

DIREITOS DA PERSONALIDADE E LEGÍTIMO INTERESSE NA PROTEÇÃO DE DADOS: A BASE LEGAL FLEXÍVEL COMPROMETE A TUTELA DA PERSONALIDADE NA ERA DIGITAL?

DERECHOS DE LA PERSONALIDAD E INTERÉS LEGÍTIMO EN LA PROTECCIÓN DE DATOS: ¿LA BASE JURÍDICA FLEXIBLE COMPROMETE LA TUTELA DE LA PERSONALIDAD EN LA ERA DIGITAL?

PERSONALITY RIGHTS AND LEGITIMATE INTEREST IN DATA PROTECTION: DOES THE FLEXIBLE LEGAL BASIS UNDERMINE THE PROTECTION OF PERSONALITY IN THE DIGITAL AGE?

Marcelo Negri Soares¹, Davi Albuquerque Geller de Oliveira², Laura Leal Carvalho³, Alender Max de Souza Moraes⁴

DOI: 10.54899/dcs.v22i85.3993

Recibido: 09/12/2025 | Aceptado: 12/12/2025 | Publicación en línea: 29/12/2025.

RESUMO

O artigo analisa criticamente a base legal do legítimo interesse no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e na Lei Geral de Proteção de Dados brasileira (LGPD), à luz dos direitos da personalidade. A problemática central é a seguinte: o legítimo interesse, como base legal flexível para o tratamento de dados pessoais, compromete a proteção adequada dos direitos da personalidade na era digital? Parte-se da compreensão de que a proteção de dados pessoais constitui desdobramento contemporâneo dos direitos da personalidade, especialmente da privacidade, intimidade, honra e identidade. Utiliza-se o método comparativo jurídico, com pesquisa bibliográfica e documental, examinando a configuração normativa do legítimo interesse, as orientações interpretativas das autoridades de proteção de dados e alguns exemplos práticos de aplicação. Sustenta-se que, embora o legítimo interesse seja funcionalmente necessário para viabilizar determinadas atividades econômicas e tecnológicas, sua natureza aberta e a assimetria informacional entre controladores e titulares geram riscos relevantes de esvaziamento da autodeterminação informacional e de violação de direitos da personalidade. Conclui-se que, na configuração atual, o legítimo interesse tende a comprometer a proteção efetiva dos direitos da personalidade, salvo se acompanhado de salvaguardas robustas, interpretação restritiva e fiscalização intensa pelas autoridades reguladoras.

Palavras-chave: Direitos da Personalidade. Proteção de Dados Pessoais. Legítimo Interesse. GDPR. LGPD.

¹ Doutor em Direito pela Pontifícia Universidade Católica de São Paulo (PUC - SP), Maringá, Paraná, Brasil. E-mail: negri@negrisoares.page Orcid: <https://orcid.org/0000-0002-0067-3163>

² Mestrando em Ciências Jurídicas pela UniCesumar, Maringá, Paraná, Brasil.

E-mail: davi.albuquerqueadv@outlook.com Orcid: <https://orcid.org/0009-0003-5722-7425>

³ Mestranda em Ciências Jurídicas pela UniCesumar, Maringá, Paraná, Brasil. E-mail: lauralealc1501@gmail.com Orcid: <https://orcid.org/0009-0009-9387-093X>

⁴ Doutorando em Ciências Jurídicas pela UniCesumar, Maringá, Paraná, Brasil. E-mail: alender@uems.br Orcid: <https://orcid.org/0000-0001-6501-8445>

ABSTRACT

This article critically analyses the legal basis of legitimate interest in the European Union General Data Protection Regulation (GDPR) and in the Brazilian General Data Protection Law (LGPD), in light of personality rights. The central research question is: does legitimate interest, as a flexible legal basis for the processing of personal data, undermine the adequate protection of personality rights in the digital age? Personal data protection is understood as a contemporary development of personality rights, especially privacy, intimacy, honour and identity. The article adopts the comparative legal method, with bibliographical and documentary research, examining the normative configuration of legitimate interest, interpretative guidelines issued by data protection authorities and some practical examples of application. It argues that, although legitimate interest is functionally necessary to enable certain economic and technological activities, its open-textured nature and the informational asymmetry between controllers and data subjects create significant risks of weakening informational self-determination and violating personality rights. The conclusion is that, in its current configuration, legitimate interest tends to compromise the effective protection of personality rights, unless accompanied by robust safeguards, restrictive interpretation and strong regulatory oversight.

Keywords: Personality Rights. Personal Data Protection. Legitimate Interest. GDPR. LGPD.

