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

doi.org/10.51891/rease.v12i5.26395

# CONSENTIMENTO DIGITAL E TOMADA DE DECISÃO (DES) INFORMADA: PERSPECTIVA LEGAL COMPARADA ENTRE BRASIL E MODELOS INTERNACIONAIS DE PROTEÇÃO DE DADOS

## DIGITAL CONSENT AND (UN)INFORMED DECISION-MAKING: A COMPARATIVE LEGAL PERSPECTIVE BETWEEN BRAZIL AND INTERNATIONAL DATA PROTECTION FRAMEWORKS

## CONSENTIMIENTO DIGITAL Y TOMA DE DECISIONES (DES)INFORMADAS: PERSPECTIVA LEGAL COMPARADA ENTRE BRASIL Y MODELOS INTERNACIONALES DE PROTECCIÓN DE DATOS

**Hewerton Soares Vieira**[1]
**Paulo Beli Moura Stakoviak Júnior**[2]

RESUMO: Diante da da crescente centralidade do consentimento como fundamento jurídico para o tratamento de dados pessoais no ambiente digital, especialmente a partir da consolidação da Lei Geral de Proteção de Dados (LGPD). Embora juridicamente reconhecido como base legítima, o consentimento digital demonstra limitações quanto à sua efetividade material, uma vez que a tomada de decisão dos usuários é influenciada por assimetrias. O objetivo geral da pesquisa consiste em analisar os limites do consentimento enquanto base legal para o tratamento de dados pessoais à luz da LGPD, em perspectiva comparada com regimes internacionais, especialmente o GDPR. Para tanto, buscou-se examinar os fundamentos jurídicos do consentimento, identificar as limitações cognitivas e estruturais que afetam a tomada de decisão dos usuários e comparar a efetividade do consentimento em diferentes ordenamentos jurídicos. Metodologicamente, trata-se de uma pesquisa qualitativa, baseada em revisão sistemática da literatura. A análise é complementada por abordagem jurídico-comparada e por aportes interdisciplinares da economia comportamental e da psicologia da decisão, permitindo uma avaliação crítica da efetividade do consentimento para além de sua validade formal. Como resultado, verificou-se que o consentimento, embora juridicamente válido, não assegura uma decisão plenamente informada, reproduzindo limitações estruturais observadas também em regimes internacionais. Ademais, evidencia-se que tais limitações são intensificadas no contexto brasileiro, marcado por desigualdades estruturais, déficits de letramento digital e vulnerabilidades informacionais, que comprometem ainda mais a autonomia decisória dos titulares de dados. Conclui-se que o modelo centrado no consentimento apresenta insuficiências enquanto mecanismo de proteção de dados pessoais, exigindo a adoção de abordagens regulatórias complementares. Destaca-se a necessidade de fortalecimento institucional da autoridade reguladora, ampliação de políticas de educação digital, desenvolvimento de mecanismos que priorizem a regulação do uso dos dados, bem como a incorporação de perspectivas críticas, como a decolonial, capazes de considerar as especificidades sociais e informacionais do contexto brasileiro.

**Palavras-chave:** Consentimento digital. Proteção de dados pessoais. LGPD. Tomada de decisão. Vieses cognitivos. Economia comportamental. GDPR.

[1] Discente da Universidade Estadual do Tocantins – UNTINS.
[2] Orientador. Coordenador e Docente do Curso de Direito da Universidade Estadual do Tocantins – UNITINS. Doutor em Direito Constitucional (IDP - Brasil). Mestre em Constituição e Sociedade (IDP - Brasil).

ABSTRACT: Given the increasing centrality of consent as a legal basis for the processing of personal data in the digital environment, particularly following the consolidation of the General Data Protection Law (LGPD), consent has been recognized as a legitimate legal foundation. However, digital consent demonstrates limitations in terms of its material effectiveness, as users' decision-making is influenced by informational asymmetries.The main objective of this research is to analyze the limits of consent as a legal basis for the processing of personal data under the LGPD, from a comparative perspective with international regimes, especially the General Data Protection Regulation (GDPR). To this end, the study examines the legal foundations of consent, identifies cognitive and structural limitations affecting user decision-making, and compares the effectiveness of consent across different legal systems. Methodologically, this is a qualitative study based on a systematic literature review. The analysis is complemented by a comparative legal approach and interdisciplinary contributions from behavioral economics and decision-making psychology, allowing for a critical evaluation of the effectiveness of consent beyond its formal validity.The results indicate that, although legally valid, consent does not ensure a fully informed decision, reproducing structural limitations also observed in international regimes. Furthermore, these limitations are intensified in the Brazilian context, which is marked by structural inequalities, deficits in digital literacy, and informational vulnerabilities that further compromise the decision-making autonomy of data subjects. It is concluded that the consent-centered model presents significant shortcomings as a mechanism for personal data protection, requiring the adoption of complementary regulatory approaches. In this regard, the study highlights the need to strengthen the institutional capacity of regulatory authorities, expand digital literacy policies, develop mechanisms that prioritize the regulation of data use rather than merely its collection, and incorporate critical perspectives, such as decolonial approaches, capable of addressing the social and informational specificities of the Brazilian context.



**Keywords:** Digital consent. Data protection. LGPD. Decision-making. Cognitive biases. Behavioral economics. GDPR.

RESUMEN: Ante la creciente centralidad del consentimiento como fundamento jurídico para el tratamiento de datos personales en el entorno digital, especialmente a partir de la consolidación de la Ley General de Protección de Datos (LGPD), si bien está jurídicamente reconocido como una base legítima, el consentimiento digital presenta limitaciones en cuanto a su efectividad material, ya que la toma de decisiones de los usuarios está influenciada por asimetrías. El objetivo general de la investigación consiste en analizar los límites del consentimiento como base legal para el tratamiento de datos personales a la luz de la LGPD, en una perspectiva comparada con regímenes internacionales, especialmente el GDPR. Para ello, se buscó examinar los fundamentos jurídicos del consentimiento, identificar las limitaciones cognitivas y estructurales que afectan la toma de decisiones de los usuarios y comparar la efectividad del consentimiento en diferentes ordenamientos jurídicos. Metodológicamente, se trata de una investigación cualitativa, basada en una revisión sistemática de la literatura. El análisis se complementa con un enfoque jurídico-comparado y con aportes interdisciplinarios de la economía conductual y de la psicología de la decisión, lo que permite una evaluación crítica de la efectividad del consentimiento más allá de su validez formal. Como resultado, se verificó que el consentimiento, aunque jurídicamente válido, no garantiza una decisión plenamente informada, reproduciendo limitaciones estructurales también observadas en regímenes internacionales. Además, se evidencia que tales limitaciones se intensifican en el contexto brasileño, marcado por desigualdades estructurales, déficits de alfabetización digital y vulnerabilidades informacionales, que comprometen aún más la autonomía decisoria de los

