Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v10i10.16270

ANÁLISE CONSTRUTIVO DA LEI GERAL DE PROTEÇÃO DE DADOS

Danyel Berk Castro Costa Silva[1]
Eliane Carvalho Falcão[2]

RESUMO: A Lei Geral de Proteção de Dados (LGPD) marca um avanço significativo na proteção da privacidade e dados pessoais no Brasil, inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. A LGPD adota um modelo preventivo e abrangente, reconhecendo que dados pessoais possuem valor intrínseco e representando aspectos essenciais da identidade dos indivíduos. Com um conceito expansivo de dado pessoal, a lei exige bases legais claras para o tratamento de dados e define hipóteses taxativas para justificá-lo. O consentimento do titular deve ser informado, explícito e específico, garantindo a compreensão do tratamento de dados. A LGPD reconhece o legítimo interesse, condicionado a um teste de balanceamento de interesses para não infringir os direitos fundamentais dos titulares. Concede uma gama de direitos aos titulares, como acesso, correção, exclusão e portabilidade, promovendo transparência e controle sobre as informações pessoais. Fundamentada em princípios como finalidade, necessidade, transparência e segurança, a LGPD implementa mecanismos para proteção de dados e exige notificação em caso de incidentes de segurança. Estabelece um regime rigoroso de responsabilidade e penalidades, assegurando o cumprimento das obrigações pelos agentes de tratamento. A LGPD representa um passo crucial na evolução das normas de proteção de dados no Brasil, promovendo uma abordagem equilibrada para enfrentar os desafios da privacidade na era digital, com a Autoridade Nacional de Proteção de Dados desempenhando um papel essencial na sua implementação eficaz.

Palavras-chave: Privacidade. Proteção de dados. Consentimento. Direitos do titular. LGPD.

ABSTRACT: The General Data Protection Law (LGPD) marks a significant advance in the protection of privacy and personal data in Brazil, inspired by the General Data Protection Regulation (GDPR) of the European Union. The LGPD adopts a preventive and comprehensive model, recognizing that personal data has intrinsic value and represents essential aspects of individuals' identities. With an expansive concept of personal data, the law requires clear legal bases for data processing and defines strict hypotheses to justify it. The holder's consent must be informed, explicit and specific, ensuring understanding of the data processing. The LGPD recognizes legitimate interest, subject to a balancing of interests test so as not to infringe the fundamental rights of data subjects. Grants a range of rights to holders, such as access, correction, deletion and portability, promoting transparency and control over personal information. Based on principles such as purpose, necessity, transparency and security, the LGPD implements mechanisms for data protection and requires notification in the event of security incidents. Establishes a strict regime of liability and penalties, ensuring compliance with obligations by processing agents. The LGPD represents a crucial step in the evolution of data protection standards in Brazil, promoting a balanced approach to addressing privacy challenges in the digital era, with the National Data Protection Authority playing an essential role in its effective implementation.

Keywords: Privacy. Data protection. Consent. Subject rights. LGPD.

[1]Graduando em direito pela Universidade de Gurupi, UNIRG.
[2]Orientadora do curso em direito pela Universidade de Gurupi, UNIRG. Especialista em direito tributário, direito público e agronegócio.

1- INTRODUÇÃO

A Lei Geral de Proteção de Dados (Lei nº 13.709/18 - LGPD) parte do princípio de que todo dado pessoal é significativo e possui valor. Por isso, adota um conceito amplo de dado pessoal, similar ao definido no Regulamento Europeu (GDPR - General Data Protection Regulation), como informação relacionada a uma pessoa natural identificada ou identificável. Dados que possam parecer irrelevantes em um momento ou que não se refiram diretamente a alguém, quando transferidos, combinados ou organizados, podem revelar informações bastante específicas sobre uma pessoa, incluindo dados sensíveis, conforme observado pelo Bundesverfassungsgericht (Tribunal Constitucional Federal Alemão) no julgamento emblemático sobre a lei do censo de 1983.

Dada a importância do tema, foi estabelecido como regra geral (Art. 1º) que qualquer pessoa que trate dados, seja física ou jurídica, de direito público ou privado, incluindo atividades realizadas em meios digitais, deve possuir uma base legal para fundamentar o tratamento de dados pessoais. Isso significa que será necessário identificar uma base legal adequada apenas nos casos excluídos pela aplicação da lei, conforme previsto no Art. 4º da LGPD. No entanto, o tratamento de dados pessoais previsto no Art. 4º, inciso III (para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais) "será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei". Para isso, já foi criada uma comissão de juristas na Câmara dos Deputados responsável pela elaboração de um anteprojeto de lei sobre essa matéria.

Portanto, exceto nas hipóteses de exclusão, o tratamento realizado deve se enquadrar em pelo menos uma das hipóteses legais para ser considerado legítimo e lícito, podendo até mesmo cumular essas hipóteses, como no GDPR. Essas bases foram estabelecidas de forma geral e variada, com detalhes e adequações a serem realizados especialmente pela Autoridade Nacional de Proteção de Dados (ANPD), pelo Legislativo e pelo Judiciário.

Entende-se que tanto o rol do Art. 7º quanto o do Art. 11 são taxativos, apesar de conterem hipóteses chamadas de "coringas", ou seja, hipóteses mais abertas e com certo grau de subjetividade (como, por exemplo, o legítimo interesse). No entanto, há autores que defendem a existência de uma outra base legal para o tratamento de dados pessoais no Art. 23 da LGPD, para o exercício geral das competências ou cumprimento de atribuições legais da Administração

Pública. Contudo, entendemos que o tratamento de dados pessoais para tais atividades já está contemplado nas hipóteses relativas ao cumprimento de uma obrigação legal (Art. 7º, II, e Art. 11, II, 'a'), uma vez que a atuação da Administração Pública decorre de um mandamento legal, e ao tratamento e uso compartilhado de dados necessários à execução de políticas públicas (Art. 7º, III, e Art. 11, II, 'b').

Para evitar abusos no tratamento de dados e garantir os direitos do titular, este pode revogar o seu consentimento, conforme será abordado no item 2, ou pleitear o direito à oposição, que significa que o titular pode se opor ao tratamento realizado com base em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD (Art. 18, §2º). Além disso, está positivado o direito à explicação (Art. 20), que dispõe que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

O sistema legal desenvolvido para o tratamento de dados representa para o titular um instrumento de controle sobre suas informações pessoais e de garantia de direitos. Nesse sentido, o presente artigo busca analisar em detalhe os requisitos para o tratamento de dados na LGPD, com ênfase nas bases legais relativas ao consentimento e ao legítimo interesse, e nas diferenças de tratamento estabelecidas para dados considerados sensíveis.