RESUMEN

El artículo analiza críticamente la base jurídica del interés legítimo en el Reglamento General de Protección de Datos de la Unión Europea (GDPR) y en la Ley General de Protección de Datos brasileña (LGPD), a la luz de los derechos de la personalidad. La cuestión central es la siguiente: ¿el interés legítimo, como base jurídica flexible para el tratamiento de datos personales, compromete la protección adecuada de los derechos de la personalidad en la era digital? Se parte de la idea de que la protección de datos personales constituye un desarrollo contemporáneo de los derechos de la personalidad, especialmente de la privacidad, la intimidad, el honor y la identidad. Se emplea el método comparado jurídico, con investigación bibliográfica y documental, examinando la configuración normativa del interés legítimo, las orientaciones interpretativas de las autoridades de protección de datos y algunos ejemplos prácticos de aplicación. Se sostiene que, aunque el interés legítimo sea funcionalmente necesario para viabilizar determinadas actividades económicas y tecnológicas, su carácter abierto y la asimetría informacional entre responsables y titulares generan riesgos relevantes de vaciamiento de la autodeterminación informativa y de violación de los derechos de la personalidad. Se concluye que, en la configuración actual, el interés legítimo tiende a comprometer la protección efectiva de los derechos de la personalidad, salvo si va acompañado de salvaguardas robustas, interpretación restrictiva y fiscalización intensa por parte de las autoridades reguladoras.

Palabras clave: Derechos de la Personalidad. Protección de Datos Personales. Interés Legítimo. GDPR. LGPD.



Esta obra está bajo una [Licencia Creative Commons Atribución- NoComercial 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUÇÃO

A centralidade dos dados pessoais na organização social, econômica e política da contemporaneidade alterou profundamente o modo como se compreendem e se protegem os direitos da personalidade. A vida cotidiana é mediada por tecnologias que coletam, armazenam, cruzam e exploram informações sobre indivíduos em escala massiva, muitas vezes em contextos pouco transparentes e sem conhecimento efetivo dos titulares. Smartphones, redes sociais, serviços de streaming, aplicativos de transporte, plataformas de comércio eletrônico, dispositivos de internet das coisas e sistemas de pagamento digital registram continuamente comportamentos, preferências, deslocamentos, relacionamentos, opiniões e características biométricas.

Cada interação digital deixa rastros informacionais que, agregados e processados por meio de algoritmos, permitem a construção de perfis individuais detalhados, capazes de antecipar escolhas, influenciar decisões e condicionar oportunidades.

Nesse cenário, a proteção de dados pessoais passou a ser compreendida como uma dimensão específica e indispensável da tutela da dignidade humana. A informação sobre a pessoa não é apenas reflexo passivo de sua existência, mas elemento ativo na construção de sua identidade social, na conformação de suas oportunidades econômicas e no exercício de suas liberdades fundamentais.

O tratamento massivo, automatizado e frequentemente opaco de dados pessoais implica riscos substanciais de violação da privacidade, discriminação algorítmica, manipulação comportamental, erosão da autonomia individual e comprometimento da própria dignidade da pessoa humana.

Os ordenamentos europeu e brasileiro estruturaram, em resposta a esse contexto, marcos normativos abrangentes: o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em vigor desde maio de 2018, e a Lei Geral de Proteção de Dados Pessoais (LGPD), vigente no Brasil desde setembro de 2020. Ambos adotam um modelo que condiciona a licitude do tratamento de dados à presença de uma base legal previamente estabelecida em lei, afastando a ideia de que a mera vontade das partes ou a disponibilidade técnica para coleta e processamento de informações seria suficiente para legitimar a circulação de dados pessoais.

Esse modelo, inspirado na tradição europeia de proteção de dados como direito fundamental, parte do pressuposto de que a personalidade humana, em sua projeção informacional, merece tutela qualificada e que o consentimento do titular, embora relevante, não

pode ser o único fundamento legitimador do tratamento.

Entre as bases legais previstas tanto no GDPR quanto na LGPD, destaca-se o legítimo interesse, que permite o tratamento de dados mesmo sem consentimento do titular, desde que atendidos determinados requisitos de legitimidade, necessidade e proporcionalidade. Essa base legal assume importância estratégica, pois viabiliza operações de tratamento essenciais para determinadas atividades econômicas, como a prevenção de fraudes, a segurança da informação, o marketing direto, a gestão de riscos empresariais e a prestação de serviços personalizados. A flexibilidade dessa hipótese, aliada à possibilidade de utilização em larga escala por agentes econômicos relevantes, especialmente grandes plataformas digitais, empresas de tecnologia, instituições financeiras e operadores de infraestruturas críticas, suscita questionamentos quanto à sua compatibilidade com a proteção efetiva dos direitos da personalidade.

O legítimo interesse, diferentemente das demais bases legais, não se apresenta como hipótese taxativa e objetiva, mas como cláusula geral que exige do controlador a realização de um juízo de ponderação entre o interesse perseguido e os direitos e liberdades fundamentais do titular. Essa abertura conceitual, ao mesmo tempo em que confere ao sistema a flexibilidade necessária para lidar com a diversidade e dinamismo das operações de tratamento de dados, pode gerar insegurança jurídica, risco de utilização abusiva e potencial esvaziamento da autodeterminação informacional dos titulares.

