema de responsabilidade civil e os desafios para a efetividade da lei.

A metodologia adotada para a consecução desses objetivos pauta-se pelo método de abordagem dedutivo, partindo-se da análise geral do fenômeno da proteção de dados para a investigação específica da LGPD. O método de procedimento é o monográfico, com o estudo aprofundado do tema a partir de uma base teórica delimitada. A técnica de pesquisa é exclusivamente a bibliográfica, com a análise e a confrontação das obras e artigos científicos fornecidos como referência, cujas ideias e formulações constituem o alicerce argumentativo deste trabalho, sendo devidamente citadas pelo sistema autor-data.

Este artigo está estruturado em seções que buscam refletir a lógica da própria LGPD. Após esta introdução, o desenvolvimento abordará a ascensão da proteção de dados como direito fundamental, os princípios basilares da lei, as hipóteses legais para o tratamento, o regime especial dos dados sensíveis, e o sistema de responsabilização dos agentes. Por fim, a conclusão sintetizará os argumentos, responderá ao problema de pesquisa e apontará para os desafios e as perspectivas futuras na consolidação da cultura de proteção de dados no Brasil.

DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS: A CONSTRUÇÃO DE UM DIREITO FUNDAMENTAL

A consagração da proteção de dados pessoais como um direito fundamental autônomo é um fenômeno jurídico relativamente recente, fruto de uma evolução doutrinária e jurisprudencial que reconfigurou o conceito tradicional de privacidade para fazer frente aos desafios da Sociedade da Informação. Se, em um primeiro momento, a privacidade era associada ao "direito de ser deixado em paz" (*right to be let alone*), focado na proteção da vida privada contra invasões, a ascensão das tecnologias de informação e comunicação exigiu uma nova dimensão: o controle sobre o fluxo das próprias informações.

O Legado de "The Right to Privacy" e a Autodeterminação Informativa

A gênese da preocupação jurídica com a privacidade remonta ao final do século XIX, com o célebre artigo "The Right to Privacy", de Samuel Warren e Louis Brandeis (1890). Publicado na *Harvard Law Review*, o ensaio reagia aos excessos da imprensa e às novas tecnologias de

fotografia, que permitiam uma exposição sem precedentes da vida íntima. Os autores defenderam a existência de um direito geral à privacidade, independente dos direitos de propriedade, como uma salvaguarda para a "inviolabilidade da personalidade" (Warren; Brandeis, 1890). Essa concepção, centrada na proteção contra a publicidade não desejada de fatos da vida privada, influenciou profundamente o direito norte-americano e o pensamento jurídico ocidental, associando a privacidade a uma esfera de intimidade e vida doméstica que deveria ser imune à curiosidade alheia (Ferraz Júnior, 1992).

Contudo, o advento dos computadores e das grandes bases de dados nas décadas de 1960 e 1970 expôs as limitações dessa visão. O problema não era mais apenas a exposição de informações íntimas, mas a coleta e o processamento sistemático de dados pessoais por governos e empresas, muitas vezes para finalidades desconhecidas pelo indivíduo. Relatórios como o "Records, Computers, and the Rights of Citizens" (1973) nos Estados Unidos já alertavam para o risco de uma vigilância massiva e para a necessidade de se estabelecerem princípios para o tratamento justo das informações.

A virada conceitual decisiva ocorreu na Alemanha, com a histórica decisão do Tribunal Constitucional Federal no caso do Censo de 1983. Diante da contestação popular contra a coleta de uma vasta gama de dados pelo Estado, a Corte reconheceu o direito à "autodeterminação informativa" (*informationelle Selbstbestimmung*). Este direito, fundamentado na dignidade da pessoa humana e no livre desenvolvimento da personalidade, garante ao indivíduo o poder de, em princípio, decidir por si mesmo sobre a divulgação e o uso de seus dados pessoais (Mendes, 2018; Doneda, 2006). Como afirma Danilo Doneda (2006), a autodeterminação informativa representa a passagem de uma tutela prevalentemente negativa da privacidade (não invasão) para uma tutela positiva (controle), conferindo ao titular um feixe de poderes sobre suas informações.

Essa noção foi fundamental para o desenvolvimento dos modelos legislativos de proteção de dados na Europa, culminando no GDPR, e influenciou diretamente a construção da LGPD no Brasil (Doneda; Mendes, 2018). A proteção de dados, portanto, descola-se da ideia de segredo ou intimidade para se afirmar como um direito à gestão dos próprios dados, um pressuposto para o exercício de outras liberdades em um ambiente digital.

