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

doi.org/10.51891/rease.v11i4.18862

A LGPD E O VÍCIO DE CONSENTIMENTO: PROTEGENDO OS DADOS PESSOAIS EM AMBIENTES VIRTUAIS

THE BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD) AND CONSENT VULNERABILITIES: PROTECTING PERSONAL DATA IN VIRTUAL PLATFORMS

Aline de Jesus Batista[1]
Karine Alves Gonçalves Mota[2]

RESUMO: A crescente digitalização das interações sociais e comerciais impulsionou a coleta massiva de dados pessoais por plataformas digitais, trazendo à tona preocupações relevantes sobre a validade do consentimento fornecido pelos usuários. A Lei Geral de Proteção de Dados Pessoais (LGPD) surgiu como resposta normativa a esse cenário, instituindo o consentimento como uma das principais bases legais para o tratamento de dados. No entanto, a obtenção deste consentimento nem sempre ocorre de forma livre, informada e inequívoca, sendo muitas vezes comprometida por vícios como engano, coação ou falta de clareza nas interfaces digitais. Este artigo analisa o conceito de vício de consentimento sob a ótica do Direito Civil e sua aplicação no contexto da LGPD, destacando as estratégias utilizadas pelas plataformas para obtenção de dados e as consequências jurídicas da violação dos direitos dos titulares. A metodologia utilizada baseia-se em revisão bibliográfica e documental, visando contribuir para uma compreensão crítica das fragilidades na efetivação do consentimento digital e a importância do fortalecimento de mecanismos de governança e transparência no tratamento de dados pessoais.

Palavras-chave: LGPD. Vício de consentimento. Dados pessoais. Plataformas digitais. Proteção de dados.

ABSTRACT: The increasing digitalization of social and commercial interactions has led to the large-scale collection of personal data by digital platforms, thereby intensifying concerns regarding the validity of user consent. The Brazilian General Data Protection Law (LGPD) was enacted as a regulatory response to this context, establishing consent as one of the primary legal grounds for personal data processing. Nonetheless, the acquisition of consent is not always conducted in a manner that is free, informed, and unambiguous, often being compromised by defects such as misinformation, coercion, or lack of transparency in digital interfaces. This article examines the notion of defective consent under Civil Law and its implications within the framework of the LGPD. It further explores the strategies employed by platforms to obtain personal data and the legal repercussions arising from violations of data subjects' rights. The study adopts a qualitative methodology, grounded in bibliographic and documentary research, with the aim of fostering a critical understanding of the structural vulnerabilities in digital consent mechanisms and emphasizing the need to enhance governance and transparency in personal data processing.

Keywords: Brazilian General Data Protection Law (LGPD). Defective consent. Personal data. Digital platforms. Data governance.

[1]Acadêmica de Direto da Universidade Estadual do Tocantins (UNITINS). Graduada em Comunicação Social - Jornalismo pela Universidade Federal do Tocantins (UFT).
[2]Doutora em Ciências pela Universidade de São Paulo. Mestre em Direito pela UNIMAR. Professora de Direito da Universidade Estadual do Tocantins (UNITINS). Lattes: http://lattes.cnpq.br/4370194488852160. ORCID: https://orcid.org/0000-0002-6820-470X.

INTRODUÇÃO

O avanço das plataformas digitais tem ampliado significativamente a coleta de dados pessoais, tornando essencial uma atenção redobrada quanto ao tratamento e à proteção dessas informações. Nesse cenário, a Lei Geral de Proteção de Dados (LGPD) foi criada para normatizar o tratamento de dados e proteger direitos dos titulares, com realce para exigência do consentimento livre, informado e claro. Porém, nem sempre o consentimento é pego de forma certa; há vezes em que ele é falso por ações ingênuas ou mudança de visuais.

Este trabalho analisa o vício de consentimento na coleta de dados em ambientes virtuais, com fundamento na Lei Geral de Proteção de Dados (LGPD), levando em conta tanto as bases legais que sustentam esse tratamento quanto as práticas utilizadas pelas plataformas digitais. O objetivo principal é compreender como a legislação brasileira regula o consentimento e suas possíveis falhas, bem como as consequências jurídicas em casos de violação.

A pesquisa se justifica pela crescente exposição dos usuários a riscos digitais e pela necessidade de fortalecer os mecanismos de proteção de dados. Para isso, adota-se como metodologia a revisão bibliográfica e documental, com análise da legislação, da doutrina e de casos práticos envolvendo sanções aplicadas pela ANPD e condenações judiciais relacionadas a falhas na coleta e gestão desses dados.

1. CONSENTIMENTO E VÍCIO DE CONSENTIMENTO: CONCEITOS NA LGPD E NO DIREITO CIVIL

1.1 CONSENTIMENTO NA LGPD

A Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018,), define que o consentimento do titular é condição legal para o tratamento de dados pessoais pelas empresas. A obrigação consta no artigo 5º, inciso XII, que estabelece que o consentimento deve ser uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"(Brasil, 2018). Ou seja, é absolutamente necessário que o consentimento seja consciente, espontâneo e bem informado, dando a pessoa que que autoriza o uso de seus dados a total autonomia.

Bioni (2019) ressalta a importância de considerar o poder de negociação do indivíduo no tratamento de seus dados pessoais. Segundo o autor, o titular deve dispor de alternativas claras quanto aos dados que serão coletados e suas finalidades. Ele enfatiza a necessidade de se

observar o equilíbrio entre o poder de barganha do cidadão e as práticas adotadas pelas empresas ou entidades responsáveis por esse tratamento.