Em contextos marcados por forte assimetria informacional, concentração de poder econômico e tecnológico, baixa consciência social sobre direitos de proteção de dados e limitada capacidade institucional de fiscalização, o recurso amplo ao legítimo interesse pode traduzir-se em prevalência sistemática dos interesses empresariais sobre os direitos fundamentais dos indivíduos.

A discussão é particularmente sensível na medida em que se insere no debate mais amplo sobre os limites da monetização de dados pessoais, sobre a legitimidade dos modelos de negócio baseados em vigilância e perfilamento comportamental e sobre o papel do direito na contenção das dinâmicas de poder inerentes à economia digital. Questiona-se se o ordenamento jurídico, ao adotar uma base legal tão aberta quanto o legítimo interesse, não estaria, na prática, facilitando a instrumentalização da personalidade humana, permitindo que informações sobre indivíduos sejam apropriadas e exploradas economicamente sem controle efetivo, em contradição com os próprios fundamentos da proteção de dados como direito fundamental.

Surge, assim, a problemática que orienta este artigo: o legítimo interesse, como base legal

flexível para o tratamento de dados pessoais no GDPR e na LGPD, compromete a proteção adequada dos direitos da personalidade na era digital? Essa pergunta desdobra-se em outras questões conexas: em que medida a abertura conceitual do legítimo interesse permite usos expansivos que fragilizam a autodeterminação informacional? Os mecanismos de controle previstos nos ordenamentos europeu e brasileiro são suficientes para equilibrar os interesses em jogo? Existe compatibilidade estrutural entre uma base legal que dispensa o consentimento e a tutela reforçada da personalidade em sua dimensão informacional? As diferenças de contexto institucional entre Europa e Brasil impactam de forma relevante o funcionamento da base?

A investigação aborda essas questões por meio do método comparativo jurídico, examinando a disciplina do legítimo interesse no GDPR e na LGPD, bem como suas interações com a tutela da personalidade. A análise considera o texto normativo, a doutrina especializada nacional e estrangeira, documentos interpretativos de autoridades de proteção de dados — em especial do Comitê Europeu para a Proteção de Dados (CEPD) e da Autoridade Nacional de Proteção de Dados brasileira (ANPD) —, além de decisões administrativas e judiciais relevantes e exemplos práticos de aplicação, com o objetivo de avaliar se a configuração atual da base do legítimo interesse preserva, limita ou fragiliza a proteção dos direitos da personalidade.

O trabalho parte da premissa de que a proteção de dados pessoais constitui dimensão contemporânea dos direitos da personalidade e que qualquer base legal de tratamento deve ser interpretada e aplicada de modo a preservar o núcleo essencial da dignidade da pessoa humana, assegurando ao titular controle real — ainda que não absoluto — sobre o fluxo de informações que lhe dizem respeito. Nessa perspectiva, o teste de adequação de uma base legal não reside apenas na sua funcionalidade econômica ou operacional, mas na sua capacidade de respeitar, na prática, os valores fundamentais que justificam a existência do próprio regime de proteção de dados.

O trabalho organiza-se em seis partes, além desta introdução. A segunda parte trata dos direitos da personalidade e de sua relação com a proteção de dados pessoais, explorando a evolução conceitual da privacidade, a emergência da proteção de dados como categoria autônoma e a centralidade da autodeterminação informacional. A terceira parte apresenta, de forma sintética, o sistema de bases legais no GDPR e na LGPD, contextualizando o papel do legítimo interesse no conjunto das hipóteses legitimadoras. A quarta parte analisa o legítimo interesse no contexto europeu, examinando sua configuração normativa, as orientações interpretativas do CEPD e exemplos de aplicação prática. A quinta parte examina o legítimo interesse na LGPD,

considerando suas especificidades textuais, as diretrizes da ANPD e os desafios de implementação no contexto brasileiro. A sexta parte desenvolve análise comparativa e discute, de forma crítica, os impactos da base sobre os direitos da personalidade, avaliando se e em que medida sua utilização compromete a tutela efetiva da personalidade na era digital. A sétima parte traz as conclusões, sintetizando os achados da investigação e propondo direcionamentos para aplicação compatível da base com a tutela dos direitos da personalidade.

Espera-se que este artigo contribua para o aprofundamento do debate acadêmico e regulatório acerca da tensão entre a flexibilidade do legítimo interesse e a proteção efetiva dos direitos da personalidade no contexto digital. Como resultado teórico, pretende-se demonstrar que a base legal do legítimo interesse, embora funcionalmente necessária, encerra riscos estruturais de enfraquecimento da autodeterminação informacional quando aplicada sem salvaguardas robustas, interpretação restritiva e fiscalização intensa. Do ponto de vista prático, almeja-se fornecer subsídios para a atuação de autoridades de proteção de dados, particularmente a ANPD, na regulamentação mais detalhada da base, bem como orientar controladores de dados na realização de avaliações de legítimo interesse verdadeiramente rigorosas e documentadas.

Por fim, pretende-se estimular a produção de estudos empíricos futuros sobre a aplicação concreta da base no Brasil, permitindo avaliar, com dados, se o legítimo interesse tem operado como instrumento equilibrado de tutela ou como mecanismo de esvaziamento dos direitos da personalidade na era digital.