A Proteção de Dados Pessoais como Direito Fundamental no Brasil

No Brasil, a proteção da privacidade e dos dados pessoais possui assento constitucional. A Constituição Federal de 1988, em seu artigo 5º, inciso X, assegura a inviolabilidade da "intimidade, a vida privada, a honra e a imagem das pessoas". O inciso XII, por sua vez, garante o sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas". Além disso, o *habeas data* (art. 5º, LXXII) foi instituído como um remédio constitucional para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, e para a sua retificação (Mendes, 2018).

Apesar dessa proteção constitucional, a doutrina e a jurisprudência debateram por muito tempo se a proteção de dados pessoais seria um direito autônomo ou uma mera faceta do direito à privacidade. A LGPD veio para consolidar a primeira visão, ao afirmar em seu artigo 1º que a lei dispõe sobre o tratamento de dados pessoais "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

A consagração definitiva veio com a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que incluiu o inciso LXXIX no artigo 5º da Constituição, estabelecendo ser "assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Essa emenda, conforme destaca Ingo Wolfgang Sarlet (2021), eleva a proteção de dados ao status de direito fundamental autônomo, ao lado da privacidade, conferindo-lhe a máxima hierarquia normativa e as garantias inerentes ao regime das cláusulas pétreas (art. 60, § 4º, IV, CF/88).

Com isso, a proteção de dados pessoais no Brasil firma-se como um pilar do Estado Democrático de Direito, sendo simultaneamente um direito de defesa do cidadão perante o Estado e particulares, e uma norma de tutela objetiva que impõe deveres de proteção e conformidade a todos os agentes de tratamento (Sarlet, 1988). A LGPD, portanto, não é uma lei ordinária qualquer, mas o instrumento legal que densifica e dá concretude a um direito fundamental recém-explicitado na Carta Magna, estabelecendo as condições e os limites para o tratamento de dados em território nacional (Bioni, 2021).

OS PILARES DA REGULAÇÃO: PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

A arquitetura da Lei Geral de Proteção de Dados Pessoais é fundamentalmente principiológica. O artigo 6º da lei estabelece um decálogo de princípios que devem ser observados em toda e qualquer operação de tratamento de dados pessoais, servindo como vetores interpretativos para a aplicação da norma e como balizas para a atuação dos agentes de tratamento. Esses princípios, que dialogam intensamente com os consagrados no GDPR europeu, formam a base sobre a qual se assenta todo o sistema de proteção, conferindo-lhe coerência e efetividade (Doneda; Mendes, 2018). A sua observância não é uma mera recomendação, mas uma obrigação legal cuja violação pode acarretar as sanções previstas na lei.

Finalidade, Adequação e Necessidade: O Tripé da Limitação do Tratamento

No topo da lista de princípios está o da finalidade, que determina que o tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedado o tratamento posterior de forma incompatível com essas finalidades. Este princípio, como aponta Chiara Spadaccini de Teffé e Mario Viola (2019), combate a prática da coleta de dados sem um objetivo claro, para uso futuro e indeterminado. A finalidade funciona como uma "cláusula de barreira", vinculando o controlador ao propósito informado e garantindo que o titular não seja surpreendido com usos de seus dados para os quais não consentiu ou que não poderiam ser razoavelmente esperados por ele.

Intimamente ligado à finalidade está o princípio da adequação, que exige a compatibilidade do tratamento com as finalidades informadas ao titular. Ou seja, os meios utilizados para o tratamento devem ser condizentes com os fins almejados. Não basta ter uma finalidade legítima; o tratamento efetivamente realizado deve corresponder a ela. Por exemplo, a coleta de dados de geolocalização em tempo real pode não ser adequada para a finalidade de simplesmente enviar um boletim informativo por e-mail.

Completa este tripé o princípio da necessidade, também conhecido como o princípio da minimização dos dados (*data minimisation*). Ele preconiza que o tratamento deve se limitar ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos. Este princípio impõe uma restrição quantitativa e qualitativa à

coleta e ao uso de dados. Os agentes de tratamento devem se questionar constantemente: "Eu realmente preciso deste dado para cumprir esta finalidade específica?". A coleta de dados "por via das dúvidas" ou para enriquecimento futuro da base de dados é, em regra, contrária ao princípio da necessidade (Bioni, 2021). Juntos, finalidade, adequação e necessidade formam a espinha dorsal da limitação do tratamento, garantindo que a intervenção na esfera privada do indivíduo seja a menor possível.