Além disso, o inciso I do artigo 7º da LGPD reforça que o tratamento de dados pessoais só é permitido quando o titular der seu consentimento de forma expressa, livre e informada. Isso garante que a pessoa compreenda, em absoluto, como suas informações serão usadas pelos sites e demais plataformas online. Outro ponto relevante trazido pelo artigo é que o consentimento precisa ser específico para cada finalidade. Ou seja, consentimentos não podem ser aproveitados em outros contextos além daquela expressamente acordado. Nesse sentido, devem ser evitadas autorizações amplas ou genéricas, que prejudicam a transparência e a autonomia do titular sobre seus próprios dados.

Sobre a temática, Maria Helena Diniz defende que "O consentimento do titular dos dados deve ser fornecido de forma livre, informada e inequívoca, para finalidades específicas, e não para finalidades genéricas ou vagas" (2019, p. 128). Esclarece ainda que o consentimento deve ser obtido de uma forma clara, onde o titular tenha total consciência do que está permitindo e sem pressões por parte de quem quer obtê-la. A autora enfatiza a importância do titular ser informado sobre a destinação específica dos dados coletados, evitando dessa forma que seja utilizada de maneira muito ampla ou ainda indefinida. Dessa forma é dada ao indivíduo maior transparência e controle sobre o uso de seus dados pessoais.

A assertiva de que o consentimento deve ser fornecido para propósitos específicos é reforçada pela Lei em seu artigo 9º parágrafos 1º e 2º,

> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
>
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações" (Brasil, 2018).

Esses dispositivos visam garantir que o consentimento seja sempre dado de forma esclarecida, sem manipulações ou omissões, o que assegura maior previsibilidade e proteção ao titular dos dados, impedindo práticas abusivas e promovendo a transparência no tratamento das informações pessoais.

Por fim, o artigo 10º estabelece que, mesmo quando o tratamento não se baseia no consentimento, deve-se atender às finalidades lícitas, legítimas e específicas, com fundamento

em uma das bases legais previstas na legislação. Isso evidencia que o consentimento é apenas um dos mecanismos de legalidade para o tratamento de dados, devendo coexistir com outros fundamentos jurídicos, dependendo do contexto.

Dessa forma, a LGPD busca garantir que o consentimento seja utilizado de forma transparente, informada e direcionada a propósitos legítimos, conferindo ao titular dos dados um papel central na gestão de suas informações pessoais.

1.2 O VÍCIO DO CONSENTIMENTO NO CÓDIGO CIVIL

Já a Lei n.º 10.406/2002, o Código Civil brasileiro, estabelece que o consentimento é um dos elementos essenciais para a validade dos negócios jurídicos. Entretanto, há situações em que esse consentimento pode ser viciado, comprometendo a validade do ato.

Conforme afirmam Cristiano Chaves de Farias e Nelson Rosenvald (2021, p. 731), os vícios de consentimento nos negócios jurídicos ocorrem quando a manifestação de vontade do agente não reflete sua real intenção. Nesse contexto, há uma distorção entre a vontade expressa e o verdadeiro desejo do declarante, o que compromete a validade do ato jurídico.

O artigo 171 do Código Civil estabelece que o negócio jurídico pode ser anulado em situações que envolvem vícios, além das hipóteses expressamente previstas na legislação. O inciso II deste artigo especifica que a anulação ocorre quando há "vício resultante de erro, dolo, coação, estado de perigo, lesão ou fraude contra credores" (Brasil, 2002). Assim, a anulação é aplicada quando a manifestação de vontade do agente é viciada por essas circunstâncias, prejudicando a liberdade de decisão.

O erro ocorre quando a manifestação de vontade é afetada por uma falsa percepção relevante, que uma pessoa atenta e razoável, diante das circunstâncias do negócio, seria capaz de identificar. Para que esse erro tenha relevância jurídica, ele deve ser substancial e perceptível por alguém com um nível comum de diligência, conforme estabelece o artigo 138 do Código Civil.

Já o dolo, previsto no artigo 145 do mesmo diploma legal, torna o negócio jurídico anulável somente quando for a causa determinante da sua realização. Trata-se de uma conduta intencional de uma das partes com o objetivo de induzir a outra em erro, visando obter vantagem indevida.

O artigo 151 trata da coação, definindo que, para haver vício na declaração de vontade, a ameaça deve ser suficientemente grave a ponto de gerar na vítima um temor fundado de dano

iminente e relevante à sua pessoa, família ou bens. A coação, portanto, precisa ser intensa o bastante para comprometer a liberdade de decisão do indivíduo.

O estado de perigo é abordado no artigo 156, segundo o qual "configura-se estado de perigo quando alguém, premido da necessidade de salvar-se, ou a pessoa de sua família, de grave dano conhecido pela outra parte, assume obrigação excessivamente onerosa"(Brasil, 2002). Esse dispositivo protege aqueles que, em situação de vulnerabilidade, assumem compromissos desproporcionais para evitar um mal maior.

A lesão é tratada no artigo 157, que define que ocorre quando uma pessoa, em situação de necessidade urgente ou por inexperiência, se obriga a uma prestação claramente desproporcional ao valor da obrigação oposta. Assim, a lei visa proteger aqueles que firmam contratos desvantajosos devido à sua falta de experiência ou a uma necessidade extrema.

Por fim, o artigo 158 trata da fraude contra credores e estabelece que "os negócios de disposição gratuita serão nulos, e os onerosos, anuláveis, quando praticados por devedor já insolvente, ou por eles reduzidos à insolvência"(Brasil, 2002). Esse dispositivo visa proteger os credores contra atos que prejudiquem a satisfação de seus créditos.

Segundo Venosa, "Esses vícios afetam a vontade intrínseca do agente e a manifestação de vontade é viciada. Se não existisse uma dessas determinantes, o declarante teria agido de outro modo ou talvez nem mesmo realizado o negócio " (2023, p. 729).