DIREITOS DA PERSONALIDADE E PROTEÇÃO DE DADOS PESSOAIS

A compreensão da relação entre direitos da personalidade e proteção de dados pessoais exige, em primeiro lugar, a retomada dos contornos clássicos desses direitos e, em seguida, a análise de como eles se projetam no contexto informacional contemporâneo. A expansão das tecnologias digitais, a circulação massiva de informações e a crescente capacidade de monitoramento e perfilamento de indivíduos alteraram profundamente o modo como a personalidade é exposta, explorada e, por consequência, tutelada juridicamente. Nesse cenário, a noção tradicional de proteção da intimidade e da vida privada passa a abranger, de forma cada vez mais intensa, o controle sobre os dados que representam a pessoa nos diversos ambientes digitais, o que torna indispensável tratar os direitos da personalidade e a proteção de dados como dimensões interdependentes de uma mesma preocupação central com a dignidade humana.

A doutrina define os direitos da personalidade como direitos subjetivos, de natureza extrapatrimonial, inerentes à pessoa humana, destinados à tutela de bens essenciais como a vida, a integridade física, a honra, a imagem, a intimidade e a identidade (TARTUCE, 2021, p. 162). No direito brasileiro, tais direitos encontram fundamento na Constituição Federal, em especial nos incisos V e X do art. 5.º, e disciplina específica nos arts. 11 a 21 do Código Civil.

Tepedino (2004, p. 57) caracteriza esses direitos como integrantes do “núcleo duro” da dignidade da pessoa humana, funcionando como limite material à atuação estatal e privada. Essa compreensão confere aos direitos da personalidade papel estruturante na ordem jurídica, impondo que qualquer atividade potencialmente lesiva à personalidade seja submetida a critérios rigorosos de legitimidade.

Com a transição para uma sociedade informacional, o foco da proteção deslocou-se progressivamente do espaço físico para os fluxos de informação. Rodotà (2008, p. 25) observa que “vivemos em uma sociedade em que a vigilância se tornou difusa e permanente”, de modo que a proteção da vida privada passa a dizer respeito, sobretudo, ao controle sobre os dados pessoais.

A LGPD conceitua dado pessoal como “informação relacionada a pessoa natural identificada ou identificável” (art. 5.º, I). Aparentemente técnica, essa definição revela que o objeto de tutela não é a informação em si, mas a pessoa a quem ela se refere. Mendes (2014, p. 102) sustenta que “os dados pessoais constituem, em termos jurídicos, uma forma de exteriorização da personalidade”, pois, combinados, permitem a reconstrução de perfis, hábitos, preferências e vulnerabilidades.

Doneda (2019, p. 51) enfatiza que “a proteção de dados pessoais não é um apêndice do direito à privacidade, mas uma categoria autônoma, ainda que relacionada, que se ocupa da circulação de informações pessoais em sociedades informacionais complexas”. Nessa perspectiva, a proteção de dados é vista como técnica específica de tutela da personalidade diante dos riscos do tratamento automatizado de informações.

A ideia de privacidade também sofreu releitura. No clássico texto de Warren e Brandeis (1890, p. 195), a privacidade era retratada como “the right to be let alone”. Em sociedades altamente conectadas, essa noção cede lugar a uma concepção de privacidade informacional, entendida como controle sobre o fluxo de informações pessoais. Rodotà (2008, p. 73) afirma que “a privacidade contemporânea deve ser compreendida como direito ao controle sobre o uso das informações pessoais”, ou seja, como poder de decidir quem sabe o quê, e em que condições.

Essa dimensão de controle é frequentemente traduzida pela expressão autodeterminação informacional, inspirada na jurisprudência constitucional alemã. Bioni (2019, p. 61) explica que essa autodeterminação “traduz a ideia de que o indivíduo deve poder decidir, de maneira livre e informada, sobre o fluxo de informações que o dizem respeito”, ainda que reconheça a possibilidade de a lei autorizar tratamentos independentes da vontade do titular, desde que respeitados seus direitos fundamentais.

A Emenda Constitucional n.º 115/2022 reforça essa arquitetura ao incluir expressamente a proteção de dados pessoais no rol dos direitos e garantias fundamentais (art. 5.º, LXXIX).

Com isso, consolida-se o entendimento de que o tratamento de dados pessoais está intrinsecamente ligado à tutela dos direitos da personalidade, exigindo que qualquer base legal de tratamento seja interpretada à luz da dignidade da pessoa humana e da proteção da personalidade em sua dimensão informacional.

