Revista Brasileira de Estudos Jurídicos
Centro Universitário FIPMoc
ISSN: 1809-7278 / 2358-9744

CONSENTIMENTO VICIADO NA PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE CRÍTICA À LUZ DA LGPD E DA GDPR

Francielle da Conceição Drumond Figueiredo[1]

RESUMO

O consentimento é a pedra angular da proteção de dados pessoais, refletindo o direito à autodeterminação informativa. No entanto, em um cenário de economia de vigilância e complexidade tecnológica, o consentimento frequentemente se torna "viciado", minando sua eficácia e a autonomia do titular dos dados. Este artigo analisa criticamente a definição e os requisitos do consentimento sob a ótica da Lei Geral de Proteção de Dados (LGPD) e do General Data Protection Regulation (GDPR). Aborda as práticas que levam ao consentimento viciado, seus impactos éticos e legais, e propõe boas práticas e recomendações para aprimorar os mecanismos de obtenção de consentimento, visando fortalecer a proteção dos dados pessoais e a confiança nas relações digitais.

Palavras-chave: Consentimento, Proteção de Dados, Consentimento Viciado, Autodeterminação Informativa.

DEFECTIVE CONSENT IN PERSONAL DATA PROTECTION: A CRITICAL ANALYSIS IN LIGHT OF THE LGPD AND GDPR

ABSTRACT

Consent is the cornerstone of personal data protection, reflecting the right to informational self-determination. However, in a scenario of surveillance economy and technological complexity, consent often becomes "flawed," undermining its effectiveness and the autonomy of the data subject. This article critically analyzes the definition and requirements of consent under the perspective of the General Data

[1] Doutoranda em Direito- Dinter (UFMG/UNIMONTES).Mestre em fundamentos e efetividade do Direito. Pós graduanda em Análise da Criminalidade e Violência no Norte de Minas. Professora universitária. ORCID: http://lattes.cnpq.br/3592680358648153E-mail: frandrumond@yahoo.com.br

Protection Law (LGPD) and the General Data Protection Regulation (GDPR). It addresses practices that lead to flawed consent, their ethical and legal impacts, and proposes best practices and recommendations to improve consent mechanisms, aiming to strengthen personal data protection and trust in digital relationships.

Keywords: Consent, Data Protection, Flawed Consent, Informational Self-Determination.

CONSENTIMIENTO VICIADO EN LA PROTECCIÓN DE DATOS PERSONALES: UN ANÁLISIS CRÍTICO A LA LUZ DE LA LGPD Y LA GDPR

RESUMEN

El consentimiento es la piedra angular de la protección de datos personales, reflejando el derecho a la autodeterminación informativa. Sin embargo, en un escenario de economía de vigilancia y complejidad tecnológica, el consentimiento frecuentemente se torna "viciado", socavando su eficacia y la autonomía del titular de los datos. Este artículo analiza críticamente la definición y los requisitos del consentimiento desde la perspectiva de la Ley General de Protección de Datos (LGPD) y del Reglamento General de Protección de Datos (GDPR). Aborda las prácticas que generan el consentimiento viciado, sus impactos éticos y legales, y propone buenas prácticas y recomendaciones para mejorar los mecanismos de obtención de consentimiento, con el objetivo de fortalecer la protección de los datos personales y la confianza en las relaciones digitales.

Palabras clave: Consentimiento, Protección de Datos, Consentimiento Viciado, Autodeterminación Informativa.

INTRODUÇÃO

A era digital transformou radicalmente a forma como interagimos, consumimos e vivemos. Neste novo cenário, os dados pessoais emergem como um ativo econômico de valor inestimável, impulsionando a chamada "economia da informação" e um modelo de negócios que muitos chamam de "capitalismo de vigilância" (Zuboff, 2018).

A coleta, processamento e compartilhamento massivo de informações sobre indivíduos tornaram-se onipresentes, gerando riqueza para empresas, mas também expondo os titulares a riscos sem precedentes, como a exploração, a discriminação e a restrição da liberdade individual.