Esse entendimento ressalta que, independentemente da natureza do vício, o aspecto central é a limitação da liberdade do agente no momento da manifestação de sua vontade. Quando essa liberdade é comprometida, o ato jurídico deixa de refletir a real intenção da parte, tornando-se inválido. Nessa hipótese, sua anulação é justificada como forma de proteger o sujeito lesado e garantir a integridade das relações jurídicas.

Dessa forma, o Código Civil busca garantir que a autonomia privada seja exercida de maneira livre e consciente, evitando que negócios jurídicos sejam celebrados sob vícios que comprometam sua validade.

1.3 A RELAÇÃO ENTRE O CONSENTIMENTO NA LGPD E O VÍCIO DO CONSENTIMENTO NO CÓDIGO CIVIL

O consentimento é um elemento fundamental tanto para a validade dos negócios jurídicos, conforme estabelece o Código Civil, quanto para o tratamento de dados pessoais, nos

termos da Lei Geral de Proteção de Dados (LGPD). No ambiente digital, entretanto, diversas práticas comprometem a autenticidade desse consentimento, levando o usuário ao erro.

A LGPD determina que o consentimento deve ser livre, informado e inequívoco. Contudo, recursos como interfaces enganosas (*dark patterns*), uso excessivo de linguagem técnica e a falta de transparência quanto ao uso dos dados dificultam a compreensão efetiva por parte do titular. Um exemplo frequente é a exigência de um consentimento abrangente para acessar serviços essenciais, sem que seja oferecida ao usuário uma escolha real.

O Código Civil, por sua vez, trata do vício de consentimento nas situações de erro, dolo, coação, estado de perigo, lesão ou fraude. No contexto digital, o erro ocorre quando o usuário consente sem compreender adequadamente as consequências, seja pela ausência de informações claras, seja por conteúdo enganoso. O dolo se caracteriza pela ocultação de informações relevantes ou pela criação de obstáculos à revogação do consentimento. A coação, por outro lado, pode ocorrer quando a aceitação dos termos se torna uma exigência para o acesso a serviços básicos, sem alternativas viáveis.

Existe, portanto, uma convergência entre a LGPD e o Código Civil quanto à necessidade de que a manifestação de vontade do titular seja genuína e livre de interferências indevidas. O consentimento obtido por meio de pressão, omissão ou manipulação pode ser considerado viciado, comprometendo sua validade tanto na esfera civil quanto no âmbito da proteção de dados. É nesse sentido que se posicionam Verbicaro e Vieira

> No ambiente virtual, o dever de informar faz parte do rol de deveres mais relevantes para a relação de consumo. Pelas próprias características do ciberespaço, em razão de sua natureza despersonalizada, a informação é o principal instrumento para a realização do negócio. (Verbicaro, Vieira, 2021, p. 8)

Dessa forma, a LGPD e o Código Civil se complementam na proteção da autonomia da vontade, assegurando que a declaração de consentimento seja resultado de uma escolha consciente e livre de manipulações.

2. PRESSÕES DAS EMPRESAS PARA OBTER CONSENTIMENTO E A DESTINAÇÃO DOS DADOS PESSOAIS

O consentimento para o tratamento de dados pessoais no ambiente digital constitui um dos pilares fundamentais da Lei Geral de Proteção de Dados (LGPD). No entanto, na prática, observa-se que diversas plataformas digitais recorrem a estratégias artificiosas e técnicas maliciosas com o objetivo de obter esse consentimento de forma forçada ou dissimulada. Nessas situações, o usuário é levado a fornecer seus dados sem plena compreensão quanto à

finalidade e ao uso futuro dessas informações. Este capítulo tem como objetivo analisar as principais táticas adotadas pelas empresas para coletar dados pessoais a qualquer custo, bem como examinar a destinação que é dada a esses dados no contexto das relações digitais.

2.1 PRÁTICAS DE COLETA DE DADOS FORÇADA

Diversas plataformas digitais adotam práticas que dificultam o acesso ou a navegação nos serviços oferecidos sem que o usuário forneça consentimento para a coleta de seus dados pessoais. Um dos recursos mais utilizados é o emprego de cookies, que são pequenos arquivos armazenados no dispositivo do usuário com a finalidade de monitorar sua atividade online. Segundo Manuela Genovese Pedro (2021), as plataformas utilizam esses cookies, em conjunto com algoritmos, para ampliar a coleta de dados, inclusive rastreando a navegação do usuário em sites concorrentes. Essa estratégia permite o enriquecimento das bases de dados e favorece a captação de publicidade direcionada.

Embora a lei não mencione a nomenclatura *cookies* especificamente, por se tratar de uma ferramenta que pode coletar dados, qualquer política de *cookies* oferecida pelo provedor ao usuário, deve estar em conformidade com a LGPD.

Segundo a orientação da Agência Nacional de Proteção de Dados, os *banners* de *cookies* devem ser utilizados no ambiente digital, como um meio de concretizar os princípios presentes na LGPD, especialmente os da transparência e do livre acesso. Os *banners* devem servir para apresentar informações essenciais de forma resumida e simplificada, auxiliando os titulares na tomada de decisões conscientes sobre o uso de seus dados. Além disso, também foram pensados para fortalecer o controle dos usuários sobre suas informações pessoais e garantir o respeito às suas expectativas legítimas, promovendo assim maior transparência, devendo estar em conformidade com os princípios da proteção de dados. (Brasil, 2022)

Outra ferramenta também utilizada por algumas empresas de forma abusiva é a chamada técnica do *paywall*, onde o acesso a informações e serviços só é permitido após um pagamento. Em uma tradução livre e quase literal, o *paywall* em um site representa um "muro de pagamento", que só pode ser ultrapassado após o usuário se tornar cliente e efetuar o pagamento para ter acesso ao conteúdo. Essa aplicação é amplamente utilizada por portais de notícias, que, de forma legal, cobram pelo acesso a suas notícias. (Almeida, 2013). Ocorre que muitos sites têm se utilizado desse artifício para forçar o consentimento do usuário, obrigando-

o a se cadastrar, sem oferecer outra alternativa. Assim, caso o usuário se negue a fornecer seus dados pessoais, ele não terá acesso ao conteúdo do site desejado. Para Manuela Genovese Pedro