2. O CONSENTIMENTO DO TITULAR

O consentimento do titular dos dados possui um papel crucial na LGPD, ainda que não seja a única base legal para o tratamento de dados pessoais, nem tenha hierarquia superior às demais listadas no Art. 7º. Em determinadas situações, a obtenção do consentimento pode ser inadequada devido à existência de outra base legal mais apropriada no Art. 7º ou no Art. 11. Nesses casos, é mais seguro e adequado utilizar essa outra base legal em vez de buscar o consentimento do titular dos dados, mesmo que seja possível obtê-lo.

Uma análise detalhada dos princípios, que são amplamente centrados no ser humano, demonstra a preocupação do legislador com a participação do indivíduo no controle de suas informações. Conforme discutido, a definição de consentimento na LGPD segue o modelo do Regulamento Europeu e as normas mais recentes sobre o tema. Existem várias disposições que

fornecem regras específicas para implementar, orientar e fortalecer o controle de dados por meio do consentimento.

Em relação ao tratamento de dados, o consentimento deve ser obtido conforme a hipótese estabelecida no artigo 7º, I, da LGPD. Para dados sensíveis, foram estabelecidas normas mais rigorosas (Art. 11, I), como será discutido mais adiante. No caso de crianças, além de um consentimento reforçado, foi incluída uma hipótese adicional de tratamento de dados sem o consentimento de um dos pais ou responsável legal (Art. 14, §3º).

A atenção maior ao consentimento do titular é de extrema importância no cenário tecnológico atual, onde há coleta massiva de dados pessoais, mercantilização desses dados por diversos agentes, e pouca transparência e informação no tratamento de dados pessoais de usuários de serviços online. A interpretação do consentimento deve ser restritiva, não permitindo que o agente estenda a autorização concedida para outros meios, momentos ou finalidades diferentes das acordadas.

O consentimento é um instrumento de manifestação individual no campo dos direitos da personalidade e legitima o uso de dados do titular por terceiros. Ele promove a personalidade, sendo meio para a construção e delimitação da esfera privada, associando-se à autodeterminação existencial e informacional, essencial para a proteção do indivíduo e a circulação de informações.

Segundo a LGPD, o consentimento é caracterizado como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Art. 5º, XII). Isso se alinha com a definição no GDPR: "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

Livre significa que o titular pode escolher entre aceitar ou recusar a utilização de seus dados sem intervenções ou situações que viciem o consentimento. É expressamente proibido o tratamento de dados pessoais mediante vício de consentimento. É importante analisar a assimetria entre as partes e a vulnerabilidade de algum contratante para garantir a validade do consentimento. Como observado, é necessário verificar o "poder de barganha" do cidadão em relação ao tratamento de seus dados, considerando as opções do titular em relação ao tipo de dado coletado e seus possíveis usos.

Para fortalecer o indivíduo, a Lei estabelece que, se o tratamento dos dados pessoais for condição para o fornecimento de um produto ou serviço ou para o exercício de um direito, o titular será informado com destaque sobre isso e sobre os meios de exercer seus direitos (Art. 9º, §3º). Isso regula a lógica binária das políticas de tudo ou nada, incentivando configurações de privacidade personalizáveis e a manifestação granular do consentimento.

Informado significa que o titular deve ter à disposição as informações necessárias para avaliar corretamente como seus dados serão tratados. A informação é crucial para um consentimento livre e consciente, direcionado a um tratamento específico, para determinado agente e sob determinadas condições. Princípios de transparência, adequação e finalidade são essenciais para restringir tanto a generalidade na utilização dos dados quanto tratamentos opacos. Para reduzir a assimetria técnica e informacional, é exigido que sejam fornecidas informações claras, adequadas e em quantidade suficiente sobre os riscos e implicações do tratamento de dados.

No contexto do consentimento informado, o Art. 9º da LGPD estabelece que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que devem ser claras, adequadas e ostensivas sobre: a finalidade específica do tratamento (I); forma e duração do tratamento (II); identificação do controlador (III); informações de contato do controlador (IV); uso compartilhado de dados e a finalidade (V); responsabilidades dos agentes que realizarão o tratamento (VI); e direitos do titular, com menção explícita aos direitos do Art. 18 (VII).

O consentimento será nulo se as informações fornecidas ao titular forem enganosas ou abusivas ou não tiverem sido apresentadas previamente com transparência, clareza e de forma inequívoca. Mudanças na finalidade do tratamento dos dados, incompatíveis com o consentimento original, devem ser informadas previamente ao titular, que poderá revogar o consentimento se discordar.

A manifestação de vontade deve ser inequívoca, ou seja, clara e evidente. O consentimento do titular está no Art. 7º como a primeira possibilidade para a realização do tratamento de dados, sendo fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (Art. 8º). Não é necessário ser escrito, mas, se for, deve constar em cláusula destacada das demais cláusulas contratuais. O consentimento não pode ser extraído da omissão do titular, mas de atos positivos que revelem claramente sua vontade. O

controlador tem o ônus da prova de que o consentimento foi obtido conforme a Lei, observando o princípio da responsabilização e prestação de contas.

A finalidade da coleta dos dados deve ser conhecida previamente, independente da base legal utilizada. Essa diretriz está relacionada à utilização não abusiva e à recomendação de eliminar ou anonimizar informações que não sejam mais necessárias. A depender do tipo de informação, seria possível desmembrar o consentimento em categorias, com requisitos variáveis conforme a natureza dos interesses, seguindo a lógica do consentimento granular.

Na dispensa do consentimento, conforme Art. 7º, §4º, para dados "tornados manifestamente públicos pelo titular", os agentes de tratamento continuam obrigados a observar os direitos do titular e os princípios da Lei. No caso de dados de acesso público, é necessário considerar o contexto em que foram disponibilizados e a compatibilidade entre seu uso e as circunstâncias de sua divulgação. Mesmo dados públicos são pessoais e a finalidade de sua circulação deve ser considerada.

O tratamento posterior dos dados públicos (Art. 7º, §§ 3º e 4º) pode ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular. A distinção entre as hipóteses dos §§ 3º e 4º do Art. 7º é que, no § 4º, não há necessidade de uma nova base legal, enquanto no § 3º é necessário enquadramento em uma base legal autorizativa.

De forma geral, a dispensa do consentimento não desobriga os agentes de tratamento das demais obrigações previstas na Lei, especialmente a observância dos princípios gerais e a garantia dos direitos do titular (Art. 7º, §6º).