Diante deste panorama, a proteção de dados pessoais consolidou-se como um direito fundamental, essencial para salvaguardar a dignidade da pessoa humana na sociedade digital.

Nesse contexto, o consentimento desponta como um dos pilares regulatórios mais relevantes, concebido para empoderar o indivíduo e permitir o controle sobre suas próprias informações.

No entanto, a complexidade e a dinâmica do ambiente digital têm levado a questionamentos sobre a real capacidade do consentimento em cumprir sua função protetiva, frequentemente resultando em um "consentimento viciado".

Este artigo tem como objetivo principal analisar criticamente a definição e os requisitos do consentimento na proteção de dados pessoais, focando nas legislações mais relevantes do cenário global: a Lei Geral de Proteção de Dados (LGPD) do Brasil e o General Data Protection Regulation (GDPR) da União Europeia.

Busca-se identificar as práticas correntes que levam ao que se denomina "consentimento viciado", bem como examinar seus profundos impactos éticos, legais e sociais na autonomia do titular dos dados.

Por fim, propõe-se um conjunto de boas práticas e recomendações, visando aprimorar os mecanismos de obtenção e gestão do consentimento, fortalecendo a proteção de dados pessoais e restaurando a confiança nas relações digitais. A metodologia empregada baseia-se em uma análise bibliográfica aprofundada, com revisão de literatura especializada e legislação pertinente, combinada com uma abordagem crítica das implicações práticas e teóricas do consentimento no ambiente digital contemporâneo.

Fundamentos do Consentimento no Contexto da Proteção de Dados

O consentimento é uma das bases legais mais importantes no tratamento de dados pessoais, sendo essencial para o exercício do direito à privacidade e da autodeterminação informativa. Como expressão da autonomia individual, ele

legitima a coleta, utilização e transferência de informações pessoais, mas também é alvo recorrente de discussões e controvérsias legais, éticas e sociais.

Este tópico explora o conceito de consentimento sob as perspectivas da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral de Proteção de Dados (GDPR), destacando sua definição, atributos essenciais e a relevância de sua aplicação no âmbito da proteção de dados pessoais.

Definição de Consentimento no Contexto da Proteção de Dados

O consentimento, no âmbito da proteção de dados, é a manifestação de vontade do titular dos dados, pela qual ele concorda com o tratamento de suas informações pessoais. Sua essência reside na garantia da autodeterminação informativa, um princípio que assegura ao indivíduo o poder de determinar o fluxo de suas informações na sociedade.

O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, em seu Artigo 4º, item 11, e o considerando 32, define o consentimento como:

> qualquer manifestação de vontade, livre, específica, informada e inequívoca do titular dos dados, pela qual ele manifesta o seu acordo, mediante uma declaração ou um ato positivo inequívoco, em que os dados pessoais que lhe dizem respeito sejam objeto de tratamento." (GDPR, 2019).

De forma análoga, a Lei Geral de Proteção de Dados (LGPD) brasileira, em seu Artigo 5º, inciso XII, estabelece que: "consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada." (LGPD, 2019).

Ambas as definições sublinham a necessidade de que o consentimento seja qualificado por atributos essenciais: livre, informado, específico (ou para "finalidade determinada") e inequívoco (ou "explícito" no GDPR). Estes adjetivos são cruciais para assegurar que a manifestação de vontade do titular seja genuína e não apenas uma formalidade burocrática.

Importância do Consentimento no Tratamento de Dados Pessoais

Historicamente, o consentimento desempenhou um papel central nas leis de proteção de dados, sendo visto como o principal mecanismo para implementar a autodeterminação informativa.

Em suas gerações iniciais, a legislação focava em capacitá-lo com o controle sobre suas informações pessoais, estabelecendo escolhas sobre a coleta, uso e compartilhamento de seus dados (Bioni, 2019).