Transparência, Livre Acesso e Qualidade dos Dados: Empoderando o Titular

O princípio da transparência assegura aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. Este princípio é a base para o exercício da autodeterminação informativa. Sem saber quem trata seus dados, para quê, e com quem são compartilhados, o titular não tem como exercer seus direitos de forma eficaz. A transparência deve se manifestar em todos os pontos de contato com o titular, desde avisos de privacidade claros e compreensíveis até respostas ágeis e completas às suas solicitações.

A transparência é instrumentalizada pelo princípio do livre acesso, que garante aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Este princípio materializa o direito de acesso, um dos mais importantes direitos do titular previstos no artigo 18 da LGPD, permitindo que o indivíduo verifique se seus dados estão sendo tratados em conformidade com a lei.

Adicionalmente, o princípio da qualidade dos dados assegura aos titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Dados incorretos, desatualizados ou incompletos podem gerar prejuízos significativos aos titulares, como a recusa de crédito, a perda de uma oportunidade de emprego ou a tomada de decisões automatizadas com base em premissas equivocadas. Este princípio impõe ao controlador o dever de manter a acurácia de sua base de dados, o que se conecta diretamente com o direito do titular à retificação.

Segurança, Prevenção e não Discriminação: A Tutela da Integridade e da Igualdade

A proteção de dados não se resume a regras sobre o que se pode ou não fazer com os dados, mas também sobre como protegê-los. O princípio da segurança impõe a 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. A segurança da informação, que envolve conceitos como confidencialidade, integridade e disponibilidade, torna-se um dever jurídico, cuja negligência pode acarretar a responsabilização do agente (Machado; Doneda, 2020).

De forma proativa, o princípio da prevenção exige a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Isso significa que os agentes de tratamento devem atuar de forma a antecipar riscos, implementando desde o início de seus projetos e processos uma mentalidade de *privacy by design* e *privacy by default*, ou seja, a privacidade desde a concepção e como padrão.

Um dos princípios de maior impacto social é o da não discriminação, que estabelece a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. Este princípio é particularmente relevante na era dos algoritmos e da inteligência artificial, onde decisões automatizadas podem perpetuar e amplificar vieses históricos contra determinados grupos. A coleta de dados sensíveis, como origem racial, convicções religiosas ou opiniões políticas, apresenta um risco discriminatório inerente, exigindo uma tutela ainda mais rigorosa. O princípio veda, por exemplo, que se negue um serviço ou se ofereça um preço mais alto a um consumidor com base em um critério discriminatório inferido a partir de seus dados.

Responsabilização e Prestação de Contas (*Accountability*)

Por fim, a LGPD adota um modelo de responsabilização e prestação de contas (*accountability*). Este princípio exige que o agente de tratamento demonstre a 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. Não basta cumprir a lei; é preciso ser capaz de comprovar o cumprimento. Isso inverte o ônus da prova, que passa a ser do controlador, e incentiva uma postura proativa de governança de dados. Instrumentos como o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) são manifestações diretas deste princípio, forçando

as organizações a analisar, documentar e mitigar os riscos de suas operações de tratamento antes mesmo de iniciá-las (Bioni, 2019]).

AS HIPÓTESES LEGAIS PARA O TRATAMENTO: QUANDO É PERMITIDO TRATAR DADOS PESSOAIS

Qualquer operação de tratamento de dados pessoais, para ser considerada lícita, deve estar fundamentada em uma das bases legais previstas na LGPD. A lei abandona o modelo anterior, largamente baseado apenas no consentimento, para adotar um rol mais amplo e diversificado de hipóteses autorizativas, elencadas nos artigos 7º (para dados pessoais em geral) e 11 (para dados pessoais sensíveis). Essa mudança, inspirada no GDPR, reconhece que o consentimento nem sempre é a base legal mais adequada ou viável, e busca fornecer um cardápio de opções que se ajustem aos múltiplos contextos de tratamento de dados na sociedade contemporânea (Teffé; Viola, 2019). A escolha da base legal adequada é uma das decisões mais críticas para o controlador, pois ela definirá os direitos do titular e os deveres do agente de tratamento naquela operação específica.

O Consentimento do Titular: Manifestação Livre, Informada e Inequívoca

O consentimento continua a ser uma das bases legais mais importantes, mas a LGPD o qualifica com requisitos rigorosos para garantir sua validade. O artigo 5º, inciso XII, define o consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". A análise de cada um desses elementos revela a profundidade da mudança em relação a práticas anteriores, que frequentemente se contentavam com cláusulas genéricas em termos de serviço.