O consentimento está vinculado ao controlador para o qual foi dado. O controlador que necessitar comunicar ou compartilhar dados com outros controladores deve obter consentimento específico do titular, exceto nas hipóteses de dispensa previstas na Lei. Isso implica um dever que deve ser observado por todos que têm acesso aos dados, verificando a licitude do acesso ou compartilhamento, inclusive quanto ao consentimento específico

O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, de forma gratuita e facilitada. O consentimento é temporário, podendo ser revogado com base na autodeterminação em relação à esfera privada e proteção da personalidade. Entretanto, a revogação não deve causar prejuízo ao interesse público e, em caso de abuso, cabe a devida reparação.

Portanto, é muitas vezes mais vantajoso para as empresas terem uma base legal alternativa para legitimar o tratamento de dados, considerando a possibilidade de revogação do consentimento.

3. O MARCO CIVIL DA INTERNET E O DIREITO À PRIVACIDADE

Uma análise concisa da história da humanidade revela que o mundo está em contínua transformação. Silva e Siqueira (2019, p. 6) observam que o centro desta mudança é a influência crescente da tecnologia, especialmente no âmbito da comunicação e da informação. Com o avanço constante de novas tecnologias incorporadas ao cotidiano das pessoas (RODRIGUES et al., 2020, p. 1), a internet e as inovações tecnológicas tornaram-se partes essenciais da vida social, sendo até reconhecidas pela Organização das Nações Unidas como direitos humanos.

Essas tecnologias trouxeram novas oportunidades para a educação, saúde, pesquisas, trabalho e entretenimento, desde a troca de mensagens por aplicativos até negociações bilionárias. A internet exemplifica bem a grande revolução tecnológica atual, e, com isso, surgem questões jurídicas importantes que precisam ser debatidas e resolvidas.

Qualquer fator que possa impactar as relações jurídicas ou interpessoais e afetar a ordem e a paz social deve ser analisado para proteger os direitos essenciais para a convivência em sociedade. Considerando que o direito visa a pacificação social (SANTOS, 2004), é relevante considerar essas mudanças sob a perspectiva jurídica.

Assim como as normas do direito brasileiro se aplicam às relações interpessoais fora do ambiente digital, é fundamental que esses princípios também sejam observados online. Por isso, foi criada a Lei 12.965/2014, conhecida como Marco Civil da Internet, com o propósito de regular as relações originadas no ambiente virtual.

A aprovação dessa lei foi considerada uma grande vitória, especialmente diante dos interesses econômicos que seriam afetados e da complexidade dos temas abordados, o que complicou sua elaboração e aprovação. Contudo, em 23 de abril de 2014, o Marco Civil da Internet foi publicado e trouxe mudanças significativas na forma como as relações jurídicas são conduzidas no ambiente virtual (TEFFÉ; MORAES, 2017, p. 111).

O objetivo da lei era estabelecer um marco que respeitasse os direitos humanos e se adaptasse à natureza dinâmica da internet. Antes do Marco Civil da Internet, as decisões judiciais sobre questões virtuais eram confusas e variadas. Com a lei, tornou-se possível obter

decisões mais consistentes, baseadas em normas infraconstitucionais (TEFFÉ; MORAES, 2017, p. 111).

O Marco Civil da Internet cumpre bem seu papel ao estabelecer que o uso da internet deve seguir os princípios previstos na lei, que estão amplamente alinhados com os da Constituição Federal de 1988. Entre esses princípios está o direito à privacidade, garantido pelo artigo 5º, inciso X da Constituição, junto com outros direitos da personalidade, sendo considerados direitos invioláveis: "são invioláveis a intimidade, a vida privada, a honra e imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Fragoso (2019) observa que o conceito de privacidade que se busca proteger atualmente vai além do definido constitucionalmente, apoiado por um legado de políticas e um processo contínuo de regulamentação da vida social. A privacidade deve ser ajustada às mudanças nas relações sociais e às formas de comunicação, especialmente com o acesso à internet e as desigualdades na proteção da privacidade.

O Marco Civil da Internet aborda questões de privacidade que antes não eram devidamente tratadas ou eram contraditórias. As inovações trazidas pela lei incluem a definição clara de regimes de acesso e uso de dados cadastrais.

A Lei 12.965/2014 também inclui disposições sobre a proteção de registros, dados pessoais e comunicações privadas, no Capítulo III, Seção II. O artigo 10 exige a preservação da intimidade, vida privada, honra e imagem das pessoas envolvidas no tratamento de registros de conexão e acesso a aplicações de internet.

Entre as disposições voltadas à proteção da privacidade, o artigo 15 da Lei 12.965/2014 estipula um prazo de seis meses para que provedores de internet, na forma de pessoa física e remunerada, mantenham registros de conexão dos usuários.

O artigo 7º da lei especifica as proibições contra violações dos direitos e garantias dos usuários da internet, algo que a Constituição trata de forma mais geral. Além disso, estabelece regras detalhadas para a violação excepcional dessas informações, sempre com autorização judicial e de acordo com a lei, conforme o parágrafo 2º do artigo 10 da Lei 12.965/2014.

A lei assume que existem várias ameaças à privacidade dos usuários, incluindo a possibilidade de violação pelo Estado. Portanto, cria mecanismos de proteção da privacidade contra todos, inclusive o Estado. Fragoso (2019) menciona que os dados pessoais são extremamente valiosos para empresas em diversos setores:

Há exemplos abundantes: privatização de bases de dados públicas, denúncias de tratamento de dados para geo-blocking e geo-pricing – bloqueio de ofertas e precificação desigual conforme localização – e coleta de dados para análise de perfis de navegação com fins de marketing digital.

A sociedade atual vive um momento complexo, com a democracia comunicacional permitindo grande capacidade de envio e recebimento de informações. No entanto, também existem riscos, desde o vazamento de dados pessoais sem autorização até a falta de verificação da veracidade das informações compartilhadas (BARRETO JÚNIOR; SAMPAIO, 2018, p. 116).

Qualquer pessoa com um celular e acesso à internet pode publicar informações na web, e essas informações frequentemente são compartilhadas sem consideração pela veracidade ou pelo potencial ofensivo do conteúdo.

Portanto, no que diz respeito ao direito à privacidade, o Marco Civil da Internet representa um grande avanço ao estabelecer regras e princípios para proteger esse direito fundamental na sociedade digital.

Embora haja questionamentos sobre a efetividade das normas da Lei 12.965/2014, por serem consideradas bastante principiológicas e com aplicabilidade prática limitada, diversos processos estão em andamento para concretizar os direitos previstos no Marco Civil da Internet.