titulares de datos. Se concluye que el modelo centrado en el consentimiento presenta insuficiencias como mecanismo de protección de datos personales, lo que exige la adopción de enfoques regulatorios complementarios. Se destaca la necesidad de fortalecer institucionalmente a la autoridad reguladora, ampliar las políticas de educación digital, desarrollar mecanismos que prioricen la regulación del uso de los datos, así como incorporar perspectivas críticas, como la decolonial, capaces de considerar las especificidades sociales e informacionales del contexto brasileño.

**Palabras clave:** Consentimiento digital. Protección de datos personales. LGPD. Toma de decisiones. Sesgos cognitivos. Economía conductual. GDPR.

## INTRODUÇÃO

A centralidade do consentimento como fundamento de legitimidade para o tratamento de dados pessoais no ambiente digital é um pressuposto jurídico no ordenamento brasileiro, especialmente a partir da consolidação de marcos normativos como a Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018).

Contudo, sustenta-se neste estudo que, embora juridicamente válido, o consentimento digital não assegura uma tomada de decisão plenamente informada por parte do titular de dados (Melo, 2025), na medida em que é atravessado por limitações cognitivas, assimetrias informacionais e estruturas tecnológicas que influenciam o comportamento do usuário (Abrusio, 2024). Tal constatação aponta para uma tensão entre a validade formal do consentimento e sua efetividade material enquanto expressão da autonomia informacional.



Nesse sentido, parte-se de alguns pressupostos teóricos, como o conceito de consentimento informado, no âmbito da proteção de dados, pressupõe que o titular compreenda, de forma clara e acessível, as condições e consequências do tratamento de seus dados pessoais (Melo, 2025). Em segundo lugar, adota-se o conceito de autodeterminação informativa, entendido como o direito do indivíduo de controlar o fluxo de suas informações pessoais (Neves; Matos, 2025). Ademais, como instrumento de análise da efetividade jurídica do consentimento, incorpora-se a perspectiva da Economia Comportamental orientada por Gerber, Stover e Marky (2022), segundo a qual a tomada de decisão dos indivíduos não ocorre em condições ideais de racionalidade (*Homos Economicus*), influenciada por vieses cognitivos e pela arquitetura da escolha.

A problemática que orienta esta pesquisa insere-se no contexto da crescente intensificação da economia de dados e da complexificação das interações digitais. Estudos empíricos indicam que a maioria dos usuários não lê integralmente as políticas de privacidade, tampouco compreende os termos aos quais consente, o que evidencia um cenário de assimetria

informacional e sobrecarga cognitiva. Além disso, práticas como o uso de interfaces persuasivas e *dark patterns* reforçam a indução de comportamentos, comprometendo a autonomia decisória.

Diante disso, coloca-se o seguinte problema de pesquisa: quais são os limites do consentimento como base legal para o tratamento de dados pessoais na LGPD, à luz de uma análise comparada com regimes internacionais e das evidências sobre a (des)informação na tomada de decisão no ambiente digital?

O objetivo geral consiste em analisar os limites do consentimento à luz da LGPD, em perspectiva comparada com regimes internacionais, notadamente o europeu, representado pelo GDPR. Como objetivos específicos, busca-se: (i) examinar os fundamentos jurídicos do consentimento na proteção de dados; (ii) identificar as limitações cognitivas e estruturais que afetam a tomada de decisão no ambiente digital; e (iii) comparar a efetividade do consentimento em diferentes ordenamentos jurídicos. A análise articula fontes normativas (LGPD e GDPR), doutrinárias e evidências empíricas oriundas de estudos interdisciplinares.

Do ponto de vista metodológico, a pesquisa adota uma abordagem qualitativa, com base em revisão da literatura orientada por busca exploratória de trabalhos, complementada por análise jurídica comparada. O estudo limita-se à estudos publicados nos últimos cinco anos (2021-2026); bases de dados: *Scielo*, *Google Schollar* e CAPES periódicos; recorte temático: consentimento como base legal para o tratamento de dados pessoais; critérios de exclusão: outras hipóteses legais previstas na LGPD. Diferencia-se de abordagens estritamente normativas ao incorporar evidências da psicologia da decisão e da economia comportamental, buscando superar análises que tratam o consentimento como expressão automática de autonomia. Assim, o presente estudo contribui ao evidenciar a insuficiência do modelo centrado no consentimento em perspectiva comparada.



Por fim, o argumento será desenvolvido em etapas. Inicialmente, examinam-se os fundamentos jurídicos do consentimento na proteção de dados, com destaque para a LGPD e o GDPR. Em seguida, analisam-se as limitações cognitivas e estruturais da tomada de decisão no ambiente digital, à luz de evidências interdisciplinares. Posteriormente, realiza-se uma análise comparada entre o Brasil e regimes internacionais, evidenciando convergências e limitações do modelo.

## 2. FUNDAMENTOS JURÍDICOS DO CONSENTIMENTO NA PROTEÇÃO DE DADOS

O art. 7º da LGPD determina que "o tratamento de dados pessoais somente poderá ser

realizado [...]" dentre outras hipóteses, "[...] mediante o fornecimento de consentimento pelo titular" (Brasil, 2018, p. *online*). Tal previsão normativa posiciona o consentimento como um dos principais fundamentos de legitimidade no ordenamento brasileiro. Contudo, a partir dessa centralidade, impõe-se a seguinte reflexão: o consentimento, conforme previsto na LGPD, constitui um instrumento suficiente para legitimar o tratamento de dados pessoais, considerando as complexidades do ambiente digital?