Sua importância reside em ser uma "mola propulsora" da estrutura da proteção de dados, permeando todo o processo de tratamento. Sem um consentimento válido, muitas atividades de tratamento de dados tornam-se ilícitas, expondo os controladores a sanções e danos reputacionais. (Doneda, 2006, p.216).

O consentimento legitima a coleta, o processamento e a difusão de dados, permitindo que o titular, em tese, determine um maior nível de proteção ou um maior fluxo de suas informações (Mendes, 2014, p.123-124).

> Para que o indivíduo possa exercer o seu papel de autodeterminação informativa, faz-se necessário um instituto jurídico por meio do qual se expresse a sua vontade de autorizar ou não o processamento de dados pessoais: o consentimento. Este é o mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão. (Mendes, p. 60)

No entanto, a dependência excessiva no consentimento também gerou um paradoxo da privacidade, onde, apesar de valorizarem sua privacidade, as pessoas frequentemente realizam ações que contradizem essa valorização.

Este dilema sublinha a fragilidade do consentimento como ferramenta única e absoluta na proteção de dados, especialmente quando confrontado com a complexidade da economia digital (Mendes, 2014, p.39).

Demonstra-se aqui uma controvérsia: a efetividade do consentimento do cidadão e o real exercício de liberdade de escolha.

Conforme explica Schertel, há três principais perspectivas sobre a natureza jurídica do consentimento no tratamento de dados pessoais: i) a primeira defende

que o consentimento possui a natureza de uma declaração de vontade com caráter negocial; ii) a segunda sustenta que se trata de um ato jurídico unilateral, desprovido de natureza negocial; e iii) a terceira interpreta o consentimento como um ato que guarda semelhanças com um negócio jurídico, mas que não pode ser considerado propriamente como tal. (Mendes, 2014, p. 62).

Danilo Doneda argumenta que não é adequado conferir ao consentimento uma natureza negocial, uma vez que ele está diretamente relacionado a elementos da personalidade, mas não implica a disposição desses elementos. (Doneda, 2006, p.377).

De acordo com ele, tratar o consentimento como um instrumento de natureza contratual seria enquadrá-lo dentro de uma lógica puramente patrimonial. Isso poderia levar à aplicação de esquemas baseados na propriedade para o tratamento de dados pessoais, o que acabaria limitando e dificultando a proteção efetiva dos atributos inerentes à personalidade.

Consentimento na LGPD e GDPR: Abordagens e Implicações

O consentimento, enquanto base legal essencial para o tratamento de dados pessoais, é abordado de forma detalhada e criteriosa tanto pela Lei Geral de Proteção de Dados (LGPD) quanto pelo Regulamento Geral de Proteção de Dados (GDPR).

Ambas as legislações elevam o consentimento a um padrão rigoroso, reconhecendo sua importância para a autodeterminação informativa e a proteção da privacidade. No entanto, ao mesmo tempo em que estabelecem atributos indispensáveis para a validade do consentimento — como liberdade, informação e especificidade —, também reconhecem suas limitações em um cenário de crescente complexidade tecnológica.

Este tópico analisa comparativamente como a LGPD e o GDPR disciplinam o consentimento, destacando suas semelhanças, diferenças e implicações práticas

para garantir um equilíbrio entre os interesses dos titulares dos dados e as necessidades do mercado digital.

Discussão sobre a LGPD e sua Aplicação no Contexto do Consentimento

As legislações de proteção de dados mais modernas, como a LGPD e a GDPR, reconhecem o consentimento como um direito fundamental, mas também tentam equilibrar sua importância com outras bases legais e mecanismos de proteção, buscando uma abordagem mais realista e eficaz para os desafios da era digital.

A LGPD, Lei nº 13.709/2018, posiciona o consentimento como um dos pilares da proteção de dados no Brasil. Embora não seja a única base legal para o tratamento de dados (Art. 7º lista outras nove hipóteses), sua "adjetivação" detalhada revela a preocupação do legislador brasileiro em assegurar a autonomia e o controle do titular. O consentimento, conforme o Art. 5º, XII, deve ser livre, informado e inequívoco, e para uma finalidade determinada.

