

Uso do consentimento genérico como risco empresarial e a governança de dados

Use of generic consent as a business and data governance risk

Thomaz Jefferson Carvalho¹
João Pedro Paião Borri²

Recebido em: 24.04.2024
Aprovado em: 23.05.2025

RESUMO

O presente artigo tem como objetivo analisar as complexidades e riscos da atividade empresarial que justifica as suas operações de tratamento de dados pessoais pela hipótese legal do consentimento, prevista no art. 7º, I, da Lei Geral de Proteção de Dados. Para tanto, será realizado um paralelo entre o contexto histórico das regulamentações relacionadas entre a privacidade e proteção de dados, com os conceitos gerais da LGPD, em especial a hipótese legal do consentimento, para chegar-se ao ponto central do presente estudo, tendo em vista a importância de entender qual o papel do consentimento na evolução das legislações sobre proteção de dados e, principalmente, de que forma a LGPD aborda este instituto. Assim, como metodologia utiliza-se conhecimento científico, método de abordagem dedutivo e método de procedimento bibliográfico. Por fim, entender quando utilizar o consentimento como base legal para tratamento de dados, para concluir que a utilização desta hipótese legal genericamente, sem o mapeamento do fluxo de dados da atividade empresarial, leva o empresário a assumir riscos que sujeitem a atividade empresarial a sanções administrativas ou judiciais, de forma a impactar severamente todo o negócio.

Palavras-chave: consentimento informado; privacidade; proteção de dados.

ABSTRACT

This article aims to analyze the complexities and risks of business activity that justify its personal data processing operations based on the legal basis of consent, as stipulated in Article 7, item I, of the Brazilian General Data Protection Law (LGPD). To this end, a

¹ Doutor em Direito pela Universidade Estácio de Sá, Mestre em Ciências Jurídicas pela Unicesumar; Pós-graduado lato sensu em LGPD pela Faculdade Legale; em Direito do Trabalho pela Universidade Castelo Branco, em Metodologia do Ensino Superior pela UNOPAR e em Direito Eletrônico pela Universidade Estácio de Sá. Graduado em Direito pela UNOPAR. Professor do curso de graduação da UNICESUMAR e advogado da Carvalho & Rodrigues Advogados Associados. E-mail: thomaz@carvalhoerodrigues.adv.br. Lattes: <http://lattes.cnpq.br/9310703121210446>.

² Bacharel em Direito pela Unicesumar. Advogado na cidade de Maringá/PR.



parallel will be drawn between the historical context of regulations related to privacy and data protection, and the general concepts of the LGPD, particularly the legal basis of consent, to arrive at the central point of this study. This is done considering the importance of understanding the role of consent in the evolution of data protection laws and, especially, how the LGPD addresses this legal concept. Thus, as a methodology, scientific knowledge, a deductive approach method, and a bibliographic procedure method are utilized. Finally, the article seeks to understand when to use consent as a legal basis for data processing, ultimately concluding that the generic use of this legal basis, without mapping the data flow of the business activity, leads the entrepreneur to assume risks that could subject the business activity to administrative or judicial sanctions, severely impacting the entire business.

Keywords: Informed consent; privacy; data protection.

1 INTRODUÇÃO

A regulamentação da temática de privacidade e proteção de dados é recente no ordenamento jurídico brasileiro, por isso, para facilitar a compreensão do presente trabalho, necessário se faz trazer o contexto histórico da proteção de dados no Brasil, bem como os principais conceitos criados pelo legislador quando da criação da Lei Geral de Proteção de Dados (LGPD).

A Lei Geral de Proteção de Dados (LGPD) regulamenta a proteção de dados pessoais no Brasil, visando resguardar a intimidade e a privacidade das pessoas físicas. A lei trouxe consigo princípios e regras para o tratamento de dados pessoais, através da criação de enquadramentos necessários para tipificá-los como lícitos e punições ante o descumprimento, bem como criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar e aplicar penalidades àqueles que violarem estas regras e princípios.

A referida norma estabelece hipóteses legais de tratamento de dados, das quais os agentes de tratamento devem se valer para tratar dados pessoais. Uma das principais hipóteses utilizadas sem dúvida é o “consentimento”, a qual tem sido utilizada de maneira genérica pelos agentes de tratamento, em especial os empresários que, em sua grande maioria, ignoram a complexidade e o risco de justificar os tratamentos de dados pessoais de suas atividades empresariais por esta hipótese legal.

Desta feita, o presente trabalho tem por objetivo o estudo da hipótese legal do consentimento, prevista no art. 7º, inciso I, da LGPD, a fim de analisar as formalidades e requisitos para utilizá-la, visando, ao final, demonstrar a complexidade e os riscos que o empresário deve avaliar antes de justificar um tratamento de dados pessoais por esta base legal e as consequências que a utilização desta base legal de forma genérica pode trazer às atividades empresariais e governança de dados.

2 DADOS PESSOAIS E A REGULAMENTAÇÃO BRASILEIRA

A análise que se fará no presente estudo prescinde a apresentação do contexto e evolução histórica do cenário da proteção de dados no Brasil e a forma que o legislador regulamentou a temática no ordenamento jurídico brasileiro.

Assim como é necessário expor os conceitos trazidos pela Lei Geral de Proteção de Dados que influirão no presente estudo, uma vez que a análise conclusiva do trabalho se dá a partir de disposição legal da lei, além de tratar-se de legislação criada recentemente e vigente por completo há menos de um ano.