BASES LEGAIS PARA O TRATAMENTO DE DADOS NO GDPR E NA LGPD

O tratamento de dados pessoais não pode ocorrer de forma arbitrária ou ilimitada. Tanto o Regulamento Geral de Proteção de Dados da União Europeia quanto a Lei Geral de Proteção de Dados brasileira estabelecem que toda operação com dados pessoais deve estar fundamentada em uma base legal expressamente prevista na norma. Esse modelo afasta a ideia de que a mera vontade das partes seria suficiente para legitimar qualquer tratamento, reconhecendo que os dados pessoais dizem respeito a direitos fundamentais que não podem ser objeto de disposição irrestrita. As bases legais funcionam, portanto, como filtros de legitimidade, delimitando as circunstâncias em que o tratamento pode ocorrer sem violar os direitos e liberdades dos titulares. Entre essas bases, destaca-se o legítimo interesse, que permite o tratamento mesmo sem consentimento do titular, desde que atendidos determinados requisitos e salvaguardas.

O GDPR estabelece, em seu art. 6.º, que o tratamento de dados pessoais só é lícito quando se enquadra em uma das bases ali previstas. Entre elas, incluem-se o consentimento, a execução de contrato, o cumprimento de obrigação legal, a proteção de interesses vitais, o exercício de funções de interesse público e o interesse legítimo do responsável ou de terceiros (UNIÃO EUROPEIA, 2016). O Considerando 40 esclarece que dados pessoais devem ser tratados com base no consentimento ou em “qualquer outro fundamento legítimo previsto por lei” (UNIÃO EUROPEIA, 2016).

Mendes (2014, p. 145) observa que o modelo europeu rompe com a noção de primazia absoluta do consentimento ao admitir múltiplas bases legítimas, reconhecendo que determinadas atividades socialmente necessárias não podem depender exclusivamente da vontade individual do titular.

No Brasil, a LGPD adota estrutura semelhante, mas com um rol mais extenso. O art. 7.º elenca dez hipóteses legais, incluindo consentimento, obrigação legal ou regulatória, execução de políticas públicas, realização de estudos por órgãos de pesquisa, execução de contrato, exercício regular de direitos, proteção da vida ou da incolumidade física, tutela da saúde, legítimo interesse do controlador ou de terceiro e proteção do crédito. Frazão, Tepedino e Oliva (2019, p. 89) destacam que essa opção reflete especificidades do contexto brasileiro, conferindo tratamento expresso a situações como a proteção do crédito e a pesquisa científica.

Os princípios previstos no art. 6.º da LGPD — finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização — funcionam como parâmetros transversais de interpretação. Doneda (2019, p. 103) enfatiza que esses princípios “constituem critérios normativos para aferir a licitude de qualquer tratamento, inclusive daqueles fundados em bases legais que dispensam o consentimento, como o legítimo interesse”.

Durante muito tempo, o consentimento ocupou posição central no discurso acerca da proteção de dados. Bioni (2019, p. 135) ressalta, porém, que “em contextos de forte assimetria informacional e de poder, o consentimento tende a ser uma ficção”, pois titulares aceitam políticas de privacidade sem efetiva compreensão, muitas vezes como condição para acessar serviços essenciais. Rodotà (2008, p. 134) adverte que, nessas circunstâncias, “o consenso, apresentado como expressão da liberdade, pode transmutar-se em instrumento de submissão”.

Diante dessas limitações, a proteção de dados não pode depender exclusivamente do consentimento. Outras bases legais assumem importância, entre elas o legítimo interesse, que permite tratamentos sem manifestação prévia do titular. A questão que se coloca é se essa flexibilização é compatível com a tutela reforçada dos direitos da personalidade.

O LEGÍTIMO INTERESSE NO GDPR

O Regulamento Geral de Proteção de Dados da União Europeia prevê o legítimo interesse como uma das hipóteses que autorizam o tratamento de dados pessoais sem necessidade de

consentimento do titular. Trata-se de base legal que, por sua natureza aberta e flexível, exige aplicação cuidadosa e ponderada. Diferentemente de outras bases que se fundamentam em critérios objetivos, como o cumprimento de obrigação legal ou a execução de contrato, o legítimo interesse demanda avaliação casuística, na qual devem ser considerados simultaneamente o interesse perseguido pelo controlador, a necessidade do tratamento e os direitos e liberdades fundamentais do titular. A experiência europeia desenvolveu, ao longo dos últimos anos, orientações interpretativas e critérios práticos para aplicação dessa base, consolidando entendimento de que o legítimo interesse não constitui autorização genérica para qualquer tratamento conveniente ao controlador, mas instrumento que deve ser utilizado de forma fundamentada, transparente e sujeita a controle rigoroso.

O art. 6.º, 1, f, do GDPR dispõe que o tratamento é lícito quando

“for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais” (UNIÃO EUROPEIA, 2016).

Trata-se de cláusula geral que exige, por construção, um juízo de ponderação.

O Considerando 47 indica exemplos de interesses que podem ser considerados legítimos, mencionando, entre outros, a prevenção de fraudes e o marketing direto. A referência a essas situações não afasta a necessidade de exame caso a caso, mas sugere campos em que a base encontra terreno típico de aplicação.