> Assim, a permuta é uma maneira comum pela qual os consumidores "pagam" pelos serviços digitais: eles oferecem sua privacidade e suas informações pessoais que interessem ao servidor em troca dos serviços disponibilizados pela tecnologia. Dessa maneira, a plataforma vende publicidade personalizada e direcionada que se torna ainda mais valiosa com os dados advindos dessa permuta, o que é viável devido, muitas vezes, a possibilidade de venda desses dados sem sua necessária renúncia pelo vendedor, tendo em vista os dados serem não-rivais e não-exclusivos: seu consumo por uma pessoa não reduz a quantidade disponível desse bem para o restante da sociedade. (Pedro, 2021, p.18)

É importante ressaltar que a discussão não gira em torno de sites que cobram para que o usuário tenha acesso ao seu conteúdo exclusivo, mas sim do uso dessa técnica para obrigar o usuário a fornecer seus dados pessoais, para ter acesso ao conteúdo da página.

Tais práticas suscitam importantes debates sobre a ética empresarial e a real efetividade das normas vigentes na proteção da autonomia e liberdade de escolha dos usuários. Quando o acesso a determinado conteúdo digital é condicionado à aceitação de cookies ou à realização de um cadastro prévio, configura-se uma relação de troca compulsória, em que a privacidade do indivíduo passa a ser tratada como moeda de negociação.

2.2 INDUÇÃO AO ERRO DE CONSENTIMENTO

Outro método amplamente utilizado para obter consentimento são os chamados *"dark patterns"*, ou padrões escuros, que são elementos de design estrategicamente planejados para manipular o comportamento do usuário. É importante ressaltar que todo sistema/site tem um padrão de *design*, nesse cenário o *design patterns* (ou padrões de projeto) são soluções reutilizáveis para problemas comuns no desenvolvimento de software. São como "receitas" ou "modelos" que ajudam os programadores a escrever códigos mais organizados e eficientes. Os dark *patterns* (padrões obscuros), por sua vez, são soluções que tem a finalidade de explorar e enganar os usuários para realizar determinadas ações. Dessa forma *Dark Patterns* diz respeito à aplicação de princípios da psicologia e do comportamento humano para projetar interfaces de usuário de forma manipulativa e enganosa, visando obter benefícios financeiros em detrimento dos interesses dos usuários. (Sobiesk; Conti, 2010, apud Oliveira et al., 2023)

Existem ainda outras estratégias de design empregadas para influenciar o consentimento do usuário de forma manipulada. Entre elas a utilização de botões que são projetados em lugares estratégicos da tela, induzindo assim ao erro, e tornando o consentimento

viciado. Outra técnica empregada, é o uso dos chamados pop-ups, que abrem na tela de forma persistente, aparecendo consecutivamente até que os termos de coleta de dados sejam aceitos. Também são utilizadas mensagens alarmistas, que induzem medo ou insegurança ao sugerirem que a recusa do consentimento pode resultar na perda do acesso ao serviço ou em uma experiência reduzida. Reforçando esse entendimento Mendes e Fonseca (2020) destacam que o titular dos dados enfrenta limitações cognitivas quanto ao uso de suas informações no ambiente digital, além de uma relação assimétrica com os agentes responsáveis pelo tratamento desses dados.

Tais ações influenciam a tomada de decisão do usuário, levando-o a fornecer consentimento sem uma verdadeira liberdade de escolha. Prática essa que é considerada abusiva contrária à LGPD.

2.3 DESTINAÇÃO DOS DADOS PESSOAIS

De acordo com Oliveira e Silva (2018), os dados pessoais passaram a ser considerados "ativos intangíveis", tornando-se fundamentais para as estratégias de negócios. Empresas como Google, Amazon, Uber e Netflix têm nesses dados seu principal ativo empresarial. Além disso, os autores alertam que acreditar na existência de serviços gratuitos na internet é um equívoco, pois, na maioria das vezes, o acesso a determinados produtos ocorre mediante a coleta de informações pessoais. Isso acontece por meio do cadastramento e da aceitação dos termos de uso, que costumam ser extensos, escritos em fonte pequena e com uma linguagem técnica de difícil compreensão para o usuário, podendo ainda ser facilmente aceitos, com um simples clique.

Dessa forma, os dados pessoais têm se tornado um dos principais ativos das empresas, especialmente em plataformas digitais, onde são usados para criar estratégias de marketing direcionado e personalização de serviços. Sobre a temática, a Lei Geral de Proteção de Dados, em seu artigo 7º, estabelece restrições específicas ao tratamento de dados, delimitando suas hipóteses de aplicação de maneira geral e proporcional. Em seus termos, o tratamento de dados deve ocorrer exclusivamente dentro das situações previstas nesse artigo, cujos dez incisos possuem caráter taxativo.