O consentimento livre implica que o titular deve ter a opção real de aceitar ou recusar o tratamento, sem coerção ou prejuízo significativo em caso de recusa. A LGPD busca ir além da lógica do "tudo ou nada" (take it or leave it), incentivando o que se chama de "granularidade" do consentimento, ou seja, a possibilidade de optar por autorizar seções específicas do tratamento, sem ter que aceitar um pacote completo. O Art. 9º, §3º, da LGPD, ao falar em granularidade, é um exemplo disso (Bioni, 2019).

O consentimento informado no art. 9º da LGPD exige que as informações sejam claras, adequadas e ostensivas, detalhando a finalidade específica do tratamento, forma e duração, identificação do controlador, seus contatos, e os direitos do titular. Esta transparência é vital para que o titular tome uma decisão consciente. A ausência de clareza ou conteúdo enganoso torna o consentimento nulo (Art. 9º, §1º).

A LGPD requer que não haja dúvidas sobre a intenção do titular em autorizar o tratamento. Isso implica uma manifestação ativa, não bastando a inação ou o

silêncio. Como Bruno Bioni aponta, isso se alinha com a ideia de comportamentos concludentes que não deixem dúvidas sobre a vontade do cidadão (Bioni, 2019).

O tratamento de dados deve estar atrelado a uma finalidade determinada e a propósitos legítimos, específicos e explícitos, previamente informados ao titular (Art. 6º, I). Isso impede o "cheque em branco" para o uso irrestrito de dados, garantindo que o tratamento seja compatível com o que foi inicialmente consentido.

A LGPD também enfatiza a revogabilidade do consentimento, permitindo que o titular retire sua permissão a qualquer momento, de forma fácil e gratuita (Art. 9º, §5º). Esta previsão é crucial para o exercício contínuo da autodeterminação informativa.

Além do consentimento, a LGPD prevê outras bases legais para o tratamento de dados (Art. 7º), como o cumprimento de obrigação legal, execução de contrato, pesquisa, e o legítimo interesse do controlador ou de terceiro (Art. 7º, IX).

O legítimo interesse, embora flexibilize a necessidade do consentimento, é balizado por princípios como as "legítimas expectativas do titular" (Art. 10º, §1º), transparência e minimização dos dados, buscando um equilíbrio entre os interesses comerciais e os direitos dos indivíduos.

Análise da GDPR e suas Implicações para o Consentimento

O GDPR (Regulamento (UE) 2016/679) é uma das legislações mais robustas e influentes sobre proteção de dados no mundo, servindo de inspiração para a LGPD. Ele eleva o consentimento a um padrão rigoroso, com foco na transparência e no empoderamento do titular dos dados.

A definição de consentimento no GDPR (Art. 4º, item 11, e Recital 32) exige que seja livre, específico, informado e inequívoco, com a adição do termo "explícito" em certos contextos.

O GDPR enfatiza que o consentimento não pode ser uma condição para a prestação de um serviço se o processamento de dados não for estritamente necessário para esse serviço (Recital 43). Em situações de desequilíbrio de poder,

como na relação empregador-empregado, o consentimento é presumido como não livre. (Breen , Ouazzane , Patel, 2020).

O consentimento deve ser dado para finalidades claramente delimitadas. Se houver múltiplas finalidades, o consentimento deve ser dado para cada uma delas, não sendo válidas autorizações genéricas (Recital 32).

A identidade do controlador, as finalidades do tratamento, os tipos de dados coletados, os destinatários, os direitos do titular e as consequências da recusa devem ser comunicados de forma concisa, transparente, inteligível e de fácil acesso, utilizando linguagem clara e simples (Recital 42, Art. 13 e 14).