Os autores Justino e Teixeira (2025) apontam que o artigo 7º da LGPD isoladamente não constitui elemento suficiente para garantir a proteção efetiva do usuário, considerando usuários de serviços digitais. Apesar de ser definido legalmente como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Brasil, 2018, p.*online*), os autores destacam que existe um abismo entre o rigor normativo e a sua eficácia na prática, complementado por Abrusio (2024, p.181, tradução nossa) "os indivíduos enfrentam dificuldades para compreender plenamente e refletir sobre os termos contidos nas políticas que são objeto do consentimento expresso".

Ao longo deste trabalho serão destacados os vieses e limitações que sustentam a crítica de diversos autores da literatura científica de dados, nos campos jurídico, tecnológico e comportamental diante do consentimento digital, instrumento que é formalmente válido e aplicado nas relações sociais no Brasil. Nesse sentido, busca-se demonstrar que fatores presentes nas interfaces digitais comprometem a efetividade do consentimento, reforçando a necessidade de uma análise crítica de sua centralidade enquanto mecanismo de legitimação do tratamento de dados.



Sendo assim, diante dos requisitos para a validade do consentimento, analisa-se, inicialmente, o elemento da liberdade, que pressupõe a possibilidade de o usuário exercer uma escolha real, livre de coerção ou imposição (Melo, 2025; Couto, 2025). Nesse contexto, Justino e Teixeira (2025) e Diniz (2025) destacam que modelos do tipo *take-it-or-leave-it*[3] e *consent or pay*[4] comprometem a voluntariedade do consentimento, na medida em que impõem ao usuário uma aceitação integral como condição para o acesso ao serviço. Tais práticas configuram uma espécie de simulação de escolha, impedindo o titular de mensurar o alcance efetivo de sua decisão e, consequentemente, limitando sua liberdade (Paixão, 2025).

Ademais, observa-se que a autonomia do usuário é condicionada por fatores tanto

[3] Pegar ou largar (tradução nossa).
[4] consinta ou pague (tradução nossa).

intrínsecos quanto extrínsecos. Nesse sentido, o aceite de termos pode estar associado, entre outros aspectos, à pressão social vinculada ao uso de tecnologias, uma vez que a não adesão pode gerar sensação de exclusão, bem como à tendência de subvalorização dos próprios dados pessoais pelos usuários contemporâneos (Diniz, 2025).

Um segundo requisito essencial à validade do consentimento é o acesso à informação, que legitima a manifestação informada do titular. Para que o consentimento seja considerado válido, o usuário deve receber informações em linguagem clara, precisa e acessível, de modo a possibilitar a compreensão efetiva acerca do tratamento de seus dados pessoais. Mesmo no ambiente digital, a doutrina relaciona a fundamentalidade do ato de consentir a uma dimensão gnoseológica, isto é, à capacidade do titular de conhecer a natureza do tratamento e suas implicações. Nesse sentido, as informações fornecidas devem abranger, entre outros elementos, a finalidade específica do tratamento, a identificação do controlador, o período de armazenamento, os riscos envolvidos e os possíveis compartilhamentos de dados. Não cabe ao titular presumir tais aspectos, recaindo sobre o controlador o dever ativo de fornecer todas as informações necessárias para uma decisão consciente e refletida (Paixão, 2025; Santos; Alves; Quintino, 2025; Melo, 2025; Couto, 2025).

A jurisprudência brasileira corrobora essa compreensão ao atribuir centralidade ao dever qualificado de informação. O Superior Tribunal de Justiça, no julgamento do REsp 1.326.592/GO, firmou entendimento de que a prestação de informação adequada e transparente constitui obrigação essencial do fornecedor, sendo indispensável à formação de um consentimento válido. Conforme destacado, a informação deficiente, seja por omissão, incompletude ou inadequação,equivale à ausência de informação, sobretudo diante da desigualdade técnica e informacional entre as partes. Ademais, reconheceu-se que o direito à informação adequada e a proteção contra práticas abusivas são direitos básicos do consumidor, cuja inobservância compromete a qualidade do consentimento e o equilíbrio contratual (Brasil, 2019).



Por fim, a inequivocidade é um dos critérios que exige do usuário uma atitude clara quanto a sua decisão, os autores Melo (2025) e Diniz (2025) destacam que o silêncio, a inatividade ou o uso de caixas de seleção pré-marcadas (*opt-out*) não constituem consentimento válido. Destaca-se que diferente do Marco Civil da Internet (Lei 12.965/2014), que exigia consentimento "expresso" (mais formal), a LGPD foca na inequivocidade (mais pragmática), priorizando a certeza de que a vontade foi manifestada (Abrusio, 2024; Brasil, 2014).

Diante do exposto, observa-se que, embora o consentimento seja estruturado

juridicamente a partir dos requisitos de liberada, informação e inequivocidade, sua concretização no ambiente digital encontra limitações que comprometem sua efetividade material. A presença de fatores como assimetrias informacionais, pressões sociais e estratégias estruturais das plataformas evidencia que o cumprimento fomal desses requisitos não é suficiente para assegurar uma manifestação verdadeiramente livre e informada por parte do titular.

## 3. LIMITAÇÕES DA TOMADA DE DECISÃO NO AMBIENTE DIGITAL

Embora o ordenamento jurídico, especialmente por meio da LGPD, pressuponha que o titular de dados seja capaz de manifestar um consentimento livre, informado e inequívoco, tal premissa repousa, em grande medida, sobre o pressuposto de que os indivíduos tomam decisões de forma racional e consciente.

Contudo, essa concepção tem sido progressivamente tensionada por evidências interdisciplinares, sobretudo no campo da economia comportamental, que demonstram que a tomada de decisão humana é marcada por limitações cognitivas, vieses e heurísticas, afastando-se do modelo clássico de racionalidade plena, frequentemente associado à figura do *Homo Economicus*, a qual se demonstra, no contexto das interações digitais, como uma construção teórica dissociada da realidade empírica (Abrusio, 2024).