Bioni (2019, p. 197) descreve o legítimo interesse como

“uma cláusula geral de licitude, que admite o tratamento de dados sem consentimento sempre que houver um interesse juridicamente legítimo e socialmente aceitável, desde que submetido a um juízo de necessidade e proporcionalidade em face dos direitos fundamentais do titular”.

A prática regulatória europeia consolidou a compreensão de que a aplicação do legítimo interesse deve seguir uma estrutura tripartida, comumente denominada “Legitimate Interest Assessment” (LIA). O Comitê Europeu para a Proteção de Dados (CEPD, 2019) orienta que o controlador identifique, em primeiro lugar, o interesse perseguido, verificando se é concreto e legítimo; em seguida, analise a necessidade do tratamento para a realização desse interesse, avaliando alternativas menos intrusivas; por fim, realize um teste de balanceamento entre o interesse identificado e os direitos e liberdades do titular, considerando, entre outros fatores, a

natureza dos dados, o contexto da coleta, as expectativas razoáveis do titular e o impacto potencial do tratamento.

Mendes (2014, p. 203) sintetiza essa lógica ao afirmar que “o legítimo interesse não é um cheque em branco”, pois exige demonstração documentada da legitimidade do interesse, da necessidade do tratamento e da conclusão de que os direitos do titular não prevalecem no caso concreto.

Na prática, autoridades europeias têm admitido o uso da base em situações como marketing direto, desde que assegurado ao titular o direito de oposição simples e efetivo, e em contextos de segurança da informação, como detecção de ataques e fraudes. O CEPD (2019, p. 15) destaca que “o marketing direto pode, em determinadas circunstâncias, basear-se em legítimo interesse, mas o titular deve ser claramente informado e dispor de mecanismo simples de opt-out”.

Por outro lado, em casos de monitoramento massivo, reconhecimento facial e tratamento de dados sensíveis, a invocação do legítimo interesse tem sido rechaçada. Decisões de autoridades como a CNIL (França) e o Garante (Itália) apontam que a coleta massiva de imagens em espaços públicos ou na internet, para formação de bases de reconhecimento facial, não pode ser justificada por interesse legítimo, dada a intensidade da intrusão e a ausência de expectativas razoáveis por parte dos titulares.

Rodotà (2008, p. 159) adverte que, quando a cláusula do interesse legítimo é utilizada para legitimar práticas de vigilância difusa, perfilamento exaustivo ou exploração econômica agressiva dos dados, “a balança tende a pender perigosamente em desfavor da pessoa”, corroendo o sentido da proteção de dados como instrumento de tutela da personalidade.

Em síntese, o GDPR admite o legítimo interesse como base relevante e necessária, mas condiciona sua aplicação a um controle rigoroso, tanto interno, via LIA, quanto externo, por autoridades de proteção de dados e tribunais.

O LEGÍTIMO INTERESSE NA LGPD

A Lei Geral de Proteção de Dados brasileira incorporou o legítimo interesse como base legal alternativa ao consentimento, seguindo o modelo europeu, mas em contexto social, econômico e institucional bastante diverso. O dispositivo legal estabelece que o tratamento pode ocorrer quando necessário para atender a interesses legítimos do controlador ou de terceiro, desde

que não prevaleçam direitos e liberdades fundamentais do titular.

A norma brasileira acrescenta ainda referência expressa às legítimas expectativas do titular, introduzindo critério adicional de avaliação. Embora a estrutura normativa seja semelhante à europeia, a aplicação prática do legítimo interesse no Brasil enfrenta desafios específicos, relacionados à recente vigência da lei, à ainda incipiente cultura de proteção de dados, à forte assimetria informacional entre controladores e titulares e ao processo de consolidação da Autoridade Nacional de Proteção de Dados. Esse conjunto de fatores torna especialmente relevante examinar de que modo essa base legal vem sendo compreendida e aplicada no ordenamento brasileiro.

No ordenamento brasileiro, o art. 7.º, IX, da LGPD prevê que o tratamento de dados pessoais poderá ser realizado “quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”.

O art. 10 complementa essa disciplina ao estabelecer que o legítimo interesse “somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas”, mencionando, entre outras, o apoio e a promoção de atividades do controlador e a proteção, em relação ao titular, do exercício regular de direitos ou prestação de serviços que o beneficiem.

O mesmo dispositivo introduz o critério das “legítimas expectativas” do titular, ao afirmar que as finalidades devem respeitar as expectativas do titular, bem como seus direitos e liberdades fundamentais. Frazão, Tepedino e Oliva (2019, p. 211) interpretam essa referência como mecanismo de limitação adicional, que exige avaliar se, à luz do contexto e das informações fornecidas, o titular poderia razoavelmente esperar o tratamento realizado.

Bioni (2019, p. 205) identifica no legítimo interesse brasileiro “uma válvula de escape necessária para que atividades de baixo risco e alto interesse social possam ser realizadas sem o peso burocrático da gestão de consentimentos”, desde que acompanhadas de salvaguardas adequadas. Ao mesmo tempo, o autor alerta que, em ambiente marcado por forte assimetria informacional, baixa educação digital e fragilidade institucional, o uso extensivo da base pode abrir espaço para práticas abusivas.