- **Livre:** A manifestação de vontade não pode ser viciada. O titular não pode ser coagido a consentir, e a recusa em fornecer o consentimento não pode lhe trazer prejuízos indevidos, especialmente quando se trata do acesso a produtos e serviços. O consentimento não é considerado livre quando o titular não possui uma escolha real, como em relações de trabalho, onde há um desequilíbrio de poder (Bioni, 2019).
- **Informada:** O titular deve receber informações claras e precisas sobre a finalidade específica do tratamento, a forma e a duração, a identificação do controlador, o uso

compartilhado de dados e as consequências de não consentir. A informação deve ser prestada previamente à coleta, de forma ostensiva e destacada, proibindo-se as autorizações genéricas.

- **Inequívoca:** O consentimento deve ser dado por meio de um ato positivo e claro do titular, que não deixe dúvidas sobre sua intenção. Caixas de seleção pré-marcadas ou o silêncio do titular não configuram consentimento inequívoco. É preciso uma ação afirmativa (opt-in).

Além disso, o consentimento deve ser fornecido para finalidades determinadas. Se o controlador desejar tratar os dados para um novo propósito, deverá obter um novo consentimento específico para tal. A LGPD também estabelece que o consentimento é revogável a qualquer momento, de forma gratuita e facilitada. Uma vez revogado, o controlador deve cessar o tratamento, a menos que possa fundamentá-lo em outra base legal (o que deve ser analisado com cautela para não esvaziar o direito à revogação).

O Legítimo Interesse do Controlador: A Mais Flexível e Desafiadora das Bases Legais

Talvez a inovação mais significativa e complexa da LGPD em matéria de bases legais seja a introdução do legítimo interesse do controlador ou de terceiros (art. 7º, IX). Esta base legal permite o tratamento de dados sem o consentimento do titular para finalidades legítimas, desde que, no caso concreto, não prevaleçam os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

O legítimo interesse é uma base legal flexível, mas não um "cheque em branco". Sua aplicação exige um exercício de ponderação criterioso, conhecido como "teste do legítimo interesse" ou, na terminologia do GDPR, *Legitimate Interest Assessment* (LIA). Conforme detalhado por Souza, Viola e Padrão (2019), esse teste envolve, em geral, três etapas:

1 **Teste da Finalidade:** O controlador deve identificar qual é o seu interesse legítimo. Esse interesse não pode ser ilícito ou contrário à moral e deve ser concreto e real. Exemplos comuns incluem a prevenção a fraudes, o apoio e promoção de atividades do controlador (marketing direto) e a proteção do crédito.

2 **Teste da Necessidade:** O controlador deve avaliar se o tratamento de dados pessoais é realmente necessário para alcançar a finalidade legítima pretendida. Se houver outras

formas menos intrusivas de atingir o mesmo objetivo, o tratamento de dados pode não ser justificado.

3 **Teste do Balanceamento:** Esta é a etapa mais crítica. O controlador deve ponderar o seu interesse legítimo em face dos direitos e liberdades fundamentais do titular, bem como de suas legítimas expectativas. Deve-se perguntar: o impacto na privacidade do titular é desproporcional ao interesse perseguido? O titular razoavelmente esperaria que seus dados fossem usados para essa finalidade? Fatores como a natureza dos dados, a forma como são tratados, e as salvaguardas adotadas (anonimização, criptografia) são cruciais nesta ponderação.

A LGPD exige, ainda, que, ao tratar dados com base no legítimo interesse, o controlador adote medidas para garantir a transparência, informando ao titular sobre o uso de seus dados. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é frequentemente o documento onde esse teste de ponderação é formalizado, demonstrando a *accountability* do controlador.

Outras Bases Legais para o Tratamento de Dados

Além do consentimento e do legítimo interesse, o artigo 7º da LGPD prevê outras oito bases legais que se aplicam a contextos específicos, dispensando a necessidade de consentimento. Entre elas, destacam-se:

- **Cumprimento de obrigação legal ou regulatória pelo controlador:** Quando uma lei ou norma exige que o controlador trate os dados (ex: obrigações fiscais, trabalhistas).
- **Execução de políticas públicas pela administração pública:** Para o tratamento de dados pelo Poder Público no exercício de suas competências.
- **Realização de estudos por órgão de pesquisa:** Garantida, sempre que possível, a anonimização dos dados.
- **Execução de contrato ou de procedimentos preliminares:** Quando o tratamento é necessário para a celebração ou execução de um contrato do qual o titular seja parte.
- **Exercício regular de direitos em processo judicial, administrativo ou arbitral:** Para a produção de provas, por exemplo.
- **Proteção da vida ou da incolumidade física do titular ou de terceiro:** Em situações de emergência.