Nesse contexto, a incorporação dessas evidências não representa um afastamento do campo jurídico, mas, ao contrário, constitui instrumento jurídico válido para avaliar a efetividade dos requisitos legais do consentimento. Isso porque, se a decisão do titular é condicionada por limitações cognitivas e por estruturas que influenciam sua escolha, torna-se necessário questionar se o consentimento, embora formalmente válido, atende, de fato, às exigências de informação e liberdade previstas na legislação.

Diante disso, o presente capítulo busca analisar em que medida a tomada de decisão dos usuários no ambiente digital é afetada por limitações cognitivas e quais são os impactos dessa condição sobre a validade e a efetividade do consentimento no âmbito da proteção de dados pessoais.

A mente humana opera em dois modos, o sistema 1 é de processamento rápido de informações, intuitivo e automático e o sistema 2 é lento, analítico e exige esforço deliberado. No ambiente digital, o fluxo constante de interações e a pressão por agilidade levam os usuários a operarem predominantemente pelo sistema 1. Como o Sistema 2 exige atenção total e é facilmente desviado, as tarefas complexas, como ler e validar políticas de privacidade, são

negligenciadas em favor de decisões automáticas e rápidas (Taneva, 2022; Gerber; Stover; Marky, 2022).

A partir do levantamento de dados bibliográficos, os principais vieses cognitivos identificados na literatura estão sintetizados no Quadro 01, evidenciando os fatores que comprometem a tomada de decisão informada no ambiente digital.

**Quadro 01 -** Principais vieses cognitivos na tomada de decisão no ambiente digital

| Viés cognitivo | Autores | Descrição | Impacto no consentimento digital |
|---|---|---|---|
| Viés da Gratificação Imediata | Melo (2025); Gerber, Stover e Marky (2022); Silveira (2024); Taneva (2022). | Tendência de priorizar benefícios imediatos, como acesso rápido a serviços, em detrimento de riscos futuros e incertos, como perda de privacidade ou uso indevido de dados. | O usuário aceita termos rapidamente, sem avaliar consequências de longo prazo, comprometendo o caráter informado do consentimento. |
| Sobrecarga de Informação e Fadiga de Decisão | Abrusio (2024); Melo (2025); Silveira (2024). | Volume excessivo e complexidade técnica das políticas de privacidade dificultam a compreensão e processamento das informações. | Gera a chamada "fadiga de consentimento", levando o usuário a clicar em "aceito" apenas para prosseguir, sem real compreensão. |
| Viés de Otimismo (Inabalabilidade) | Gerber, Stover e Marky (2022); | Crença de que riscos digitais são menores para si ou de que não há consequências relevantes ("não tenho nada a esconder"). | Estimula o compartilhamento excessivo de dados e reduz a percepção de risco, enfraquecendo a tomada de decisão crítica. |
| Aversão à Perda e Efeito de Rede | Gerber, Stover e Marky (2022); Nogueira; Oldoni (2025); Vasconcelos (2024). | Medo de perder acesso a serviços ou de exclusão social ao não aderir a determinadas plataformas. | Induz o usuário a aceitar termos potencialmente abusivos para evitar perdas sociais ou funcionais, limitando a liberdade do consentimento. |

**Fonte:** elaboração própria, com base na literatura analisada, 2025.

Essas limitações cognitivas explicam o paradoxo da privacidade, fenômeno em que os indivíduos afirmam valorizar muito sua privacidade em questionários, mas, na prática, adotam comportamentos que a comprometem em troca de pequenas conveniências. Em que, o consentimento converte-se em um ato automatizado e acrítico, desprovido de reflexão e crítica, deixando de ser uma escolha e passa a ser um comportamento induzido (Melo, 2025).

A quantidade e a complexidade das informações fornecidas aos usuários não apenas comprometem, mas frequentemente inviabilizam a possibilidade de um consentimento realmente informado, transformando esse requisito legal em um "mito" ou uma mera "formalidade legal" (Lima, 2025, p.02). As fontes indicam que o modelo atual cria barreiras intransponíveis para a compreensão do titular através de diversos mecanismos.

A partir do exposto, é possível responder se as interfaces efetivamente influenciam ou

manipulam a decisão do titular dos dados no momento do consentimento?

Para responder a esse questionamento, a literatura aponta que, no momento do consentimento, o usuário é exposto à arquitetura da escolha que pode ou não estar associado à padrões obscuros (*dark patterns*) discutidos por Melo (2025) e Abrusio (2024). As fontes indicam que o design das interfaces não é axiologicamente neutro e, frequentemente, é construído para induzir comportamentos que favorecem os interesses econômicos das plataformas em detrimento da privacidade do indivíduo.

Além dos vieses supramencionados associam-se outros mecanismos psicológicos explorados pelo *marketing* como a hierarquia e realce de cores em que em um estudo realizado por Melo (2025) 51,33% dos casos analisados o botão aceitar utilizam cores chamativas e contrastantes, enquanto enquanto as opções de "Rejeitar" ou "Gerenciar" são apresentadas em cores neutras, fontes menores ou escondidas, induzindo o clique por conveniência identificado também pela autora Taneva (2022), do mesmo modo, por um estudo sobre *dark patterns* através da Lei Europeia de privacidade de dados pelos autores Martini e Drews (2021).

Ainda sobre isso, Melo (2025) identificou que em 95,35% dos casos analisados houve ocultação de configurações ou obstrução de informações, em que o usuário precisava navegar por menus complexos ou realizar múltiplos cliques (até 18 em alguns casos) para recusar o tratamento de dados, enquanto a aceitação é facilitada com um único clique.



Essas práticas criam um ambiente de autodeterminação informativa ilusória. Ao dificultar a recusa e facilitar a aceitação, as interfaces subvertem a vontade do titular, transformando o consentimento, que deveria ser uma "manifestação livre e inequívoca", em uma renúncia forçada e impensada da privacidade. O resultado é o que as fontes chamam de "cultura do consentimento cego", onde o *design* persuasivo anula a capacidade de reflexão crítica do sujeito informacional (Melo, 2025; Vasconcelos, 2024; Couto, 2025).

Diante do exposto, verifica-se que a tomada de decisão no ambiente digital não ocorre em condições ideais de racionalidade, mas é condicionada por limitações cognitivas, vieses comportamentais e estruturas tecnológicas que influenciam o comportamento dos indivíduos. Assim, evidencia-se que a validade formal do consentimento não é suficiente para assegurar sua efetividade material, o que impõe a necessidade de repensar sua posição enquanto instrumento central de legitimação do tratamento de dados pessoais no contexto contemporâneo.