A necessidade de limitar outros direitos – como a liberdade de expressão quando usada para prejudicar outros direitos da personalidade – e de criar regras para o uso da internet são tão essenciais no mundo virtual quanto fora dele. Como Santos e Silva (2020, p. 41) destacam, "a escolha pela democracia impõe ônus, o que é fundamental para um convívio pacífico e harmônico em sociedade", indicando que viver em um Estado Democrático de Direito envolve muitas responsabilidades.

4. USO DO INTERESSE LEGÍTIMO

O interesse legítimo é uma base legal que permite o tratamento de dados importantes, relacionados às atividades do controlador, quando há uma justificativa válida. Devido à flexibilidade desta base, as expectativas do titular dos dados têm um peso especialmente significativo para sua aplicação. A finalidade, a necessidade e a proporcionalidade do uso dos dados devem ser consideradas. Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que o interesse legítimo seja reconhecido.

Aqui estão incluídos tratamentos em que obter o consentimento do titular poderia dificultar o uso regular dos dados, atendendo a interesses legítimos do controlador ou de terceiros, ou quando outras bases legais não são adequadas, especialmente no contexto da Internet das Coisas e Big Data. Muitas vezes, pode não ser necessário obter novo consentimento para usos implícitos dentro de uma relação já estabelecida. Além disso, quando o interesse é de terceiros, essa base pode ser aplicada em situações em que não é possível obter tal autorização ou quando essa interação inviabilizaria o tratamento dos dados.

Para demonstrar que há um interesse legítimo, o controlador (ou um terceiro) deve ter um benefício ou resultado específico em mente. Não basta alegar interesses comerciais vagos ou genéricos. É necessário pensar detalhadamente no que se busca alcançar com o tratamento de dados. Embora um objetivo possa ser potencialmente relevante, ele deve ser considerado "legítimo". Qualquer interesse ilegítimo, antiético ou ilegal não será reconhecido como legítimo pela LGPD.

Alguns exemplos de aplicação do interesse legítimo incluem: a) tratamento de dados pessoais estritamente necessários para prevenir e controlar fraudes ou garantir a segurança da rede e das informações em sistemas informáticos; b) fornecimento de imagens de câmeras de segurança para fins de seguro; c) segurança e melhoria de produtos e serviços; d) tratamento de dados de empregados para programas de retenção de talentos e iniciativas de bem-estar; e) uso de dados por uma empresa para fazer ofertas mais personalizadas a seus clientes, utilizando apenas os dados estritamente necessários; f) envio de e-mails com descontos específicos para produtos procurados por um usuário com base em seu histórico de compras; g) notificação a um usuário sobre itens deixados no carrinho online sem finalizar a compra; h) coleta de informações sobre um candidato em processos seletivos. Como o conceito está em desenvolvimento, caberá principalmente à Autoridade Nacional de Proteção de Dados (ANPD) e ao Poder Judiciário interpretá-lo em casos específicos.

A LGPD não permite o uso do interesse legítimo para o tratamento de dados sensíveis, devendo essas atividades serem enquadradas em outras bases legais previstas no art. 11 da lei, que inclui o tratamento para prevenção de fraudes e segurança do titular, processos de identificação e autenticação em sistemas eletrônicos, e o exercício regular de direitos contratuais.

Para dar maior clareza a esse requisito, tanto a LGPD quanto a experiência internacional, especialmente a europeia, sugerem alguns parâmetros interpretativos. O antigo Grupo de

Trabalho do Artigo 29, que influenciou o GDPR, propôs o uso do teste de Interesse Legítimo (Legitimate Interest Assessment - LIA) ou teste de ponderação. O objetivo é equilibrar os direitos do titular dos dados com os interesses de quem usa essas informações, verificando tanto o interesse legítimo do controlador quanto o respeito às expectativas e direitos fundamentais dos titulares.

O teste de Interesse Legítimo possui quatro fases: (i) avaliação dos interesses legítimos; (ii) impacto sobre o titular dos dados; (iii) equilíbrio entre os interesses do controlador e o impacto sobre o titular; e (iv) medidas de proteção para o titular dos dados e prevenção de impactos indesejados. A LGPD também estabelece parâmetros exemplificativos para a utilização do interesse legítimo como base para o tratamento de dados sem consentimento, conforme o artigo 10:

> Art. 10. O interesse legítimo do controlador pode fundamentar o tratamento de dados pessoais para finalidades legítimas, considerando situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção das atividades do controlador; e
> II - proteção dos direitos do titular ou prestação de serviços que o beneficiem, respeitando suas expectativas legítimas e direitos fundamentais, de acordo com esta Lei.
> § 1º Quando o tratamento se basear no interesse legítimo do controlador, apenas os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deve adotar medidas para garantir a transparência do tratamento de dados baseado no interesse legítimo.
> § 3º A autoridade nacional pode solicitar ao controlador um relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento o interesse legítimo, respeitando os segredos comercial e industrial.

Os artigos da LGPD que tratam dos interesses legítimos (arts. 7º, IX, e 10) permitem aplicar parte do teste mencionado para avaliar a existência de interesse legítimo em casos específicos. O Art. 10 exige a avaliação de uma finalidade legítima e uma situação concreta. Segundo Bioni, o primeiro passo é verificar se o interesse do controlador é legítimo (finalidade legítima) e se não contraria outras normas legais. Deve-se observar se há algum benefício com o uso dos dados. Em seguida, avalia-se se o interesse está claramente definido para evitar o uso genérico dos dados e se há uma situação concreta que o suporte.

O §1º do Art. 10 introduz o princípio da necessidade/minimização, verificando se os dados coletados são realmente necessários para a finalidade pretendida e se o tratamento poderia ser coberto por outras bases legais da LGPD.

No inciso II do art. 10, é mencionado o balanceamento de interesses, considerando a legítima expectativa do titular dos dados e seus direitos e liberdades. Essa é a principal fase do

teste de proporcionalidade, onde se compara os interesses do controlador e de terceiros com os do titular dos dados. Avalia-se se o uso adicional dos dados está dentro das expectativas do titular e se o impacto sobre ele é razoável.

Além disso, deve-se verificar como os titulares serão impactados, principalmente se poderão sofrer discriminação. Se o interesse for de terceiros, como alguém sem uma relação pré-estabelecida com o titular, a dificuldade em demonstrar a expectativa legítima é maior.