- **Tutela da saúde:** Em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- **Proteção do crédito:** Conforme previsto na legislação pertinente.

A escolha correta da base legal é um passo fundamental para a conformidade com a LGPD, pois impacta diretamente a relação com o titular dos dados e define o escopo dos direitos e deveres de cada parte. A multiplicidade de hipóteses reflete a complexidade das interações na Sociedade da Informação e exige dos agentes de tratamento uma análise jurídica cuidadosa e documentada.

O REGIME ESPECIAL DOS DADOS PESSOAIS SENSÍVEIS: UMA TUTELA REFORÇADA

A Lei Geral de Proteção de Dados Pessoais estabelece uma distinção crucial entre dados pessoais comuns e uma categoria especial que, por sua natureza, apresenta um maior potencial de dano e discriminação ao titular: os dados pessoais sensíveis. Essa diferenciação não é meramente terminológica; ela implica a aplicação de um regime jurídico significativamente mais restritivo para o tratamento de dados sensíveis, refletindo uma preocupação elevada do legislador com a proteção de aspectos íntimos da personalidade e com a prevenção de práticas excludentes. A lógica subjacente é que certas informações, se utilizadas de forma indevida, podem expor o indivíduo a estigmas, preconceitos e violações de seus direitos mais básicos (Mulholland, 2018).

Definição e Riscos Associados

O artigo 5º, inciso II, da LGPD, define dado pessoal sensível como toda informação sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Este rol é taxativo e sua amplitude demonstra a intenção de proteger informações intrinsecamente ligadas à identidade, às crenças, à saúde e às liberdades individuais do cidadão.

O tratamento dessas informações acarreta riscos elevados. Como ilustra Caitlin Sampaio Mulholland (2018) através de casos emblemáticos, o vazamento ou o uso indevido de dados sobre saúde ou comportamento sexual pode levar à exposição pública e ao constrangimento. A

utilização de dados sobre opinião política ou filiação sindical pode resultar em perseguição. O processamento de dados sobre origem racial ou étnica pode alimentar algoritmos discriminatórios que perpetuam desigualdades sociais no acesso a crédito, emprego ou seguros. É justamente para mitigar esses riscos que a lei impõe um ônus muito maior para quem deseja tratar dados pessoais sensíveis.

O princípio da não discriminação, previsto no artigo 6º, ganha aqui uma importância superlativa. Enquanto para dados comuns se proíbe o tratamento para fins discriminatórios *ilícitos ou abusivos*, a própria natureza do dado sensível já acende um alerta máximo. O tratamento de um dado sobre a convicção religiosa de uma pessoa, por exemplo, é inerentemente mais arriscado do que o tratamento de seu endereço de e-mail, pois o potencial para um uso discriminatório é muito maior.

As Bases Legais Restritas para o Tratamento de Dados Sensíveis

Refletindo essa preocupação, o artigo 11 da LGPD estabelece um conjunto de bases legais para o tratamento de dados sensíveis que é notavelmente mais restrito do que o rol do artigo 7º para dados comuns. A regra geral é a proibição do tratamento, sendo as hipóteses do artigo 11 exceções que devem ser interpretadas restritivamente.

A principal base legal para o tratamento de dados sensíveis é o consentimento do titular, que, neste caso, deve ser fornecido de forma específica e destacada, para finalidades específicas. A exigência de ser "destacado" é um requisito adicional em relação ao consentimento para dados comuns, significando que a autorização para tratar dados sensíveis deve estar visualmente separada de outras cláusulas contratuais ou termos, garantindo que o titular tenha plena e inequívoca ciência da sensibilidade da informação que está compartilhando.

Na ausência do consentimento, o tratamento de dados sensíveis só é permitido em um número limitado de situações, que incluem:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;

b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

e) Proteção da vida ou da incolumidade física do titular ou de terceiro;

f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Uma ausência notável e de extrema importância no rol do artigo 11 é a base legal do legítimo interesse. A LGPD não permite o tratamento de dados pessoais sensíveis com fundamento no legítimo interesse do controlador. Essa vedação é uma das mais importantes salvaguardas da lei, impedindo que os controladores realizem um teste de ponderação para justificar o uso de informações tão críticas sem o consentimento explícito do titular. A mensagem do legislador é clara: o risco inerente aos dados sensíveis é tão alto que a flexibilidade do legítimo interesse não é aplicável, exigindo-se uma justificativa legal mais robusta e objetiva para o seu tratamento.