De forma geral os dez incisos do artigo 7º da LGPD determinam que o tratamento de dados pessoais deve ocorrer apenas nas hipóteses previstas em lei, incluindo o consentimento do titular, o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas, a

realização de estudos por órgãos de pesquisa, a execução de contratos ou procedimentos preliminares a pedido do titular, o exercício regular de direitos, a proteção da vida ou da incolumidade física, a tutela da saúde por profissionais ou entidades da área, o atendimento ao interesse legítimo do controlador ou de terceiros e a proteção ao crédito. (Brasil, 2018)

Além disso, o artigo 7º, em seus parágrafos, reforça que o tratamento deve basear-se em interesse legítimo, e deve considerar a necessidade e a expectativa do titular, respeitando seus direitos e liberdades fundamentais. No caso de tratamento para a tutela da saúde, por exemplo, este deve ser realizado por profissionais ou entidades de saúde ou autoridades sanitárias, observando-se a proteção dos dados sensíveis. O tratamento de dados para prevenir fraudes e garantir a segurança do titular, incluindo processos de identificação e autenticação, pode ser feito, desde que respeite seus direitos fundamentais. (Brasil, 2018)

Embora a Lei Geral de Proteção de Dados estabeleça um rol taxativo de finalidades legítimas para o tratamento de dados pessoais, na prática observa-se que essas informações, uma vez coletadas, são frequentemente utilizadas de forma abusiva ou prejudicial ao titular. Entre os usos indevidos mais comuns, destaca-se a comercialização de dados com terceiros, fomentando um mercado paralelo de informações pessoais. De posse desses dados, muitas plataformas elaboram perfis detalhados dos usuários, direcionando anúncios e conteúdo personalizados. Em alguns casos, a coleta é tão abrangente que permite a análise do comportamento individual, possibilitando a antecipação de padrões de consumo e influenciando diretamente as estratégias comerciais.

Existe ainda a chamada *Dark Web* (Web Sombria/Internet Sombria) local onde os dados pessoais e/ou sensíveis são divulgados de forma indiscriminada. Para Monteiro e Fidêncio (2013), a *Dark Web* é considerada o território mais verdadeiramente obscuro do ciberespaço, ou o mais oculto. Os autores afirmam que essa *web* é uma rede global composta por usuários e computadores que operam à margem da visibilidade e da fiscalização. Nesse ambiente o usuário fica sujeito ao vazamento de seus dados para uso em todo tipo de golpes e roubos, deixando-o totalmente vulnerável aos criminosos que agem no ambiente virtual.

Existem ainda as situações em que os dados pessoais são vazados pelas próprias empresas que o coletaram, expondo milhares ou até milhões de pessoas na *Dark Web*. Foi o que ocorreu recentemente com a AT&T, uma das maiores empresas de telecomunicações do mundo que, por meio de um ataque cibernético em março do ano passado, teriam sido expostos cerca de 73 milhões de contas (Forbes, 2024). A Ticketmaster, plataforma global de vendas de

ingressos, também assumiu o vazamento de dados pessoais de aproximadamente 560 milhões de consumidores, ocorrido no início de 2024 (Info Money, 2024). O caso mais recente no Brasil, envolveu o Banco Central, que relatou o vazamento de dados de 2.534 mil clientes da QI Sociedade de Crédito, incluindo CPF e dados bancários (G1, 2025).

Em resumo, as práticas adotadas pelas empresas para obter consentimento muitas vezes ultrapassam os limites da legalidade, configurando vício de consentimento, conforme previsto na LGPD e no Direito Civil Brasileiro. Além disso, a destinação dos dados coletados pode expor os titulares a riscos significativos, como evidenciado pelos recentes vazamentos de dados. Esses incidentes reforçam a necessidade de maior investimento em segurança digital, maior responsabilização das empresas por falhas e a implementação de uma regulamentação mais rigorosa para proteger os direitos dos usuários de seus serviços.

3. MEDIDAS DE SEGURANÇA PARA USUÁRIOS E RESPONSABILIDADES DAS EMPRESAS

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) trouxe importantes mudanças no modo como as empresas devem lidar com as informações de seus clientes, parceiros e colaboradores. Em um cenário cada vez mais digitalizado e orientado por dados, torna-se indispensável que as organizações adotem práticas responsáveis e transparentes no tratamento dessas informações. Este capítulo busca analisar os deveres legais impostos pela LGPD às organizações, os riscos associados ao seu descumprimento, bem como a importância da responsabilidade empresarial na consolidação de um ambiente mais seguro e ético no tratamento de dados pessoais.

3.1 PROTEÇÃO PARA OS USUÁRIOS E REVOGAÇÃO DO CONSENTIMENTO

Além das responsabilidades das empresas, a LGPD confere aos titulares diversos direitos que visam garantir maior controle sobre seus dados pessoais. Segundo Doneda (2020), a sociedade da informação demanda um mecanismo que garanta tanto a proteção dos indivíduos em relação aos seus dados pessoais quanto a regulamentação da circulação de informações. Nesse contexto, o consentimento pleno e consciente para o tratamento de dados pessoais desempenha um papel fundamental.

A verificação do consentimento representa uma ferramenta essencial de controle por parte do titular dos dados. Para que essa autorização seja efetiva, é fundamental que o usuário

analise cuidadosamente os termos de uso e as políticas de privacidade antes de concedê-la. Somente com base nessas informações é possível compreender quais dados estão sendo coletados e para quais finalidades. Essa exigência está prevista no artigo 8º da Lei Geral de Proteção de Dados, juntamente com seus parágrafos, que reforçam a necessidade de transparência e informação clara no processo de obtenção do consentimento.

Esse conhecimento prévio daquilo que está sendo consentido é reforçado por Tobbin e Cardin (2021) que o adjetivo "informado" indica que o consentimento do titular dos dados deve ocorrer com pleno conhecimento sobre todas as informações relacionadas ao tratamento. Isso significa que é essencial repassar, de maneira detalhada, verdadeira e transparente, todos os aspectos que envolvem o tratamento de dados. Além disso, também se faz necessário esclarecer as possíveis consequências da recusa em conceder o consentimento. Essa autodeterminação informativa, segundo Sousa e Silva (2020)

> Constitui o direito do indivíduo de decidir, em princípio, sobre o uso de dados relacionados à sua pessoa. Em outras palavras, consiste no direito do indivíduo de decidir quem utiliza, para quem são repassados e com que finalidades os dados e informações pessoais são utilizados. Essa afirmação conduz ao entendimento de que a permissão do titular em todas as fases do processamento e utilização da informação a partir do consentimento torna-se importante no momento de definir o sentido e o alcance do fundamento da autodeterminação informativa. Isto para que, o referido termo, como instrumento de exteriorização do referido fundamento, possua aplicabilidade prática e possa cumprir seu papel com eficiência. (Sousa; Silva,2020, p. 11)

O consentimento também pode ser delimitado pelo usuário, uma vez que muitos serviços digitais oferecem opções para personalizar a coleta de dados, permitindo a desativação de cookies não essenciais e limitando o compartilhamento de informações com terceiros. Cumprindo a previsão no artigo 9º e em seus sete incisos da LGPD.