O GDPR exige um "ato positivo inequívoco", descartando boxes pré-selecionados, silêncio ou inatividade como formas de consentimento válido (Recital 32). Para dados sensíveis, o consentimento deve ser "explícito", impondo um padrão ainda mais elevado de clareza e formalidade.

O GDPR também exige que o consentimento seja *auditable,* ou seja, que o controlador possa demonstrar que o consentimento foi obtido de forma válida (Recital 42). Além disso, a retirada do consentimento deve ser tão fácil quanto a sua concessão (Art. 7º, §3º).

Assim como a LGPD, o GDPR prevê outras bases legais para o tratamento de dados (Art. 6º), sendo o legítimo interesse (Art. 6º, §1º, alínea f) uma das mais flexíveis. No entanto, sua aplicação é condicionada a uma "avaliação cuidadosa", considerando as "expectativas razoáveis dos titulares dos dados" e a ausência de prevalência dos seus direitos e liberdades fundamentais (Recital 47).

Consentimento Viciado e suas Implicações

Apesar dos requisitos rigorosos estabelecidos pela LGPD e GDPR, a complexidade do ambiente digital e as estratégias de negócios baseadas em dados frequentemente resultam em práticas que levam ao "consentimento viciado". Este termo refere-se a uma manifestação de vontade que, embora possa parecer formalmente válida, não atende aos critérios de ser livre, informado, específico e inequívoco, minando a autonomia real do titular dos dados.

O consentimento pode ser considerado viciado quando os seus elementos essenciais são comprometidos, seja por falhas na informação, por coação, ou por uma falsa percepção de escolha. Algumas práticas comuns incluem:

Empresas frequentemente apresentam termos de uso e políticas de privacidade extensos, cheios de jargões jurídicos e técnicos, que a maioria dos usuários não lê nem compreende. Quando o usuário clica "aceito" sem entender, o consentimento é formal, mas não informado. (Solove, 2013).

Muitos serviços online exigem que o usuário aceite integralmente os termos de tratamento de dados para ter acesso ao serviço. A recusa implica na impossibilidade de usar o serviço, o que, para muitos, equivale a uma forma de coerção, especialmente se o serviço é essencial para a socialização ou o trabalho. Neste cenário, o consentimento não é verdadeiramente livre.

Algumas plataformas utilizam caixas de seleção pré-marcadas, assumindo o consentimento do usuário a menos que ele as desmarque. O GDPR proíbe explicitamente essa prática, exigindo um "ato positivo inequívoco" (Recital 32). A falta de uma ação afirmativa torna o consentimento ambíguo e, portanto, inválido. (GDPR, 2019).

Quando as finalidades para o tratamento de dados são vagas ("para melhorar sua experiência") ou são alteradas substancialmente sem novo consentimento, o consentimento original torna-se viciado por não ser específico ou determinado. O uso de dados genéticos para fins securitários ou o monitoramento de funcionários sem delimitação clara de propósito são exemplos de como a finalidade pode ser distorcida (Bioni, 2019).

A grande maioria dos usuários não possui o conhecimento técnico para entender como seus dados são coletados, processados e compartilhados por uma miríade de "third parties" e "data brokers". Esta assimetria torna difícil para o usuário tomar decisões informadas e genuinamente livres. (Pasquale, 2017).

Essas práticas evidenciam como o consentimento pode ser facilmente desvirtuado em um ambiente de crescente complexidade tecnológica e assimetria informacional entre empresas e titulares de dados.

Quando o consentimento não é genuíno, mas apenas uma formalidade burocrática que mascara a falta de escolha, ele deixa de cumprir seu propósito de proteger a autodeterminação informativa do indivíduo.

É essencial que regulamentações como a LGPD e o GDPR sirvam não apenas para coibir essas práticas, mas também para incentivar mecanismos mais transparentes, acessíveis e efetivos de obtenção de consentimento.

Dessa forma, busca-se restabelecer o equilíbrio nas relações digitais, garantindo que o titular dos dados tenha controle real sobre suas informações pessoais e possa tomar decisões informadas, livres e específicas.