## 4. CONSENTIMENTO DIGITAL EM PERSPECTIVA COMPARADA

Em 2012 a Comissão Europeia propôs o Regulamento Europeu 2016/679, conhecido

como Regulamento Geral de Proteção de Dados (GDPR), mecanismo de direito comunitário, considerado "um novo paradigma de proteção de dados pessoais não restrito à UE, sendo um autêntico marco regulatório e modelo legislativo de *compliance* para o mundo". Com forte influência deste modelo, no ano de 2018 o Congresso brasileiro publicou a Lei nº 13.709/2018, conhecida como LGPD, "foca na defesa dos direitos fundamentais à privacidade e liberdade que recaem sobre os dados pessoais, sendo que as sanções aos autores de vazamentos estão positivadas nos artigos da lei, porém as indenizações exigem a prova dos danos" (Mello *et al.*, 2025, p. 05).

A análise comparativa entre a LGPD e o GDPR evidenciou uma relação de forte inspiração, mas também distinções importantes em termos de detalhamento e aplicação prática que serão explicitados ao longo desta seção, pois, pesar das convergências estruturais, as diferenças entre os regimes demonstram limites quanto à efetividade da proteção de dados, especialmente no que se refere à operacionalização normativa e à capacidade institucional de fiscalização.

É necessário destacar que o GDPR é citado na literatura como uma norma que serve de parâmetro para diversos ordenamentos, sendo assim, é possível estabelecer semelhanças extraídas do padrão adotado pelo Parlamento Europeu na LGPD, como: visa proteger os direitos fundamentais de liberdade e privacidade, tais como o livre desenvolvimento da personalidade; as definições de dados pessoais e dados sensíveis são quase idênticas nos dois diplomas, tratamento também como amplo e similar; direitos dos titulares como acesso, confirmação de tratamento, retificação, eliminação e a portabilidade de dados; consentimento como base central, incluindo-se o legítimo interesse; incorporação do princípio *privacy by design* de proteção de dados "desde a concepção" (*by design*) e "por padrão" (*by default*), exigindo que a segurança seja integrada ao sistema desde o início (Couto, 2025; Paixão, 2025; Abrusio, 2024; Cohen; Slotje, 2026).



Não obstante as convergências normativas entre os diplomas, a análise comparada também apontou divergências quanto ao grau de detalhamento, à aplicação prática e aos mecanismos de efetividade das normas, que são apresentadas no Quadro 02, abaixo:

**Quadro 02 -** Principais divergências entre LGPD e GDPR

| Aspecto | Autores | LGPD (Brasil) | GDPR (União Europeia) |
|---|---|---|---|
| Robustez e detalhamento normativo | Paula (2023); Medeiros e Feller (2024). | Considerada menos extensiva, com maior margem de subjetividade e uso de termos abertos, como "prazo | Apresenta maior detalhamento normativo, com regras mais específicas, como prazos |

| | | | |
|---|---|---|---|
| | | razoável". | definidos (ex: 72 horas para notificação de incidentes). |
| Quantidade de bases legais | Melo (2025); Andrade *et al.*, (2024); Couto (2025); Vasconcelos (2024). | Prevê 10 bases legais para o tratamento de dados pessoais (art. 7º), incluindo hipóteses como proteção ao crédito e segurança pública. | Estabelece 6 bases legais, com estrutura mais enxuta e sistematizada. |
| Sanções e penalidades | Justino e Teixeira (2025); Araujo (2023); Medeiros e Feller (2024). | Multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração. | Permite sanções mais elevadas, podendo chegar a até 4% do faturamento global anual da empresa. |
| Autoridades de controle | Justino e Teixeira (2025); Gaigher e Pasqualotto (2025); Silveira (2024). | Fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD), ainda em processo de consolidação institucional. | Fiscalização por autoridades nacionais independentes e consolidadas (ex: CNIL – França), com maior tradição regulatória |

**Fonte:** elaboração própria, com base na literatura analisada, 2025.

A comparação evidencia que, embora ambos os regimes compartilhem uma base principiológica semelhante, as distinções estruturais influenciam diretamente a forma como a proteção de dados se concretiza na prática. O maior grau de detalhamento normativo e a consolidação institucional do modelo europeu tendem a reduzir margens interpretativas e a reforçar a previsibilidade regulatória, ao passo que a flexibilidade presente no modelo brasileiro, embora permita adaptações contextuais, pode comprometer a uniformidade na aplicação da norma.



Além disso, a diversidade de bases legais prevista na legislação brasileira (que elenca dez hipóteses autorizativas no art. 7º da LGPD) amplia as possibilidades de tratamento de dados, o que, por um lado, favorece a operacionalização das atividades econômicas, mas, por outro, pode enfraquecer a centralidade do consentimento como mecanismo de controle pelo titular (Justino; Teixeira, 2025). Sendo assim, essa ampliação visa garantir que a lei não "enrijeça" ou impeça o empreendedorismo e a inovação, permitindo que as atividades econômicas fluam sem depender exclusivamente da vontade do titular em todas as interações (Couto, 2025). Contudo, a diversidade de bases legais facilita a transformação dos dados em uma mercadoria (*commodity*)(Corrêa, 2023).

Soma-se a isso a função das autoridades de fiscalização, cuja capacidade institucional impacta diretamente a efetividade das garantias legais, evidenciando que a proteção de dados não depende apenas da norma em si, mas também das condições concretas de sua implementação (Neves; Matos, 2025).

Sendo assim, verifica-se que, embora a LGPD e o GDPR compartilhem fundamentos principiológicos semelhantes, as diferenças estruturais e institucionais entre os regimes revelam

limites relevantes quanto à efetividade da proteção de dados pessoais, observa-se, ainda que as diferenças entre os regimes não se limitam a aspectos formais, mas demonstram distintos níveis de maturidade regulatória, com implicações materiais e formais para a efetividade do consentimento enquanto instrumento de proteção.