É possível ainda ao titular o uso de aplicações de bloqueadores de rastreamento, ou ainda a utilização de redes virtuais privadas (VPNs) e o mais comum que são os navegadores focados em privacidade, que podem dificultar a coleta de dados invasiva por plataformas digitais. Possibilidade amparada também pelo artigo 46 da citada lei.

Outro ponto importante que demonstra a autonomia do usuário com relação ao seu consentimento, é a possibilidade de revogação do consentimento. De acordo com o Art. 8º, o consentimento deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Além disso, em seu parágrafo 5º fica estabelecido que o consentimento pode ser revogado a qualquer momento, desde que o titular manifeste sua vontade de forma

expressa e por meio gratuito e facilitado, ratificando os tratamentos realizados enquanto não houver requerimento de eliminação, conforme o inciso VI do art. 18 (Brasil, 2018).

Nesse sentido Lugati e Almeida (2020) reforçam que o titular tem o direito de solicitar a interrupção do tratamento caso não concorde com as práticas adotadas pelos responsáveis pelo uso desses dados. Dessa forma o usuário tem total controle sobre suas informações, podendo dessa forma, proteger seus interesses e assegurar que seu consentimento seja respeitado durante todo o processo.

E por último e não menos importante, sempre haverá a possibilidade de denunciar à autoridade competente essas violações a LGPD e ao próprio Código Civil Brasileiro. Dessa forma, caso o titular do serviço identifique irregularidades no tratamento de seus dados, ele pode apresentar uma reclamação à Autoridade Nacional de Proteção de Dados (ANPD) através dos seus vários canais de comunicação, ou ainda, buscar medidas judiciais para reparação de danos. Conforme previsão do Art. 18 parágrafo 1º da citada Lei.

A conscientização dos usuários quanto aos seus direitos, aliada à adoção de medidas de segurança digital, é fundamental para reduzir riscos e prevenir o uso indevido de informações pessoais. Ao combinar a responsabilidade das empresas com a atuação ativa dos titulares, torna-se possível construir um ambiente digital mais seguro, transparente e em conformidade com os princípios da proteção de dados.

3.2 RESPONSABILIDADE DAS EMPRESAS E BOA GOVERNANÇA DE DADOS

A Lei Geral de Proteção de Dados impõe às empresas que realizam a coleta e o tratamento de dados pessoais o dever de assegurar a legalidade, a transparência e a segurança dessas operações. Isso implica a obrigação de agir em conformidade com a legislação vigente, informando de forma clara e acessível aos titulares a finalidade do uso dos dados e adotando medidas técnicas e administrativas eficazes para prevenir vazamentos, acessos não autorizados ou qualquer forma de utilização indevida das informações.

Além disso, as organizações precisam implementar mecanismos de governança que assegurem o cumprimento dessas diretrizes, minimizando riscos e promovendo a proteção da privacidade dos indivíduos. O não cumprimento dessas diretrizes pode resultar em uma multas de até dois por cento de seu faturamento total da empresa, além da publicização da infração ou ainda a eliminação dos dados pessoais de seus clientes, conforme previsto no artigo 52 em seus incisos de I a XII da LGPD.

Foi o que aconteceu com o Instituto Nacional do Seguro Social (INSS), que recebeu uma sanção da Autoridade Nacional de Proteção de Dados (ANPD) devido a um vazamento de dados pessoais de segurados, revelando falhas na implementação de medidas de segurança exigidas pela LGPD. O INSS não cumpriu a obrigação legal de informar os titulares afetados e a própria ANPD dentro do prazo estipulado, violando os princípios de transparência e de resposta a incidentes previstos na referida legislação. Como penalidade, a ANPD determinou a publicização da infração, que deveria ser feita por meio de nota oficial publicada no site do órgão e em suas redes sociais, de forma visível ao público. (Migalhas, 2023).

O artigo 6º, incisos I e II da LGPD, determina que o uso de dados pessoais deve atender a propósitos legítimos, específicos e informados ao titular, sendo vedado qualquer desvio dessas finalidades. Além disso, conforme o inciso X, as organizações devem prestar contas, comprovando a adoção de medidas eficazes de proteção de dados, como políticas internas, auditorias e relatórios de impacto. Como afirma Maria Celina Bodin de Moraes, "não descumprir a lei não é mais suficiente, é preciso, 'proativamente' prevenir a ocorrência de danos." (Bodin de Moraes, 2019, p. 5).