Finalmente, os §§2º e 3º do art. 10 estabelecem exigências como transparência e mecanismos de oposição (opt-out), e medidas para mitigar riscos aos titulares dos dados, como a pseudonimização. Esse requisito legitima o tratamento de dados pessoais apenas na medida necessária para a finalidade proposta e o agente de tratamento deve manter registros das operações realizadas, especialmente quando baseado no interesse legítimo. Recomenda-se elaborar um relatório de impacto para minimizar riscos.

Leonardi destaca que o teste deve ser documentado, conforme o §3º do art. 10, já que o relatório pode ser solicitado pela ANPD, devendo ser preparado no momento da decisão de utilizar o interesse legítimo e antes do tratamento. No art. 38 da lei, o legislador não exige a elaboração prévia do relatório: "A autoridade nacional pode exigir ao controlador a elaboração de relatório de impacto à proteção de dados pessoais, incluindo dados sensíveis, para suas operações de tratamento, conforme regulamento e respeitados os segredos comercial e industrial".

É importante destacar que uma aplicação adequada e estratégica do interesse legítimo pode gerar novos modelos de negócios e estratégias comerciais e de segurança, exigindo um equilíbrio entre o interesse legítimo e as expectativas e direitos dos titulares.

De acordo com o art. 7º, IX, os interesses legítimos podem ser do controlador ou de terceiros, englobando "interesses comerciais, individuais ou mesmo interesses da coletividade e da sociedade". O art. 10 da LGPD menciona apenas o controlador, e a doutrina e a ANPD devem esclarecer se sua interpretação pode ser ampliada. O termo "terceiro" pode incluir não apenas outras organizações, mas também indivíduos não diretamente envolvidos ou o público em geral.

Um exemplo é uma companhia de seguros que deseja processar dados pessoais para identificar fraudes. O interesse legítimo é garantir que seus clientes não realizem fraudes contra ela. Clientes e o público também têm interesse em evitar e detectar fraudes. Outro exemplo é uma empresa financeira que não consegue localizar um cliente que parou de pagar uma dívida.

A empresa quer contratar uma agência de cobrança para encontrar o cliente e recuperar a dívida. O interesse legítimo da empresa é recuperar a dívida, e é razoável que os clientes esperem que medidas sejam tomadas para cobrar dívidas pendentes, mesmo que os interesses possam ser opostos.

Assim, pode-se concluir que: a) o interesse legítimo pode ser a base mais adequada em diversas situações, se aplicado de forma proporcional e limitada, com benefícios claros para o controlador e/ou terceiros; b) deve ser aplicado quando não tiver um impacto elevado nos direitos do indivíduo; c) o titular dos dados deve esperar razoavelmente que seus dados sejam usados dessa forma; e d) pode ser aplicado quando não for possível ou desejável dar total controle ao titular dos dados ou quando o controlador não quiser incomodá-lo com solicitações de consentimento para tratamentos que provavelmente seriam aceitos.

5. OUTRAS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

O artigo 7º da LGPD apresenta diversas justificativas legais para o tratamento de dados pessoais, sem que haja uma base superior às demais, como mencionado em tópico específico (item 2). Embora seja possível utilizar múltiplas bases legais para um determinado tratamento, é necessário escolher a base mais apropriada e segura para cada situação específica.

Após a discussão sobre o consentimento, a lei afirma que o tratamento de dados pessoais pode ocorrer para cumprir uma obrigação legal ou regulatória pelo controlador, como nas obrigações trabalhistas, deveres relacionados à lei anticorrupção e a manutenção de registros por certos provedores conforme o Marco Civil da Internet. Outro exemplo inclui empresas do setor de seguros ou financeiro, que estão sujeitas a várias regras legais e regulatórias e podem necessitar tratar dados pessoais de seus clientes para cumprir tais obrigações. Uma política de privacidade bem estruturada e transparente pode esclarecer o uso dessa base legal pela organização.

A seguir, o tratamento de dados pessoais pela administração pública é abordado, abrangendo o tratamento e compartilhamento de dados necessários para a execução de políticas públicas conforme previsto em leis, regulamentos, contratos, convênios ou instrumentos similares, respeitando as disposições do Capítulo IV da lei, que regula o tratamento de dados pessoais pelo Poder Público. Essas políticas podem incluir a implementação de saneamento básico, assistência a cidadãos vulneráveis ou projetos educacionais para crianças e adolescentes.

A execução de políticas públicas é uma justificativa para que o setor público trate dados. Esse requisito está relacionado ao artigo 23 da LGPD, que estabelece que o tratamento de dados pessoais por entidades públicas deve ocorrer para atender à sua finalidade pública, visando o interesse coletivo e a execução das funções legais ou atribuições do serviço público, desde que:

> a) sejam informadas as situações em que, ao exercer suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e práticas utilizadas, preferencialmente em seus sites oficiais; e b) seja designado um encarregado quando houver operações de tratamento de dados pessoais. A previsão no art. 23 sugere requisitos adicionais para o tratamento de dados pela Administração Pública, já que, como destacado no item 1, entendemos que a base legal para o tratamento de dados pessoais pela Administração Pública na execução de suas funções legais ou no cumprimento das atribuições do serviço público é o cumprimento de uma obrigação legal ou a execução de políticas públicas, conforme os artigos 7º e 11 da LGPD.

Dados podem também ser tratados para a realização de estudos por órgãos de pesquisa, sempre que possível garantindo a anonimização dos dados pessoais. O Art. 5º, XVIII, da lei define órgão de pesquisa como "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, cuja missão institucional ou objetivo social ou estatutário inclua a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico". Em relação à anonimização, que é a utilização de técnicas razoáveis e disponíveis para impedir a identificação de um indivíduo, a Lei considera essa prática mais protetiva para os titulares, pois um dado anonimizado não pode ser associado a uma pessoa específica, tornando-se não pessoal, conforme o art. 12 da LGPD. Um exemplo é quando dados de intenção de voto em uma eleição são agrupados por sexo, escolaridade, região e classe social de forma agregada, tornando impossível identificar os indivíduos que expressaram essas intenções. A instituição deve garantir a segurança e anonimização desses dados nos bancos de dados.

A Lei também permite, conforme o art. 13, que órgãos de pesquisa em saúde pública acessem bases de dados pessoais, desde que o tratamento ocorra exclusivamente dentro do órgão e para fins de estudo e pesquisa, mantidos em ambiente seguro, conforme regulamentações específicas e sempre que possível com anonimização ou pseudonimização dos dados, respeitando os padrões éticos. A divulgação dos resultados ou qualquer parte do estudo não pode revelar dados pessoais. O órgão de pesquisa é responsável pela segurança das informações e não pode transferir dados a terceiros. O acesso aos dados será regulamentado pela autoridade nacional e pelas autoridades de saúde.