## 5. CONSENTIMENTO COMO INSTRUMENTO DE PROTEÇÃO DE DADOS: UMA ANÁLISE CRÍTICA AO CONTEXTO LOCAL

A partir das análises realizadas, impõe-se a problematização acerca da efetividade do consentimento enquanto instrumento de proteção de dados pessoais. Nesse contexto, surge o questionamento quanto a efetividade de garantia do consentimento, o modelo europeu seria, portanto, um modelo mais efetivo do que o brasileiro? e a problemática de consentimento do Brasil é específico ou representa em algum ponto uma limitação estrutural global?

Em resposta a isso, é necessário destacar, que embora o modelo Europeu seja considerado por alguns autores como padrão-ouro municipal e seja a principal base para a criação da LGPD, a sua superioridade em termos de efetividade material é objeto de debate, a partir do disposto no Quadro 02, acrescenta-se mais uma lente comparativa a de que ambos os países possuem desafios na efeitvidade da norma, conforme foi demonstrado ao longo desta pesquisa, como o "mito" do consentimento, a prevalência do *dark patterns*, bem como o modelo *consent-or-pay*.



A partir de uma perspectiva deocolonial, Melo (2025) questiona se a busca pela "efetividade" deve se dar apenas pela reprodução do modelo europeu. Argumenta-se que, como país do Sul Global, o Brasil deveria construir marcos próprios que considerem suas especificidades locais e desigualdades estruturais, em vez de apenas adaptar diretrizes eurocêntricas que podem perpetuar dependências epistemológicas e tecnológicas.

Essa "dependência epistemológica" ignora que o Brasil possui problemas sociais e estruturais considerados muito mais urgentes pela população, o que faz com que a proteção de dados só seja percebida como relevante após a satisfação de outras necessidades básicas (Paula, 2023). O analfabetismo funcional e digital são barreiras presentes no país: mesmo indivíduos que possuem acesso a equipamentos muitas vezes carecem de competências para interpretar dados, buscar informações públicas ou participar ativamente de processos digitais (Gomes; Souza; Duarte, 2025).

Estudos com estudantes universitários brasileiros revelaram que apenas 9,42% da amostra reconhecia de fato as implicações de conceder acesso aos seus dados, enquanto a maioria

absoluta tinha pouco ou nenhum conhecimento sobre os riscos envolvidos (Justino; Teixeira, 2025).

Observa-se, portanto, que no contexto de comunidades tradicionais (como no Semiárido), a dependência de sistemas burocráticos digitais e o requisito de "letramento jurídico" resultam em uma exclusão epistemológica, onde saberes locais são convertidos em dados técnicos sem o consentimento efetivo ou a compreensão dessas populações (Ramos, *et al.*, 2026).

Portanto, no contexto brasileiros, os estudos apontam a hiper-fragilidade local em comparação ao contexto global, visto que, a fragilidade da leitura compreensiva e a exposição a fluxos acelerados de informação comprometem a capacidade dos cidadãos de diversos nichos populacionais de analisar criticamente os dicursos digitais, consequentemente o consentimento de fornecimento de dados. Sendo necessárias políticas para garantia de justiça informacional (Melo, 2025).

Diante das limitações estruturais e cognitivas do modelo centrado no consentimento, as fontes sugerem uma abordagem multidimensional que combine soluções tecnológicas, fortalecimento institucional e justiça social adaptada à realidade brasileira.. Destaca-se, que a LGPD aponta a Autoridade Nacional de Proteção de Dados (ANPD) como ator de governança no âmbito da proteção de dados, para isso é necessário que possua maior autonomia, recursos e uma postura fiscalizatória mais rígida para coibir práticas abusivas das grandes corporações (Lima, 2025).



Além disso, a proteção do titular de dados deve ser compreendida como resultado de uma atuação articulada entre diferentes esferas institucionais. Nesse sentido, destaca-se a necessidade de cooperação entre a Autoridade Nacional de Proteção de Dados (ANPD) e os órgãos de defesa do consumidor, de modo a viabilizar a aplicação integrada do Código de Defesa do Consumidor como instrumento de equilíbrio das relações marcadas pela hipossuficiência informacional do usuário. Tal articulação permite ampliar a efetividade da tutela jurídica, especialmente diante das assimetrias estruturais presentes no ambiente digital (Justino; Teixeira, 2025; Silva, 2024).

Nesse contexto, emerge a necessidade de reorientação do eixo regulatório, deslocando-se o foco tradicional do momento do consentimento para a análise da finalidade e do uso efetivo dos dados pessoais. Essa perspectiva busca superar a centralidade formal do consentimento, restringindo interpretações excessivamente amplas do "legítimo interesse" e promovendo um controle mais substancial sobre as práticas de tratamento de dados. Assim, propõe-se uma

abordagem que privilegie a responsabilização contínua dos agentes de tratamento, em detrimento de uma lógica meramente autorizativa baseada no aceite do titular (Melo, 2025).

Sob uma perspectiva decolonial, evidencia-se que a formulação de políticas públicas no campo da proteção de dados deve considerar a pluralidade de saberes e contextos socioculturais, especialmente em países do Sul Global. Nesse sentido, torna-se imprescindível garantir que o tratamento de dados envolvendo comunidades tradicionais respeite sua autodeterminação informativa, evitando a conversão de saberes locais em dados técnicos sem a devida compreensão ou consentimento efetivo dessas populações. Tal abordagem busca romper com padrões epistemológicos hegemônicos que desconsideram as especificidades locais (Ramos *et al.*, 2026).

Ademais, a promoção da alfabetização tecnológica configura-se como elemento que soma para o fortalecimento da autonomia dos titulares de dados. A educação digital, nesse contexto, exerce protagonismo ao capacitar os indivíduos para a compreensão crítica das práticas de coleta e tratamento de dados, reduzindo sua vulnerabilidade a mecanismos de manipulação comportamental (Andrade *et al.*, 2024; Gomes; Souza; Duarte, 2025; Pinto; Ferreira, 2025).