Doneda (2019, p. 119) destaca que a LGPD importou a figura do legítimo interesse do GDPR para contexto em que a autoridade de proteção de dados ainda se encontra em processo de consolidação, o que exige aplicação estrita da base, sob pena de fragilização da nascente cultura

de proteção de dados.

A ANPD tem papel central nessa concretização. Em documentos orientativos, a autoridade enfatiza a necessidade de o controlador documentar o teste de balanceamento, demonstrando a necessidade do tratamento e a prevalência do interesse legítimo sobre os direitos do titular, bem como de assegurar transparência reforçada, com indicação clara da base legal e das finalidades, e mecanismos de oposição acessíveis.

Conforme guia orientativo, a ANPD (2024, p. 12) assevera que “o legítimo interesse não deve ser utilizado como base residual para qualquer tratamento que não se enquadre nas demais hipóteses”, e que o controlador deve estar preparado para demonstrar, à própria ANPD e ao titular, a legitimidade do interesse, a necessidade do tratamento e as medidas adotadas para proteção dos direitos e liberdades do titular.

Apesar dessas diretrizes, a prática revela incertezas e divergências. Decisões judiciais e discussões administrativas em temas como score de crédito, perfilamento de consumidores por aplicativos e compartilhamento de dados entre empresas evidenciam tendência de invocação ampla do legítimo interesse, nem sempre acompanhada do rigor exigido pelos princípios da LGPD.

ANÁLISE COMPARATIVA E IMPACTOS SOBRE OS DIREITOS DA PERSONALIDADE

A disciplina do legítimo interesse no GDPR e na LGPD apresenta significativa convergência textual, mas divergências relevantes no plano da aplicação concreta. Ambos os diplomas adotam estrutura normativa que exige identificação de interesse legítimo, avaliação da necessidade do tratamento e ponderação com os direitos e liberdades fundamentais do titular.

No entanto, as condições institucionais, culturais e econômicas em que cada norma opera produzem resultados distintos. Enquanto o contexto europeu se caracteriza por autoridades de proteção de dados consolidadas, jurisprudência robusta e maior consciência social sobre direitos de privacidade, o ambiente brasileiro ainda se encontra em fase de estruturação, com assimetrias informacionais mais acentuadas e mecanismos de fiscalização em processo de amadurecimento.

Essas diferenças impactam diretamente a efetividade da proteção conferida aos direitos da personalidade, especialmente quando a base do legítimo interesse é invocada para tratamentos de grande escala, baixa transparência ou finalidades distantes das expectativas razoáveis dos

titulares.

A comparação entre GDPR e LGPD evidencia significativa convergência textual na disciplina do legítimo interesse. Em ambos os diplomas, a base é alternativa ao consentimento, exige identificação de um interesse legítimo, submissão a um teste de necessidade e ponderação em face dos direitos e liberdades fundamentais do titular. Mendes (2014, p. 211) observa que os dois regimes partem da mesma matriz conceitual: admitem que interesses privados e públicos possam justificar tratamento sem consentimento, desde que não violem o núcleo dos direitos fundamentais.

Há, contudo, diferenças relevantes de contexto institucional e de implementação. Na União Europeia, a proteção de dados possui trajetória consolidada, com autoridades dotadas de maior estrutura, tradição jurisprudencial rica e cultura social mais amadurecida em torno da privacidade. No Brasil, a LGPD é recente, a ANPD ainda se estrutura e há elevada assimetria informacional e econômica entre controladores e titulares.

Rodotà (2008, p. 187) alerta para o risco de “transplantes jurídicos acríticos”, em que institutos concebidos em determinado ambiente regulatório são reproduzidos em outro sem adaptações proporcionais. No caso brasileiro, a importação da cláusula de legítimo interesse ocorre em ambiente de proteção institucional mais frágil, o que potencializa o risco de uso ampliado e pouco controlado da base.

Esse cenário tem impactos concretos sobre os direitos da personalidade. No que se refere à privacidade e à intimidade, a coleta e o cruzamento extensivo de dados para fins de perfilamento comportamental, marketing direcionado ou análise de risco, justificados por legítimo interesse, podem revelar aspectos sensíveis da vida privada, muitas vezes em desconexão com a finalidade original da coleta. Em relação à honra e à reputação, scores de crédito, rankings de confiabilidade e perfis de risco, elaborados com base em dados tratados por legítimo interesse, podem afetar diretamente a imagem social de indivíduos, sem transparência adequada sobre critérios e fontes.

A identidade e a autonomia também se veem afetadas. O uso de dados pessoais para tomada de decisões automatizadas, orientadas por interesses empresariais, tende a limitar possibilidades de escolha, “confinando” indivíduos em perfis que influenciam silenciosamente as oportunidades que lhes são oferecidas ou negadas (BIONI, 2019, p. 243). Doneda (2019, p. 132) assinala que tratamentos realizados à revelia da vontade do titular, com base em interesses de terceiros, sem transparência e possibilidade efetiva de oposição, produzem enfraquecimento da autodeterminação informacional, refletindo-se em uma personalidade menos livre.