Outro dever essencial diz respeito à segurança da informação, previsto no artigo 46 da LGPD, que obriga os agentes de tratamento a adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas. Impotente destacar ainda que cabe a responsabilização civil em casos de incidentes de segurança ou uso indevido dos dados. Dessa forma as empresas podem ser responsabilizadas, devendo reparar eventuais danos causados aos titulares. A previsão é explícita no artigo 42 da LGPD

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. (Brasil, 2018)

A Justiça Federal em São Paulo, atendendo a pedido do Ministério Público Federal (MPF), condenou a União ao pagamento de R$15 mil em indenização por danos morais a cada

um dos cidadãos afetados pelo vazamento massivo de dados pessoais ocorrido em 2022. O caso envolveu o comprometimento de informações sensíveis de mais de 160 milhões de brasileiros, incluindo CPF, endereço, renda e dados vinculados ao SUS. A decisão enfatiza a responsabilidade do Estado na guarda e proteção dos dados pessoais sob sua custódia, especialmente à luz das obrigações impostas pela Lei Geral de Proteção de Dados Pessoais (LGPD). Para o juízo, houve falha grave na adoção de medidas eficazes de segurança da informação, o que gerou risco concreto e dano moral aos titulares. (MPF,2024)

O Superior Tribunal de Justiça (STJ) também tem desempenhado um importante papel na interpretação e aplicação dessa legislação. Até outubro de 2024, o STJ estabeleceu diversos precedentes relacionados à LGPD, abordando questões como a responsabilidade por vazamento de dados e as condições para indenização. (STJ, 2024). Em uma rápida pesquisa no site do Superior Tribunal de Justiça é possível encontrar referências à LGPD em 10 acórdãos e 180 decisões monocráticas, demonstrando o quando a Lei já está sendo usada no âmbito do tribunal.

O cenário de aplicação de da Lei vem ao encontro da opinião defendida por Junior et al. (2020) que afirma que a entrada em vigor da LGPD é fator fundamental a implementação de uma nova cultura organizacional que esteja alinhada às exigências legais, o que inclui a revisão dos fluxos internos de dados e o desenvolvimento de um Programa de Governança de Proteção de Dados.

Dessa forma, conclui-se que a responsabilidade das empresas no tratamento de dados pessoais vai além do mero cumprimento formal da Lei Geral de Proteção de Dados, exigindo uma postura proativa de conformidade e governança. A adoção de medidas concretas de segurança, transparência e accountability não só previne eventuais sanções administrativas e judiciais, como também fortalece a confiança dos titulares e preserva a integridade das relações comerciais. A governança de dados, portanto, deve ser compreendida como elemento central da estratégia organizacional, refletindo o comprometimento ético e jurídico das instituições com a proteção da privacidade no contexto digital atual.

CONCLUSÃO

A análise empreendida ao longo deste trabalho permitiu compreender que o consentimento, embora seja um dos fundamentos centrais da Lei Geral de Proteção de Dados Pessoais (LGPD), não é um mecanismo isento de fragilidades, especialmente quando coletado em ambientes digitais. A partir do conceito civilista de vício de consentimento, identificou-se

que a ausência de clareza, a linguagem técnica e a forma como as informações são apresentadas ao usuário podem comprometer a liberdade e a consciência necessárias para uma autorização válida no tratamento de dados pessoais.

Ao abordar os fundamentos da LGPD, notou-se que a legislação brasileira oferece princípios importantes para nortear o tratamento de dados, como o da finalidade, da adequação e da necessidade. No entanto, a simples existência de tais normas não garante sua efetividade. O princípio da responsabilização e prestação de contas, previstos na lei, exige não apenas seu cumprimento formal, mas também a demonstração de boas práticas pelas organizações, o que inclui medidas técnicas e administrativas que assegurem o cumprimento dos direitos dos titulares.

A análise das práticas adotadas por plataformas digitais evidencia que, em muitos casos, a coleta de dados ocorre de forma automática e indiscriminada, frequentemente sem a devida oferta de informações claras e acessíveis ao usuário. Nesse contexto, o consentimento é, por vezes, obtido por meio de mecanismos automatizados que não asseguram a autonomia do titular, configurando um cenário de fragilidade na manifestação de vontade.

As deficiências relacionadas à segurança da informação e à ausência de mecanismos eficazes de prestação de contas têm motivado a aplicação de sanções administrativas e judiciais tanto pela Autoridade Nacional de Proteção de Dados (ANPD) quanto pelo Poder Judiciário. Diversos entes públicos e privados vêm sendo responsabilizados por falhas no tratamento de dados pessoais e pela omissão na comunicação de incidentes de segurança, especialmente vazamentos. Em complemento, decisões judiciais têm assegurado indenizações por danos morais decorrentes do uso indevido de dados, reforçando a aplicabilidade da LGPD e seu papel essencial na tutela da privacidade.

Diante desse cenário, conclui-se que a LGPD constitui um marco regulatório fundamental, cuja efetividade depende da articulação entre normas jurídicas, fiscalização rigorosa, responsabilização adequada dos agentes de tratamento e, principalmente, da adoção de práticas concretas que respeitem os direitos dos titulares. A prevenção ao vício de consentimento deve figurar como prioridade, especialmente diante da acentuada assimetria de poder e informação existente entre usuários e plataformas digitais. A consolidação de uma cultura de proteção de dados exige, portanto, uma mudança estrutural na forma como o consentimento é interpretado, obtido e operacionalizado no ambiente digital.

REFERÊNCIAS

ALMEIDA, Mauro de Bias. ***Paywall* ou gratuidade:** o que esperar dos modelos de negócios no jornalismo online? 2013. 69 f. Trabalho de Conclusão de Curso (Graduação em Comunicação - Habilitação em Jornalismo) – Escola de Comunicação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2013. Disponível em: https://pantheon.ufrj.br/handle/11422/5855. Acesso em: 06 de mar. 2025.

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

BODIN DE MORAES, Maria Celina. **LGPD:** um novo regime de responsabilização civil dito "proativo". Editorial à Civilistica.com. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448. Acessado em 24 de mar. De 2025.

BRASIL. *Agência Nacional de Proteção de Dados.* **Guia orientativo: cookies e proteção de dados pessoais.** 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 15 de mar. 2025.

BRASIL. **Código Civil. Lei n.º 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União: seção 1*, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 20 fev. 2025.