Por fim, a superação das limitações do modelo centrado no consentimento demanda a adoção de soluções que transcendam o ambiente exclusivamente digital. A implementação de alternativas analógicas mostra-se fundamental para garantir o acesso a direitos por populações vulneráveis, evitando que a exclusão digital se converta em barreira ao exercício da cidadania. Paralelamente, impõe-se o reconhecimento de uma responsabilidade compartilhada na proteção da privacidade, na qual o Estado seja garantidor frente ao poder das grandes plataformas digitais. Tal perspectiva reforça a necessidade de uma atuação regulatória capaz de equilibrar as relações entre indivíduos e agentes econômicos no ecossistema informacional contemporâneo (Nogueira; Oldoni, 2025; Melo, 2025; Castellan, 2023).



## 4 CONSIDERAÇÕES FINAIS

A presente pesquisa partiu da problematização acerca dos limites do consentimento como base legal para o tratamento de dados pessoais no contexto da LGPD, especialmente diante das evidências empíricas e teóricas que demonstram a (des)informação na tomada de decisão no ambiente digital. Ao longo da investigação, verificou-se que, embora o consentimento seja juridicamente reconhecido como mecanismo legítimo de autorização, sua

efetividade material encontra barreiras decorrentes de fatores cognitivos, estruturais e tecnológicos.

Nesse sentido, a análise dos fundamentos jurídicos do consentimento evidenciou uma tensão entre sua validade formal e sua concretização prática, na medida em que os requisitos de liberdade, informação e inequivocidade, embora previstos normativamente, não se realizam plenamente nas interações digitais contemporâneas. A partir da incorporação de evidências da economia comportamental, constatou-se que a tomada de decisão dos usuários é condicionada por vieses cognitivos, sobrecarga informacional e pela arquitetura das escolhas, o que compromete a autonomia decisória e fragiliza a noção de consentimento informado.

Do mesmo modo, a análise comparada entre o modelo brasileiro e o europeu permitiu identificar que, apesar do maior grau de detalhamento normativo e da consolidação institucional do GDPR, as limitações do consentimento não são exclusivas do contexto brasileiro, mas demonstram uma fragilidade estrutural do próprio modelo regulatório centrado na autorização do titular. Assim, conclui-se que o problema do consentimento não se restringe a *déficits* normativos ou institucionais locais, mas constitui um desafio global associado à dinâmica da economia de dados e às formas contemporâneas de interação digital.

Todavia, a pesquisa também demonstrou que tais limitações são intensificadas no contexto brasileiro, em razão de desigualdades estruturais, deficiência de letramento digital e vulnerabilidades informacionais que ampliam a assimetria entre titulares e agentes de tratamento. Nesse contexto, a simples importação de modelos estrangeiros demonstra-se insuficiente, sendo necessária a construção de estratégias regulatórias que considerem as especificidades sociais, econômicas e culturais do país.



Diante disso, conclui-se que o modelo centrado no consentimento apresenta insuficiências relevantes enquanto instrumento de proteção de dados pessoais, exigindo a adoção de abordagens complementares. Entre elas, destacam-se o fortalecimento institucional da ANPD, a ampliação da cooperação com órgãos de defesa do consumidor, a reorientação do foco regulatório para o uso efetivo dos dados, bem como o investimento em políticas de educação digital e inclusão informacional. Ademais, a incorporação de perspectivas críticas, como a decolonial, mostra-se necessárias para a construção de um modelo mais adequado às realidades do Sul Global.

Por fim, como prospecção, aponta-se que futuras investigações podem aprofundar a análise empírica sobre o comportamento dos usuários em contextos específicos, bem como explorar mecanismos regulatórios alternativos que reduzam a dependência do consentimento

como eixo central da proteção de dados. Assim, persiste uma lacuna na literatura quanto à operacionalização jurídica de alternativas ao modelo centrado no consentimento, com vistas à construção de um modelo mais efetivo, equitativo e alinhado às condições reais de tomada de decisão no ambiente digital contemporâneo e sensível às diversidades regionais.

## .REFERÊNCIAS

ABRUSIO, Juliana. The (in)efficacy of consent for the processing of personal data. **Human(ities) and Rights: Global Network Journal**, v. 6, n. 1, 1 set. 2024.

ANDRADE, Amanda Figueiredo de; SIQUEIRA, Jorge Eduardo de Lima; SILVA, José Edson Fortunato da; OLIVEIRA, Naiara Aparecida Pereira de; TEIXEIRA, Rafaela Carrilho; FERREIRA, Rayane Xavier; FERNANDES, Stephany Lyriel; MARTINS, Wellen Chris de Jezus. Privacidade e proteção de dados na era do capitalismo de vigilância. **Revista da Faculdade de Direito de São Bernardo do Campo**, v. 30, n. 2, 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União***: seção 1*, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União***: seção 1*, Brasília, DF, 15 ago. 2018.

CASTELLAN, Felipe Amorim. **Criptografia, direito fundamental à privacidade e deveres fundamentais dos provedores de mensageria privada na persecução penal**. 2023. 138 f. Dissertação (Mestrado em Direitos e Garantias Fundamentais) - Programa de Pós-Graduação em Direitos e Garantias Fundamentais, Faculdade de Direito de Vitória, Vitória, 2023.

COHEN, I. Glenn; SLOTTJE, Andrew.**Artificial intelligence and the law of informed consent.**In: SOLAIMAN, Barry; COHEN, I. Glenn (org.). Research handbook on health, AI and the law. Cheltenham: Edward Elgar Publishing, 2024. p. 167–182.

CORRÊA, Rafael. Danos diluídos e a insuficiência do paradigma da autodeterminação informativa: o desafio da tutela da privacidade na era da *data-driven economy*. **Ânima: Revista Eletrônica do Curso de Direito do Centro Universitário UniOpet,** Curitiba, v. 29, jul./dez. 2023. ISSN: 2175-7119.

COUTO, José Henrique de Oliveira. **Direito fundamental à autodeterminação informativa e a proteção da personalidade nos contratos eletrônicos**. 2024. Dissertação (Mestrado em Direito) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Direito, Uberlândia, 2024.

DINIZ, Giovanna. **A mercantilização dos dados pessoais sob a lente do fetichismo da mercadoria em Marx**. 2025. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2025.

GAIGHER, Enzo Gabriel de Oliveira; PASQUALOTTO, Ionara. Responsabilidade civil das empresas de tecnologia na venda de dados pessoais: aspectos legais e éticos. **Revista científica REMAD.** n.2. 2025.