Em suma, o regime dualista da LGPD, com regras mais brandas para dados comuns e um regime de exceção para dados sensíveis, constitui um mecanismo fundamental para a gradação da proteção conforme o potencial de risco aos direitos e liberdades dos titulares, materializando uma abordagem baseada em risco que é central para os modernos sistemas de proteção de dados.

O EMPODERAMENTO DO INDIVÍDUO: OS DIREITOS DOS TITULARES DE DADOS

Um dos objetivos centrais da LGPD é reequilibrar a relação assimétrica entre os indivíduos e as organizações que tratam seus dados. Para tanto, a lei não se limita a impor deveres aos agentes de tratamento, mas também confere aos titulares um robusto catálogo de direitos, elencados principalmente no artigo 18. Esses direitos são os instrumentos que materializam o princípio da autodeterminação informativa, permitindo que os cidadãos exerçam um controle efetivo sobre o fluxo de suas informações pessoais. O exercício desses direitos deve ser facilitado pelo controlador, de forma gratuita, e as solicitações devem ser atendidas em prazos razoáveis, sob pena de sanções.

O rol de direitos do titular inclui:

- **Confirmação da existência do tratamento:** O direito mais basilar. O titular pode questionar qualquer organização para saber se ela realiza algum tipo de tratamento com seus dados pessoais.
- **Acesso aos dados:** Caso o tratamento seja confirmado, o titular tem o direito de acessar os dados específicos que o controlador possui a seu respeito. A resposta deve ser fornecida em formato claro e que permita a sua compreensão.
- **Correção de dados incompletos, inexatos ou desatualizados:** Conectado ao princípio da qualidade dos dados, este direito permite que o titular solicite a retificação de informações incorretas, garantindo a acurácia dos registros.
- **Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei:** Este direito é uma ferramenta poderosa contra os abusos. Se o titular constatar que o tratamento viola o princípio da necessidade ou que está sendo feito sem uma base legal adequada, ele pode exigir que os dados sejam anonimizados (perdendo a capacidade de identificá-lo), bloqueados (suspensão temporária do tratamento) ou definitivamente eliminados.
- **Portabilidade dos dados a outro fornecedor de serviço ou produto:** Inspirado no GDPR, o direito à portabilidade permite que o titular solicite a transferência de seus dados de um controlador para outro, em formato interoperável. Este direito visa a fomentar a concorrência e a reduzir o chamado "efeito de aprisionamento" (*lock-in*), facilitando a migração do consumidor entre diferentes plataformas e serviços (Bioni, 2019).
- **Eliminação dos dados pessoais tratados com o consentimento do titular:** Salvo as exceções previstas em lei (como o cumprimento de obrigação legal), o titular que forneceu seus dados com base no consentimento tem o direito de solicitar sua eliminação após revogar o consentimento.
- **Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados:** Em linha com o princípio da transparência, este direito permite ao titular mapear o fluxo de suas informações, sabendo quem, além do controlador original, teve acesso aos seus dados.
- **Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa:** Reforça o caráter informado do consentimento, garantindo que o titular tome sua decisão com plena ciência das implicações.

- **Revogação do consentimento:** Como já mencionado, o consentimento pode ser retirado a qualquer momento, de forma simples e gratuita.

Além desses, o artigo 20 garante ao titular o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, como decisões de crédito, recrutamento ou marketing. A lei assegura o direito à explicação sobre os critérios e procedimentos utilizados na decisão automatizada, buscando combater a opacidade das "caixas-pretas" algorítmicas (Bioni, 2021).

Esse conjunto de direitos representa uma mudança de paradigma, transformando o titular de um mero objeto do tratamento em um sujeito de direitos ativo, com poderes para fiscalizar, questionar e determinar os rumos de suas informações pessoais na Sociedade da Informação.

O SISTEMA DE RESPONSABILIZAÇÃO: A RESPONSABILIDADE CIVIL NA LGPD

A eficácia de um regime de proteção de dados depende não apenas da definição de direitos e deveres, mas também da existência de um sistema de responsabilização robusto, capaz de garantir a reparação de danos causados aos titulares e de incentivar a conformidade por parte dos agentes de tratamento. A LGPD, em seus artigos 42 a 45, estrutura um regime de responsabilidade civil que, embora dialogue com as bases do Código Civil e do Código de Defesa do Consumidor, apresenta particularidades que refletem a natureza específica dos riscos na Sociedade da Informação (Tasso, 2019).