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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 de fev. 2025.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro:** Responsabilidade Civil. 35. ed. São Paulo: Saraiva, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Tribunais,2019. Edição Kindle.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de Direito Civil** - Parte Geral e LINDB. 19. ed. Salvador: Ed. JusPodivm, 2021.

FORBES. **Dados vazados da AT&T são de cerca de 73 milhões de contas**. Forbes, 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/03/dados-vazados-da-att-sao-de-cerca-de-73-milhoes-de-contas. Acesso em: 21 mar. 2025.

G1. **BC comunica vazamento de dados de 2.534 mil pessoas com conta na QI Sociedade de Crédito**. G1, 2025. Disponível em: https://g1.globo.com/economia/noticia/2025/03/17/bc-comunica-vazamento-de-dados-de-2534-mil-pessoas-com-conta-na-qi-sociedade-de-credito.ghtml. Acesso em: 21 mar. 2025.

INFO MONEY. **Vazamento na Ticketmaster pode ter exposto 560 milhões de consumidores**; entenda danos. InfoMoney, 2024. Disponível em: https://www.infomoney.com.br/consumo/vazamento-na-ticketmaster-pode-ter-exposto-560-milhoes-de-consumidores-entenda-danos/. Acesso em: 21 mar. 2025.

JUNIOR, S. D. S. P., NORONHA, V. F., CARDOSO, C. P., VIEIRA, C. K., DOS SANTOS, C. R. G., & COSTA, M. C. (2020). **Governança responsável e as boas práticas de *compliance*:** qual o estado d'arte no caso brasileiro? Revista Interdisciplinar De Ensino, Pesquisa E Extensão, 8(1), 173-184.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. **Da Evolução Das Legislações Sobre Proteção De Dados:** a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito*, Viçosa, v.12 n.02 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 24 de mar. De 2025.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. **Proteção de dados para além do consentimento:** tendências contemporâneas de materialização. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 16 de mar. 2025.

MIGALHAS. **ANPD condena INSS por vazamento de dados.** *Migalhas*, 5 fev. 2024. Disponível em: https://www.migalhas.com.br/quentes/401393/anpd-condena-inss-por-vazamento-de-dados. Acesso em: 11 abr. 2025.

MINISTÉRIO PÚBLICO FEDERAL. **Justiça determina indenização de R$ 15 mil a cidadãos que tiveram dados pessoais vazados em 2022**. São Paulo: MPF, 2024. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/justica-determina-indenizacao-de-r-15-mil-a-cidadaos-que-tiveram-dados-pessoais-vazados-em-2022. Acesso em: 5 abr. 2025.

MONTEIRO, S. D.; FIDÊNCIO, M. V. **As dobras semióticas do ciberespaço:** da web visível à invisível. TransInformação, Campinas-SP, v. 1, n. 25, p. 35-46, jan./abr. 2013. Disponível em: https://periodicos.puc-campinas.edu.br/transinfo/article/view/6122/3832. Acesso em: 21 de mar. 2025.

OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. **Cookies de computador e história da internet:** desafios à lei brasileira de proteção de dados pessoais. Revista de Estados Jurídicos UNESP, ano 22, n. 36, p. 307-388, 2018. Disponível em: https://periodicos.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/2767. Acesso em: 20 mar. 2025.

OLIVEIRA, Thiellen Caroline de; COLETI, Thiago Adriano; MORANDINI, Marcelo; BALANCIERI, Renato; OLIVEIRA, André Luiz de. **Dark Patterns nos marketplaces:** uma investigação com base nas reclamações dos consumidores. *Anais do Workshop de Infraestruturas de Dados Espaciais (WIDE)*, 2023. Disponível em: https://sol.sbc.org.br/index.php/wide/article/view/32163/31965. Acesso em: 11 abr. 2025.

PEDRO, Manuela Genovese. **Dados como barreira à entrada, LGPD e direito antitruste:** uma análise dos impactos na concorrência a partir da legislação brasileira de proteção de dados pessoais e do uso comercial destas informações. 2021. Trabalho de Conclusão de Curso

(Bacharelado em Direito) – Escola de Direito de São Paulo, Fundação Getulio Vargas, São Paulo, 2021. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/7b602833-4d60-445c-859e-a8d2ccb3755f/content. Acesso em: 02 mar. 2025.

SOUSA, Rosilene Paiva Marinho de; SILVA, Paulo Henrique Tavares da. **Proteção de dados pessoais e os contornos da autodeterminação informativa.** *Informação & Sociedade*: Estudos, João Pessoa, v. 30, n. 2, p. 1-19, abr./jun. 2020. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/52483. Acesso em: 10 mar. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Os precedentes do STJ nos primeiros quatro anos de vigência da Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 27 out. 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/27102024-Os-precedentes-do-STJ-nos-primeiros-quatro-anos-de-vigencia-da-Lei-Geral-de-Protecao-de-Dados-Pessoais.aspx. Acesso em: 5 abr. 2025.

TOBBIN, Raissa Arantes; CARDIN, Valéria Silva Galdino. **Política de *cookies* e a "crise do consentimento":** Lei Geral de Proteção de Dados e a autodeterminação informativa. *Revista da Faculdade de Direito da UFRGS*, Porto Alegre, n. 47, p. 241-262, dez. 2021. DOI: https://doi.org/10.22456/0104-6594.113663. Acessado em 24 de mar. de 2025.

VENOSA, Sílvio de Salvo. **Direito civil:** parte geral. 23. ed. Barueri, SP: Atlas, 2023.

VERBICARO, Dennis; VIEIRA, Janaína do Nascimento. **A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço**. Revista de Direito do Consumidor [Recurso Eletrônico]. São Paulo, n.134, mar./abr. 2021. Disponível em: https://dspace.almg.gov.br/handle/11037/40415. Acesso em: 10 de mar. 2025.