Impacto do Consentimento Viciado na Proteção de Dados Pessoais

O consentimento viciado tem implicações profundas, tanto éticas quanto legais, que desvirtuam o propósito da proteção de dados pessoais. A principal consequência ética é a erosão da autonomia do indivíduo. Quando o consentimento não é livre nem informado, a pessoa perde a capacidade de controlar sua própria narrativa digital e de tomar decisões conscientes sobre sua vida. Isso pode levar à manipulação de comportamento, à formação de "perfis comportamentais" que não correspondem à realidade e à estigmatização, afetando o livre desenvolvimento da personalidade. A confiança nas relações digitais é minada, e a sociedade pode caminhar para uma "ditadura dos dados". (Bioni, p.122-123).

Quanto as implicações legais, o consentimento viciado invalida o tratamento de dados pessoais, tornando-o ilícito. Isso pode resultar em sanções e multas, além da imposição de ações reparadores, ou seja, os titulares de dados podem buscar indenização por danos materiais e morais resultantes do tratamento ilícito de seus dados.

Boas Práticas para o Consentimento

Para combater o consentimento viciado e garantir que ele cumpra seu papel de salvaguarda da autonomia do titular, é fundamental adotar e implementar boas

práticas que promovam clareza, transparência e mecanismos eficazes de obtenção e gestão do consentimento.

A clareza e a transparência são requisitos fundamentais para um consentimento informado e válido, conforme exigido tanto pela LGPD (Art. 9º) quanto pelo GDPR (Art. 13 e 14).

As informações sobre o tratamento de dados devem ser apresentadas em linguagem simples, direta e de fácil compreensão para o público em geral, evitando termos excessivamente técnicos ou jurídicos. Em vez de longos textos, priorizar a concisão e a objetividade. Utilizar frases curtas e diretas para explicar o que será feito com os dados.

Bruno Bioni sugere a utilização de ícones, infográficos e dashboards que visualizem de forma clara os tipos de dados coletados, as finalidades do tratamento e os terceiros envolvidos. (Bioni, p. 246), além de explicitar de forma transparente quais serão as consequências da não concessão do consentimento, para que a decisão seja livre e informada.

Além disso é necessário informar os titulares de forma proativa sobre quaisquer alterações significativas nas finalidades ou métodos de tratamento de dados, solicitando novo consentimento quando necessário.

Integrar a proteção de dados nas fases iniciais de desenvolvimento de produtos e serviços, garantindo que os sistemas e processos sejam projetados para proteger a privacidade dos usuários (Art. 46, §2º da LGPD; Art. 25 do GDPR). A privacidade não deve ser um recurso adicional, mas um elemento fundamental do design.

Definir as configurações mais protetivas da privacidade como padrão (privacy by default), exigindo uma ação afirmativa do usuário para relaxar essas configurações. Isso garante que a privacidade seja protegida mesmo para usuários menos engajados.

Acrescente-se que o processo de retirada do consentimento deve ser tão fácil e acessível quanto o de concessão. Botões de "cancelar consentimento" ou "excluir dados" devem estar visíveis e funcionar de forma imediata. A retirada do

consentimento não deve resultar em desvantagens desproporcionais para o titular, exceto quando o tratamento dos dados seja intrínseco à prestação do serviço.

Outro ponto importante é o investimento em programas de educação digital para aumentar a conscientização dos usuários sobre os riscos e as melhores práticas de proteção de dados. Disseminar o conhecimento sobre as ferramentas e direitos disponíveis, para que os usuários possam exercer sua autodeterminação informativa de forma mais eficaz.

CONSIDERAÇÕES FINAIS

A análise do consentimento na proteção de dados pessoais sob a perspectiva da LGPD e da GDPR revela um cenário de avanços legislativos, mas também de desafios persistentes no contexto da economia digital. O consentimento, embora fundamental para o direito à autodeterminação informativa, está frequentemente sujeito a vícios que comprometem a autonomia e a privacidade dos titulares.