A Natureza da Responsabilidade e os Agentes Envolvidos

O artigo 42 da LGPD estabelece que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". Este dispositivo é a pedra angular do sistema de responsabilidade da lei.

Uma das discussões centrais diz respeito à natureza dessa responsabilidade. A doutrina majoritária, com base na redação do artigo 42 e no diálogo com o Código de Defesa do Consumidor (aplicável subsidiariamente às relações de consumo), entende que a responsabilidade do controlador é, em regra, objetiva e solidária. Isso significa que, para que o dever de indenizar seja configurado, basta a comprovação do dano e do nexo de causalidade entre a conduta do

agente e o prejuízo sofrido pelo titular, sendo desnecessária a demonstração de culpa ou dolo do agente (Tasso, 2019; Bioni, 2021). Esse modelo se justifica pelo risco inerente à atividade de tratamento de dados em larga escala; quem lucra com a atividade deve arcar com os riscos que ela gera.

O controlador, a quem competem as decisões referentes ao tratamento, é o principal responsável pela reparação dos danos. O operador, que realiza o tratamento em nome do controlador, responde solidariamente pelos danos causados quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador. Nesse último caso, o operador equipara-se ao controlador para fins de responsabilização. Essa distribuição de responsabilidades incentiva o controlador a escolher operadores diligentes e a formalizar suas instruções, enquanto exige do operador uma postura crítica em relação às ordens recebidas.

O Dano na Proteção de Dados: Patrimonial, Moral e a Perda do Tempo

O dano indenizável na LGPD pode ser de natureza patrimonial (um prejuízo financeiro direto, como uma fraude bancária decorrente de um vazamento de dados) ou moral. O dano moral em matéria de proteção de dados é particularmente relevante e assume contornos próprios. Ele pode decorrer da mera violação do direito à privacidade e à autodeterminação informativa, da angústia gerada pela perda de controle sobre as próprias informações, do constrangimento de ter dados sensíveis expostos, ou da discriminação sofrida em virtude de um tratamento ilícito.

A jurisprudência tem evoluído para reconhecer o chamado dano moral *in re ipsa* em casos de vazamento de dados, especialmente os sensíveis, presumindo-se o abalo psicológico a partir do próprio fato. Além disso, discute-se a aplicação da teoria do desvio produtivo do consumidor, ou perda do tempo útil, para indenizar o tempo que o titular despende tentando resolver problemas causados por um tratamento de dados inadequado, como solicitar a correção de dados ou o cancelamento de um serviço não solicitado.

As Excludentes de Responsabilidade

O artigo 43 da LGPD prevê as hipóteses em que os agentes de tratamento não serão responsabilizados. São elas:

- Quando provarem que **não realizaram o tratamento** de dados pessoais que lhes é atribuído;
- Quando provarem que, embora tenham realizado o tratamento, **não houve violação** à legislação de proteção de dados; ou
- Quando provarem que o dano é decorrente de **culpa exclusiva do titular dos dados ou de terceiros**.

É importante notar que o ônus da prova para a configuração dessas excludentes recai sobre o agente de tratamento, em linha com o princípio da *accountability*. A excludente de "culpa exclusiva de terceiro" é particularmente sensível em casos de ataques cibernéticos (ataques de *hackers*). A jurisprudência tem entendido que, se o ataque foi possibilitado por uma falha de segurança do agente (ou seja, descumprimento do princípio da segurança), o evento não pode ser considerado como um fato de terceiro capaz de romper o nexo causal, caracterizando-se como um fortuito interno, inerente ao risco da atividade.

O sistema de responsabilidade civil da LGPD, portanto, é um mecanismo poderoso para a tutela dos direitos dos titulares. Ao estabelecer uma responsabilidade que tende à objetividade e ao impor um pesado ônus probatório aos agentes de tratamento, a lei cria um forte incentivo econômico para a adoção de boas práticas de governança e para o investimento em medidas técnicas e administrativas de segurança, tornando a proteção de dados um elemento central na gestão de riscos de qualquer organização.

CONCLUSÃO

A travessia da sociedade industrial para a Sociedade da Informação reposicionou o dado pessoal como um elemento central de poder econômico e social, tornando sua regulação uma matéria de urgência para a salvaguarda dos direitos fundamentais. Este artigo buscou responder à questão de como a Lei Geral de Proteção de Dados Pessoais (LGPD) estrutura a proteção da privacidade no Brasil e quais são seus principais desafios. A análise da doutrina de referência permite concluir que a LGPD institui um microssistema jurídico complexo e sofisticado, que representa um avanço civilizatório para o ordenamento brasileiro.