Outra base autorizativa para o tratamento de dados é quando necessário para a execução de contrato ou procedimentos preliminares relacionados ao contrato do qual o titular é parte, a pedido do titular dos dados. Essa disposição é mais ampla do que a prevista no art. 11, II, "d", da LGPD, permitindo que dados necessários para a contratação sejam tratados sem consentimento, desde que o titular esteja envolvido ou em negociações para um contrato. Exemplos incluem:

> a) a aquisição de produtos ou serviços, que exige o conhecimento de dados de contato do consumidor; e b) análises realizadas por instituições financeiras antes da concessão de crédito. No setor de seguros, essa base é importante para realizar análises preliminares e cumprir o contrato, como na regulação de sinistros e fornecimento de assistência

Essa base se assemelha ao tratamento de dados via consentimento, mas a principal diferença é que o titular dos dados não pode revogar a qualquer momento, pois a outra parte está protegida pela LGPD para manter os dados enquanto o contrato estiver em vigor. O Regulamento europeu de proteção de dados, em seu art. 6º, estabelece que o tratamento é lícito se necessário para a execução de um contrato do qual o titular seja parte ou para diligências pré-contratuais a pedido do titular. Essa base legal diferencia "consentimento" para entrar em um contrato e "consentimento" para o tratamento dos dados pessoais.

O tratamento também pode ser baseado no exercício regular de direitos em processos judiciais, administrativos ou arbitrais (nos termos da Lei nº 9.307/96). Essa base legal ampla autoriza o uso de dados pessoais em processos para assegurar o direito de produzir provas. O exercício regular de direitos inclui ações autorizadas por lei e deve ser realizado de forma não abusiva. A doutrina afirma que dados podem ser armazenados se forem necessários para o exercício de direitos em demandas, protegendo a ampla defesa e o contraditório.

Outras possibilidades incluem a proteção da vida ou integridade física do titular ou de terceiros. Essa base é aplicável em situações excepcionais e não deve justificar ações genéricas. Exemplos incluem a obtenção de dados de geolocalização para encontrar pessoas desaparecidas em desastres ou epidemias, como no caso do COVID-19.

Finalmente, a lei permite o tratamento de dados para a proteção da saúde exclusivamente por profissionais de saúde, serviços de saúde ou autoridades sanitárias. A lei estabelece algumas questões: quem são os profissionais de saúde e quais serviços são considerados de saúde? Por exemplo, um plano de saúde pode utilizar essa base legal de forma ampla? Quais riscos isso implica? A proteção da saúde deve ser direcionada especificamente à pessoa a quem os dados pertencem ou pode envolver um grupo? A base deve ser utilizada com cautela para evitar a inferência de situações sensíveis e garantir que não haja discriminação ilegítima ou abusiva

(Art. 6º, IX). Em relação à autoridade sanitária, a Lei nº 9.782/99 define o Sistema Nacional de Vigilância Sanitária e a Agência Nacional de Vigilância Sanitária.

Como penúltima base, a Lei permite o tratamento de dados quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto quando prevalecerem os direitos e liberdades fundamentais do titular que exijam proteção dos dados pessoais, conforme tratado no item 3 deste artigo.

Por fim, a última base legal para o tratamento de dados [não sensíveis] refere-se à proteção do crédito. Espera-se que essa base legal facilite a concessão de crédito, melhore as análises de risco e impulsione o mercado de consumo. A base deve estar alinhada com normas como o Código de Defesa do Consumidor (Lei nº 8.078/90), a lei do cadastro positivo (Lei nº 12.414/11) e portarias do Ministério da Justiça.

A informação e transparência são direitos básicos do consumidor, que deve ter acesso claro a todos os aspectos da relação contratual e ao tratamento de seus dados. Como mencionado no Recurso Especial nº 1.348.532, a exposição de dados financeiros pode levar a diversas intrusões na vida do consumidor: "Conhecem-se seus hábitos, monitoram-se sua forma de viver e despesas".

O tema relacionado à base legal acima inclui o credit scoring, um sistema de pontuação utilizado por instituições para auxiliar na concessão de crédito. Essa pontuação considera variáveis como idade, sexo, estado civil, profissão, renda e histórico de crédito. O STJ considerou essa prática lícita, conforme o art. 5º, IV, e o art. 7º, I, da Lei nº 12.414/11. No entanto, o Recurso Especial nº 1.419.697 estabeleceu que a avaliação de risco deve respeitar os limites de proteção ao consumidor, como disposto no CDC e na Lei 12.414/11. No sistema de scoring, mesmo sem o consentimento do consumidor, devem ser fornecidos esclarecimentos sobre as fontes de dados utilizados.

A lei do cadastro positivo proíbe anotações excessivas, ou seja, informações não relacionadas à análise de risco de crédito, e informações sensíveis, como origem social e étnica, saúde, informação genética, orientação sexual e convicções políticas, religiosas e filosóficas (Art. 3º, §3º). A proibição do uso de dados sensíveis visa evitar discriminação e garantir a privacidade do consumidor. O STJ, no REsp 1.419.697, determinou que não se devem considerar informações sensíveis, excessivas, sem relação com o crédito ou sem consentimento do titular.

6. TRATAMENTO DE DADOS SENSÍVEIS

Os dados pessoais classificados como sensíveis estão presentes em todos os registros informacionais do indivíduo. Na Lei Geral de Proteção de Dados (LGPD) — assim como no Regulamento Geral sobre a Proteção de Dados (GDPR) —, o legislador determinou que a melhor maneira de protegê-los era listar exemplos claros desses dados. Portanto, conforme o art. 5º, inciso II, da LGPD, dados sensíveis incluem informações sobre origem racial ou étnica, crenças religiosas, opiniões políticas e afiliações a sindicatos ou organizações de caráter religioso, filosófico ou político. Também são considerados sensíveis os dados relacionados à saúde ou à vida sexual, bem como dados genéticos ou biométricos.

Esses dados são especialmente críticos do ponto de vista dos direitos e liberdades fundamentais, pois seu tratamento pode expor o titular a riscos significativos. Eles compõem o núcleo essencial da privacidade, uma vez que a natureza das informações pode levar à discriminação do titular, exigindo, portanto, uma proteção mais rigorosa.

Quanto a essa especificação, é pertinente questionar: ao lidar com informações pessoais, não seria mais adequado utilizar uma lista exemplificativa de dados sensíveis? Dada a variedade de usos e combinações possíveis de dados pessoais, há algum dado que não possa ser considerado sensível? Todos os dados classificados como sensíveis pelo legislador estão na mesma esfera íntima do titular? Em que medida a criação de novas categorias de dados beneficiaria os indivíduos?