GERBER, Nina; STÖVER, Alina; MARKY, Karola.**Human factors in privacy research**. Cham: Springer, 2023.

GOMES, Laísa de Lima Fiuza; SOUZA, Salim Silva; DUARTE, Zeny.Inclusão digital no Brasil:

avanços e limites nas políticas contemporâneas. **Revista EDICIC**, San José (Costa Rica), v. 25, e-6026, p. 1–13, 2025.

GREEN, Daniel. Strategic indeterminacy and online privacy policies: (un)informed consent and the General Data Protection Regulation**. International Journal for the Semiotics of Law**, v. 38, p. 701–729, 2025.

JUSTINO, Thais Keila Fernandes de Freitas; TEIXEIRA, Rodrigo Valente Giublin.Os direitos da personalidade do consumidor frente às políticas de privacidade e o termo de uso e a Lei Geral de Proteção de Dados. **Revista Argumentum (RA),** Marília, SP, v. 26, n. 1, p. 65–83, jan./abr. 2025. eISSN: 2359-6889.

LIMA, Gabryel Fraga. A exposição oculta: o uso indevido de imagens e dados pessoais em sites digitais e a fragilidade da privacidade na era da informação. **Revista Científica Di Fatto**, n. 5, 2025. ISSN: 2966-4527.

MARTINI, Mario; DREWS, Christian. **Making choice meaningful: tackling dark patterns in cookie and consent banners through European data privacy law**. Germany: Speyer, 2021.

MEDEIROS, João Marcos Amorim; FELLER, Thiago de Almeida. Análise das questões éticas e legais em torno da privacidade digital. Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE), v. 10, n. 11, p. 662–688, nov. 2024. DOI: https://doi.org/10.51891/rease.v10i11.16492.

MELO, Jonas Ferrigolo. ***Consentimento informado e proteção de dados pessoais: proposta de um modelo de gerenciador de consentimento para plataformas digitais.*** 2025. Tese (Doutorado) Informação e Comunicação em Plataformas Digitais – Fundação para a ciência e a tecnologia: Faculdade de Letras da Universidade do Porto, 2025.

NEVES, Cleuler Barbosa das; MATOS, Gisele Gomes. Microssistema legal brasileiro da "proteção" dos dados pessoais: uma suposta efetiva garantia da titularidade privada dos próprios dados pessoais. **Revista Aracê**, São José dos Pinhais, v. 7, n. 3, p. 10805–10867, 2025.

NOGUEIRA, Ana Carolina de Oliveira Martins; OLDONI, Lisiany Ferrari.**A exclusão digital como novo risco socioambiental**. In: Congresso Constitucionalismo para a Sustentabilidade e Riscos Climáticos. Itajaí: Universidade do Vale do Itajaí (UNIVALI), 2025.

PAIXÃO, Ester Miura Freitas. **Coleta e monetização de dados pessoais na esfera digital: ameaça ao direito à privacidade e à autodeterminação informativa**. 2025. Artigo científico (Trabalho de Curso II) – Escola de Direito, Negócios e Comunicação, Pontifícia Universidade Católica de Goiás, Goiânia, 2025.

PINTO, Yanka dos Santos; FERREIRA, Rafael Fonseca. Vigilância digital: poder e controle sobre a privacidade e os dados pessoais. **Revista FIDES**, *[S. l.]*, v. 15, n. 1, p. 124–145, 2024.

PAULA, Pedro Pontes de. **Violação à privacidade e coleta de dados através de meios eletrônicos: tratar sobre a coleta e uso de dados com ou sem conhecimento.** Artigo científico (Trabalho de Curso II) – Escola de Direito e Relações Internacionais, Pontifícia Universidade Católica de Goiás, Goiânia, 2023.

RAMOS, Paulo Roberto; FIGUEIRÊDO NETO, Acácio; PEREIRA FILHO, Antônio; OLIVEIRA, Flávio José Vieira de; ALVES, Maria Miryam da Silva; ARAÚJO, Heráclitton Neves; OLIVEIRA, Kelma dos Santos Passos; FERREIRA, Rodrigo Almeida; DURANDO, Giovanna Monteiro Cavalcante; SILVA, Marciano Carvalho da; GOMES, Mara Carlota Pereira; SANTOS, Aila de Souza. Justiça cognitiva e biopirataria 2.0: desafios à soberania de comunidades tradicionais do Nordeste do Brasil. **Veredas do Direito**, v. 23, n. 4, e235057, 2026.

SANTOS, Igor Rodrigues; ALVES, Miriam Coutinho de Faria; QUINTINO, Emanuelle Moura. A

vida não é útil, mas os dados pessoais são? O direito fundamental à proteção de dados pessoais à luz dos desafios contemporâneos na economia da informação. **Revista Direitos Culturais**, Santo Ângelo, v. 20, n. 51, p. 93–114, maio/ago. 2025.

SILVA, Amanda Rodrigues da; PAIXÃO, Jayne Knoblauch Binow; LIMA, Teófilo Lourenço de.O Supremo Tribunal Federal e a garantia dos direitos fundamentais: limites e possibilidades da atuação jurisdicional. **Revista Nativa Americana de Ciências, Tecnologia & Inovação**, Ji-Paraná, RO, v. 8, n. 3, p. 42–55, 2025.

SILVA, Marla Souza. **A publicidade por algoritmo e o direito à privacidade nas relações de consumo**. 2024. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Sergipe, Departamento de Direito, São Cristóvão, SE, 2024.

SILVEIRA, João Victor Pires. **Tutela jurídica dos dados pessoais: sob o contexto da sociedade digital**. 2024. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal de Uberlândia, Uberlândia, 2024.

TANEVA, Joanna. Amatas. Do cognitive biases and dark patterns affect the legality of consent under the GDPR? In: **SECURWARE 2022: The Sixteenth International Conference on Emerging Security Information, Systems and Technologies**. Sofia, Bulgaria, 2022.

VASCONCELOS, Marianna Lays Alves de. **Validade do negócio juridico**: oferta direcionada ao consumidor no ambiente virtual a partir do tratamento irregular de dados pessoais. TCC (Graduação) - UFPB/CCJ. João Pessoa, 2024.