Do ponto de vista do desenho normativo, o legítimo interesse apresenta natureza de cláusula geral. Rodotà (2008, p. 190) nota que esse tipo de cláusula pode funcionar tanto como instrumento de flexibilidade racional do sistema quanto como brecha para erosão de direitos fundamentais, sobretudo quando o controle institucional é frágil. Em sistemas em que a fiscalização é intensa, a documentação das avaliações de interesse legítimo é efetivamente exigida e há cultura de contestação dos titulares, a balança tende a ser mais equilibrada. Em sistemas em que essas condições não se verificam plenamente, cresce o risco de que o legítimo interesse se converta em “base coringa”, invocada para justificar uma ampla gama de tratamentos, em detrimento da centralidade da autodeterminação informacional.

Dessa forma, a análise comparativa indica que o legítimo interesse, em sua formulação atual, possui potencial para comprometer a proteção adequada dos direitos da personalidade, sobretudo em contextos de forte assimetria informacional, baixa transparência, baixa consciência dos titulares acerca de seus direitos e fiscalização limitada. Esse comprometimento decorre menos do texto normativo em si e mais da combinação entre a abertura conceitual da base e as condições concretas de sua aplicação.

CONCLUSÃO

O artigo examinou a base legal do legítimo interesse no GDPR e na LGPD à luz dos direitos da personalidade, tendo como eixo a questão de saber se essa base, em razão de sua flexibilidade, compromete a proteção adequada da personalidade na era digital.

A análise evidenciou que a proteção de dados pessoais se consolidou como dimensão específica da tutela da personalidade, em especial no que se refere à privacidade, à intimidade, à honra, à imagem e à identidade. A inclusão expressa da proteção de dados como direito fundamental no texto constitucional brasileiro reforçou a necessidade de interpretar o regime de tratamento de dados à luz da dignidade da pessoa humana.

Verificou-se que tanto o GDPR quanto a LGPD adotam sistema de bases legais múltiplas, no qual o consentimento é apenas uma entre diversas hipóteses que autorizam o tratamento de dados. Nesse contexto, o legítimo interesse assume função relevante ao permitir tratamentos necessários a determinadas atividades econômicas, tecnológicas e de interesse social, sem depender da manifestação prévia do titular.

Constatou-se, porém, que a natureza de cláusula geral do legítimo interesse exige controle

rigoroso. A previsão de testes de necessidade e de balanceamento, bem como de documentação das avaliações realizadas, compõe mecanismo destinado a evitar que interesses empresariais ou institucionais se sobreponham, de forma desproporcional, aos direitos e liberdades fundamentais dos titulares.

A comparação entre o contexto europeu e o brasileiro indicou que, embora exista forte similitude textual entre as normas, as condições institucionais e culturais de aplicação diferem significativamente. Em ambiente marcado por forte assimetria de poder entre grandes controladores e titulares, por limitada consciência social sobre direitos de proteção de dados e por autoridade reguladora ainda em consolidação, tende a aumentar o risco de uso expansivo e pouco controlado do legítimo interesse.

Diante desse quadro, a conclusão é que, na configuração atual, o legítimo interesse tem potencial para comprometer, em medida relevante, a proteção efetiva dos direitos da personalidade, especialmente quando utilizado de forma ampla, com baixa transparência, mecanismos de oposição pouco acessíveis e fiscalização limitada. Esse comprometimento não decorre da incompatibilidade necessária entre a base e a tutela da personalidade, mas da ausência, em muitos casos, de salvaguardas suficientes para conter a tendência de prevalência dos interesses do controlador.

A compatibilização entre legítimo interesse e proteção dos direitos da personalidade requer, portanto, medidas complementares, entre as quais se destacam: regulamentação mais detalhada pelas autoridades de proteção de dados, com exemplos setoriais de usos admitidos e vedados; exigência de maior transparência quanto ao uso da base e às avaliações de balanceamento; fortalecimento do direito de oposição, com procedimentos simples e efeitos concretos; auditorias independentes em operações de alto risco; e investimentos em educação digital, de modo a permitir que titulares compreendam o significado da base e possam reagir a seu uso indevido.

Nessas condições, o legítimo interesse pode ser preservado como instrumento funcionalmente necessário do sistema de proteção de dados, sem que isso implique esvaziamento da proteção conferida aos direitos da personalidade. Sem tais salvaguardas, contudo, a tendência é de que a flexibilidade da base se traduza, na prática, em fragilização da tutela da personalidade em sua dimensão informacional.

REFERÊNCIAS

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

BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS (CEPD). *Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*. Bruxelas, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

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

TARTUCE, Flávio. **Manual de direito civil**. Vol. único. 12. ed. Rio de Janeiro: Forense, 2021.

TEPEDINO, Gustavo. **Temas de direito civil**. Rio de Janeiro: Renovar, 2004.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – GDPR).

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