Entende-se que é crucial avaliar o contexto em que um dado é utilizado para determinar sua sensibilidade, além das relações que podem ser estabelecidas com outras informações disponíveis e a possibilidade de que seu tratamento sirva para estigmatizar ou discriminar o titular. Como a doutrina destaca: "(...), deve-se considerar que certos dados, mesmo que não possuam inicialmente essa natureza especial, podem ser classificados como sensíveis dependendo do uso que se faz deles."

A LGPD estabelece que o tratamento de dados pessoais sensíveis só pode ocorrer nas seguintes situações:

> I - quando o titular ou seu responsável legal fornecer consentimento específico e destacado para fins determinados; ou
>
> II - na ausência de consentimento do titular, nas situações indispensáveis expressas nas alíneas deste artigo:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;

> b) tratamento compartilhado de dados necessários à execução de políticas públicas pela administração pública, conforme leis ou regulamentos;
>
> c) realização de estudos por órgãos de pesquisa, garantindo, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, incluindo em contratos e processos judiciais, administrativos e arbitrais, conforme a Lei de Arbitragem;
>
> e) proteção da vida ou integridade física do titular ou de terceiros;
>
> f) tutela da saúde, exclusivamente em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias; ou
>
> g) garantia da prevenção de fraudes e segurança do titular, em processos de identificação e autenticação em sistemas eletrônicos, respeitados os direitos previstos no art. 9º desta Lei e exceto quando prevalecerem direitos e liberdades fundamentais do titular que exijam proteção adicional.

Nestes casos, todos os cuidados para o tratamento dos dados devem ser intensificados, já que a proteção dos dados sensíveis requer um padrão ainda mais rigoroso.

O Art. 11 da LGPD mantém várias das bases já previstas no art. 7º para o tratamento de dados pessoais, excluindo as hipóteses de atendimento aos interesses legítimos do controlador ou de terceiros (Art. 7º, IX) e proteção do crédito (Art. 7º, X). Em substituição à hipótese de interesse legítimo, o Art. 11, II, "g", introduziu uma base mais específica voltada para a prevenção de fraudes e segurança do titular, vinculada aos interesses dos titulares e de certas entidades. Um exemplo de aplicação é o seguinte: instituições bancárias e empregadores podem tratar dados biométricos para prevenir fraudes, sem o consentimento prévio dos titulares, para confirmar que é o empregado autorizado que está acessando uma área restrita da empresa ou que é o cliente autorizado realizando uma transação bancária em um caixa eletrônico.

Além disso, a norma adicionou a possibilidade de exercício regular de direitos também em relação a um contrato (Art. 11, II, "d"), mas não replicou a disposição do Art. 7º, V. Por exemplo, um seguro de saúde ou seguro de vida pode precisar coletar dados sensíveis para o exercício regular de direitos, pois sem esse tratamento, pode não ser possível cumprir com a prestação contratual, como o ressarcimento de despesas médicas ou o pagamento de indenização por invalidez. Nesse caso, a seguradora não teria apenas o dever de cumprir a obrigação contratual, mas também o direito de fazê-lo. De forma similar, a doutrina europeia no GDPR reconhece a possibilidade de uma seguradora tratar dados de saúde para verificar a regularidade de uma reclamação de indenização decorrente de um sinistro de seguros de pessoas.

Voltando às situações autorizativas para o tratamento de dados sensíveis, a primeira (Art. 11, I) diz respeito ao consentimento do titular ou de seu responsável legal, que deve ser fornecido de forma específica e destacada para fins determinados. A Lei oferece uma camada

adicional de proteção para que esses dados não sejam usados contra seus titulares, o que poderia causar restrições a bens e serviços ou ao exercício de direitos. Parte da doutrina vê nesse dispositivo uma preferência legal por essa hipótese, com base na técnica legislativa, que insere dois incisos no art. 11: um sobre o consentimento e outro permitindo o tratamento de dados sensíveis sem consentimento apenas nas situações indispensáveis listadas nas alíneas. Essa interpretação é criticada na doutrina, que observa que a técnica legislativa utilizada implica uma posição de igualdade entre as hipóteses e não a prevalência do consentimento.

Um dos desafios é entender o conceito de consentimento como específico e destacado. De acordo com a doutrina, deve-se "considerá-lo como um vetor para maior assertividade do titular com relação a esses 'movimentos específicos' de seus dados". Essa noção se aproxima da ideia de consentimento expresso, exigindo maior envolvimento do titular e cuidados mais rigorosos no tratamento da informação.

Específico deve ser entendido como um consentimento dado para propósitos concretos e claramente definidos pelo controlador antes do tratamento dos dados, com ênfase nas obrigações de granularidade. Destacado pode ser interpretado como a necessidade de que o titular tenha pleno acesso ao documento que apresenta todos os aspectos relevantes do tratamento, com as disposições claramente destacadas para assegurar que o consentimento seja igualmente destacado. A manifestação de vontade deve estar claramente indicada no documento que autoriza o tratamento.

Segundo a LGPD, a proteção do Art. 11 se aplica a qualquer tratamento de dados pessoais que revele dados sensíveis e possa causar danos ao titular, salvo disposições em legislação específica. Mesmo dados que não sejam inicialmente sensíveis podem se tornar sensíveis em determinados contextos, revelando informações sensíveis sobre os titulares. Um exemplo frequentemente citado é a análise do histórico de compras em supermercados ou farmácias, ou o acesso à fatura do principal cartão de crédito, que pode revelar dados sensíveis como crenças religiosas, estado de saúde ou orientação sexual.

Em relação à COVID-19, a discussão sobre o uso de dados pessoais e sistemas de vigilância para combater o vírus ganhou relevância. Até que ponto o interesse coletivo pode sobrepor o individual? Quais mecanismos de rastreamento e coleta de dados serão implementados e por quanto tempo? Quem terá acesso aos bancos de dados criados? Esses dados serão eventualmente descartados? O que é justificável em uma pandemia global e qual legado isso deixará para a proteção de dados? Essas perguntas permanecem sem respostas claras.

Stefano Rodotà, em "A Vida na Sociedade da Vigilância: a Privacidade Hoje", destaca que a proteção especial dos dados de saúde não se justifica apenas pela sua natureza íntima, mas também pelo risco de discriminação que seu conhecimento pode provocar. O acesso a informações sobre indivíduos infectados, sem salvaguardas adequadas, pode levar a discriminações e prejudicar contratações. Dados de geolocalização, inicialmente não sensíveis, podem ser manipulados para usos prejudiciais e para verificar informações íntimas.