O consentimento, quando livre, informado, específico e inequívoco, é uma ferramenta poderosa para a proteção de dados pessoais, refletindo a capacidade do indivíduo de controlar suas informações. Tanto a LGPD quanto o GDPR estabelecem padrões elevados para a sua validade, exigindo transparência, clareza e facilidade na gestão do consentimento.

No entanto, a realidade do ambiente digital, marcada pela "economia da vigilância" e pela complexidade das tecnologias de tratamento de dados expõe o consentimento a múltiplos vícios. A assimetria informacional e de poder entre controladores e titulares, as políticas de privacidade obscuras, os mecanismos "take it or leave it" e a falta de granularidade das opções de consentimento contribuem para um "paradoxo da privacidade", onde a vontade do titular é formalmente expressa, mas substancialmente comprometida.

As implicações do consentimento viciado são vastas, abrangendo desde a erosão da autonomia individual e a manipulação de comportamentos até as severas sanções legais impostas por autoridades de proteção de dados. Isso demonstra a

necessidade de uma abordagem mais abrangente que transcenda a mera formalidade do consentimento, integrando-o a um contexto mais amplo de ética e responsabilidade.

Para aprimorar a eficácia do consentimento e garantir uma proteção de dados pessoais robusta, são necessárias ações coordenadas em diferentes frentes.

As autoridades de proteção de dados (ANPD, DPAs europeias) devem emitir diretrizes detalhadas e exemplos práticos sobre como implementar um consentimento válido, especialmente em cenários complexos.

A fiscalização deve ser proativa e rigorosa, aplicando sanções proporcionais e educativas para desencorajar práticas de consentimento viciado. Deve-se ainda incentivar regularmente a implementação de mecanismos de consentimento granular, oferecendo opções detalhadas ao usuário para cada finalidade de tratamento.

Empresas devem incorporar a proteção de dados desde a concepção de seus produtos e serviços. Isso significa que as configurações mais protetivas devem ser o padrão, e a privacidade deve ser uma funcionalidade central, não um anexo.

As organizações devem demonstrar proativamente a conformidade com as leis de proteção de dados, implementando medidas técnicas e organizacionais adequadas e documentando seus processos de gestão de consentimento.

Ao abraçar essas recomendações, a LGPD e a GDPR podem transcender a mera formalidade do consentimento, garantindo que ele seja uma expressão genuína da vontade do titular e um instrumento eficaz para a proteção de dados pessoais em um mundo cada vez mais digitalizado. O desafio é complexo, mas a busca por um consentimento que seja verdadeiramente livre, informado e autêntico é essencial para construir uma sociedade digital mais justa, transparente e respeitosa dos direitos fundamentais.

REFERÊNCIAS

BIONI, Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro.Editora Forense, 2019.

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.

BREEN Stephen , OUAZZANE Karim , PATEL Preeti. **GDPR**: Is your consent valid? 2020. p. 19-24. Disponível em:https://www.researchgate.net/publication/339320664_GDPR_Is_your_consent_valid. Acesso: 31.out.2025.

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

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

PASQUALE, Frank. **The Dark Market for Personal Data**. Disponível em: <https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html> Acesso em 31. Out. 2025.

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

SOLOVE, DJ. **Privacy self-management and the consent dilemma**. Harvard Law Review 126: 1880–1903. Disponível em: https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-theconsent-dilemma/ 2013. Acesso: 01. Nov.2025

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, 4 maio 2016. Disponível em: eur-lex.europa.eu. Acesso em: 28. Out.2025.

ZUBOFF, Shoshana. **Big Other**: capitalismo de vigilância e perspectivas para uma civilização de informação. Trad. Antonio Holzmeister Oswaldo Cruz e Bruno Cardoso. In BRUNO, Fernanda (org.). Tecnopolíticas da vigilância: perspectivas da margem. 1 ed. São Paulo: Boitempo, 2018. p. 151-180.