A estrutura de proteção delineada pela lei se assenta em múltiplos pilares. Primeiramente, ela consolida a evolução do direito à privacidade para o direito à autodeterminação informativa, recentemente alçado ao status de direito fundamental autônomo pela Emenda Constitucional nº

115/2022, conferindo ao indivíduo um poder de controle sobre suas informações. Em segundo lugar, a lei estabelece um robusto arcabouço principiológico, com destaque para o tripé finalidade-adequação-necessidade, que impõe limites estritos à voracidade da coleta de dados, e para os princípios da transparência, segurança e não discriminação, que garantem a eticidade do tratamento.

Ademais, a LGPD estrutura-se sobre um rol diversificado de bases legais, superando a antiga dependência do consentimento e introduzindo hipóteses como o legítimo interesse e a execução de contratos, que conferem flexibilidade ao tratamento lícito, embora exijam dos agentes uma análise criteriosa e documentada. A criação de um regime especial e mais rigoroso para dados pessoais sensíveis, vedando o uso do legítimo interesse para seu tratamento, demonstra uma abordagem baseada em risco, que gradua a proteção conforme o potencial de dano ao titular. O empoderamento do indivíduo é materializado por um amplo catálogo de direitos, como o acesso, a correção, a portabilidade e a revisão de decisões automatizadas. Por fim, o sistema de responsabilização, pautado na *accountability* e em um regime de responsabilidade civil que tende à objetividade, cria um forte incentivo para a conformidade.

Contudo, a promulgação da lei é apenas o primeiro passo. Os desafios para sua plena implementação são monumentais. O principal deles é a promoção de uma efetiva cultura de proteção de dados, que impregne as práticas do setor público e do setor privado, superando a mentalidade de que dados pessoais são ativos a serem explorados sem limites. Isso exige investimentos em governança, segurança da informação e treinamento contínuo.

Outro desafio crucial reside na consolidação do papel da Autoridade Nacional de Proteção de Dados (ANPD). A eficácia da lei dependerá da capacidade da ANPD de fiscalizar, orientar o mercado, regulamentar os pontos em aberto da legislação e, quando necessário, aplicar as sanções de forma proporcional e efetiva. A interpretação e aplicação da LGPD pelo Poder Judiciário também serão determinantes para a criação de uma jurisprudência estável que ofereça segurança jurídica aos titulares e aos agentes de tratamento.

As limitações deste estudo residem em sua natureza estritamente bibliográfica, baseada no conjunto de obras fornecido. Pesquisas futuras poderiam se debruçar sobre a análise empírica da implementação da LGPD em setores específicos da economia, o impacto das decisões da ANPD na conformidade das empresas, ou as complexas interações entre a proteção de dados, a inteligência artificial e outras tecnologias emergentes.

Em síntese, a LGPD não é apenas uma lei; é um projeto de sociedade. Um projeto que busca conciliar o inevitável avanço tecnológico com os valores perenes da dignidade humana, da liberdade e da privacidade, reafirmando que, mesmo na era digital, o ser humano deve permanecer no centro da tutela do Direito.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo. **Xeque-Mate:** o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). O direito e o futuro: a tecnologia e o amanhã. São Paulo: Thomson Reuters Brasil, 2019. p. 123-145.

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

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 17-31, nov./dez. 2018.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 87, p. 37-50, 1992.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 4, n. 1, p. 1-20, jan./jun. 2018.

MENDES, Laura Schertel Ferreira. Habeas Data e Autodeterminação Informativa: os dois lados da mesma moeda. São Paulo: **Revista dos Tribunais**, 2018.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direito, Governança e Novas Tecnologias**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. DOI: http://dx.doi.org/10.18759/rdgf.v19i3.1603 ISSN: 2175-6058

RECORDS, **Computers, and the Rights of Citizens:** Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington: U.S. Department of Health, Education & Welfare, 1973.

SARLET, Ingo Wolfgang. A proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988. **Revista de Direito Público**, Brasília, v. 18, n. 100, p. 25-48, nov./dez. 2021.

SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; PADRÃO, Vinícius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. **RDU - Revista de Doutrina e Jurisprudência**, Porto Alegre, v. 16, n. 90, p. 109-131, nov./dez. 2019.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 3, p. 1-20, abr./jun. 2019.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 5, p. 1-38, out./dez. 2019.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, 15 dez. 1890.