Medidas emergenciais, proporcionais e justificadas, que restrinjam a liberdade individual para garantir a saúde pública podem ser necessárias atualmente. Contudo, os agentes que tratam informações pessoais devem atuar dentro dos limites legais, evitando medidas arbitrárias que ultrapassem a proporcionalidade na restrição de direitos individuais.

O Art. 11 da LGPD também prevê que a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica pode ser proibido ou regulamentado pela Autoridade Nacional, ouvidos os órgãos setoriais do Poder Público.

A Lei proíbe a comunicação ou o uso compartilhado de dados sensíveis de forma a garantir a proteção do titular, exceto em situações como prevenção de fraude ou proteção da vida, estabelecendo regras claras e rigorosas para garantir que o tratamento dos dados seja feito com o devido cuidado e respeito aos direitos dos titulares.

Essa abordagem se alinha com as diretrizes internacionais e a necessidade de adaptação das normas às mudanças tecnológicas e desafios contemporâneos, equilibrando o direito à privacidade com as exigências de proteção da saúde pública.

7- CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados (LGPD) representa um avanço significativo na abordagem da privacidade e proteção de dados pessoais no Brasil. Inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece um modelo preventivo e abrangente para a proteção de dados, reconhecendo a importância da privacidade na era digital. A nova legislação introduz uma abordagem rigorosa e detalhada para a proteção de dados, reconhecendo que todos os dados pessoais possuem valor intrínseco, representando aspectos essenciais da identidade dos indivíduos.

Os principais pilares da LGPD incluem um conceito expansivo de dado pessoal, abrangendo qualquer informação que possa identificar ou tornar identificável uma pessoa. Esse

conceito não se limita a informações diretamente identificáveis, mas também inclui dados que, quando combinados, podem levar à identificação do titular. A legislação exige que qualquer tratamento de dados pessoais tenha uma base legal clara e define um rol taxativo de hipóteses legais que justificam tal tratamento, limitando as exceções e garantindo maior transparência no uso dos dados.

Um aspecto fundamental da LGPD é a detalhada caracterização do consentimento do titular. A lei estabelece que o consentimento deve ser informado, explícito e específico para finalidades determinadas, garantindo que o titular compreenda claramente o propósito e as implicações do tratamento de seus dados. Essa exigência visa assegurar que a manifestação de vontade do titular seja autêntica e não resultante de pressões ou falta de informação.

A LGPD também reconhece o legítimo interesse como uma das bases para o tratamento de dados, com a condição de que um teste de balanceamento de interesses seja realizado. Esse teste é essencial para garantir que o tratamento de dados com base no legítimo interesse não infrinja os direitos e liberdades fundamentais dos titulares. A necessidade de um equilíbrio entre os interesses do controlador e os direitos dos titulares é uma característica distintiva da LGPD, que visa prevenir abusos e garantir a proteção adequada dos dados.

O rol de direitos do titular é um dos aspectos mais abrangentes da LGPD. A lei concede aos titulares uma gama de direitos, incluindo acesso, correção, exclusão e portabilidade dos dados. Esses direitos permitem que os indivíduos mantenham o controle sobre suas informações pessoais e exijam transparência nas práticas de tratamento de dados. A legislação também estabelece uma série de obrigações para os agentes de tratamento, que devem adotar medidas adequadas para proteger os dados e garantir sua segurança.

A carga principiológica da LGPD é outra característica marcante. A lei está fundamentada em princípios sólidos que orientam todas as práticas de tratamento de dados, como a finalidade, a necessidade, a transparência e a segurança. Esses princípios são fundamentais para garantir que o tratamento de dados seja realizado de maneira ética e responsável, promovendo uma cultura de respeito à privacidade.

Para alcançar seus objetivos, a LGPD implementa mecanismos que facilitam o controle sobre os dados tratados e impõem deveres aos agentes de tratamento. Isso inclui a obrigação de implementar medidas técnicas e organizacionais para proteger os dados e a exigência de notificação em caso de incidentes de segurança. A lei visa antecipar e mitigar os riscos de violação da privacidade, promovendo uma abordagem proativa em relação à proteção de dados.

Finalmente, a LGPD busca evitar tratamentos abusivos e vazamentos de dados, estabelecendo um regime rigoroso de responsabilidade e penalidades. As sanções previstas na lei são projetadas para assegurar que os agentes de tratamento cumpram com suas obrigações e ajam de acordo com as normas estabelecidas. A legislação, portanto, não apenas fornece uma estrutura para a proteção de dados, mas também estabelece um sistema de supervisão para garantir sua efetiva implementação.

Em suma, a LGPD representa um passo crucial na evolução das normas de proteção de dados no Brasil, promovendo uma abordagem equilibrada e moderna para enfrentar os desafios da privacidade na era digital. A implementação efetiva da LGPD exige comprometimento contínuo dos agentes de tratamento e da Autoridade Nacional de Proteção de Dados, garantindo que os direitos dos titulares sejam sempre protegidos e respeitados.

REFERENCIAS

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 197.

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 232.

BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 377.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019, p. 460 e ss.

LEONARDI, Marcel. Legítimo interesse. Revista do Advogado, v. 39, 2019, p. 70.

LIMA, Caio César C. Seção I - Dos Requisitos para o Tratamento de Dados Pessoais. MALDONADO, Viviane Nóbrega; BLUM, Renato (Coord.). LGPD Lei Geral De Proteção De Dados. Revista dos Tribunais, 2019, p. 184.

MENDES, Laura Schertel; DONEDA, Danilo. "Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil". Revista de Direito do Consumidor, v. 120, p. 555, 2018.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei geral de Proteção de Dados Pessoais. Revista do Advogado, n. 144, nov. 2019, p. 47-53.

PEREIRA DE SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais. Direito Público, v. 16, n. 90, dez. 2019.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.106.

STJ. REsp 1.348.532 – SP. Rel. Min. Luis Felipe Salomão. DJe: 30/11/2017.

TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e de adolescentes. Revista do advogado, n. 144, nov. 2019, p. 54-59.

TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: proteção e consentimento. In: Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids online Brasil 2018. São Paulo: Comitê Gestor da Internet no Brasil, 2019. p.47-54.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: Ana Frazão, Gustavo Tepedino e Milena Donato Oliva (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019, p. 287-322.

VOIGT, Paul; BUSSCHE, Axel von dem. The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer, 2017, p. 101