2.1 Contexto histórico da proteção de dados no Brasil

Para a construção do contexto histórico sobre a proteção de dados no Brasil, é imprescindível conectá-lo ao direito à privacidade, pois, antes mesmo de surgir ao ordenamento jurídico a expressão “proteção de dados pessoais”, este instituto jurídico era associado, principalmente, à privacidade das pessoas naturais, como bem se destaca:

É muito recente a incorporação do termo “proteção de dados pessoais” ao glossário jurídico brasileiro, o que se deu principalmente na esteira do debate que antecedeu a promulgação da Lei Geral de Proteção de Dados. No entanto, questões que hoje associamos diretamente à proteção de dados não eram, de forma alguma, estranhas à práxis jurídica no País. [...]

Entre esses diversos institutos e matérias entre os quais, por muito tempo, a proteção de dados no Brasil foi associada, a mais relevante é o direito à privacidade – como também pela forte ressonância entre os dois institutos. A bem da verdade, até hoje se observa, coloquialmente ou mesmo em literatura

especializada, uma certa ambivalência na utilização dos conceitos de privacidade e proteção de dados. (Bioni, 2021, p. 29)

O direito à privacidade está consolidado no direito brasileiro há décadas e, até à sua previsão constitucional (art. 5º, X) e posteriormente ao Código Civil Brasileiro, já era considerado pela doutrina e jurisprudência como um dos direitos da personalidade.

A temática de proteção de dados, inegavelmente, evoluiu à medida que o direito à privacidade se consolidava no Brasil, pois compartilham, majoritariamente, dos mesmos valores, entretanto, a proteção de dados no Brasil foi se desenvolveu dialogando relativamente pouco com o direito à privacidade.

Isso porque a proteção de dados, desde a década de 1970, mesmo que não introduzida especialmente desta maneira, o legislador a tratou de maneira autônoma, sem que fosse necessário associar-se ao direito à privacidade. Ainda em referência à exposição de Bioni (2021, p. 30), algumas legislações trouxeram a temática de proteção de dados, embora não tenha se evoluído, naquela época, algo que pudesse consolidar o tema no Brasil, assim como o direito à privacidade.

No advento da Constituição Federal, o *habeas data*, mesmo que não tenha enfrentado os desafios existentes da época relacionado a tratamento de dados pessoais, na crescente sociedade da informação, embora esta ação constitucional efetivar o direito de acesso e retificação de dados pessoais, quando estes relacionados a pessoa física e pleiteados por ela mesma.

Em que pese a inovação Constitucional em 1988 com a criação deste remédio constitucional, dos direitos à vida privada e intimidade (art. 5º, X) e o segredo das comunicações telefônicas, telegráficas e de dados (art. 5º, XII), nada se fez para identificar, de forma autônoma, o direito à proteção de dados pessoais.

Não obstante a inexistência de menção própria sobre proteção de dados na redação originária da Constituição Federal, a emenda constitucional n. 115/2022, sem sombra de dúvidas, estabeleceu um marco recente no direito interno brasileiro com a criação do direito à proteção dos dados pessoais (art. 5º, LXXIX), consolidando, formalmente, este direito fundamental que foi extensamente regulamentado pela LGPD.

Contudo, em uma sequência cronológica, após a promulgação da Constituição, outras normas do direito interno estabeleceram disposições pertinentes a respeito da proteção de dados, algumas delas servindo de base para a formação da LGPD. Uma das principais é o Código de Defesa do Consumidor (1991), em especial o seu art. 43, que trata da garantia de acesso aos consumidores às suas informações existentes nos bancos de dados dos fornecedores, o que contribuiu para o debate a respeito do registro de dados sobre operações financeiras do consumidor.

Com a intensificação desta temática a respeito do registro de dados sobre operações financeiras do consumidor, surge a Lei do Cadastro Positivo (Lei n. 12.414/2011) que, em um cenário internacional mais consolidado, trouxe importantes conceitos sobre proteção de dados, como o de dados sensíveis (art. 3º, § 3º, II), e importantes princípios, dentre eles o da finalidade (art. 5º, VII), transparência (art. 7º, §§ 1º e 2º), segurança (art. 5º, II), entre outros. Apesar disso, esta lei não contribuiu como o esperado para o desenvolvimento da cultura jurídica de proteção de dados, muito pela utilização dos serviços de cadastro positivo não ter sido como esperava o legislador.

De modo diferente, o Marco Civil da Internet (Lei n. 12.965/2014), ainda que não objetivasse suprir uma legislação específica sobre proteção de dados pessoais, ao criar um regime de direitos para o usuário da internet, concebeu direitos e procedimento atinentes ao uso dos dados pessoais destes. Tanto é que algumas das expressões presentes nesta lei, são de difícil adaptação para a temática específica de proteção de dados, em especial à LGPD, até porque, trouxe como regra geral, a obrigatoria coleta do consentimento para tratar dados pessoais, o que será exaustivamente abordado neste estudo, pois o consentimento trata de apenas uma hipótese legal para tratar dados pessoais.

Diante de um cenário internacional em que a cultura de proteção de dados pessoais já estava implementada, com discussões avançadas a respeito desta temática, em 14/08/2018 é publicada a Lei Geral de Proteção de Dados, que visa regulamentar os tratamentos de dados pessoais, com fundamento na proteção da privacidade e intimidade das pessoas naturais.

Encerrando o contexto histórico da proteção de dados no Brasil de forma cronológica, os dados pessoais foram incluídos no rol de direitos e garantias fundamentais do art. 5º, da Constituição Federal, pela EC 115/2022, como já mencionado anteriormente, o que materializou o entendimento uníssono da doutrina brasileira, de a proteção de dados pessoais ser um direito fundamental da pessoa humana.

2.2 A Regulamentação Brasileira Sobre Proteção De Dados

A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) nasce com o objetivo de gerar proteção aos dados pessoais de pessoas naturais. Destina-se à proteção dos direitos fundamentais destas, como a liberdade e privacidade, garantindo ao titular o uso seguro e ético de seus dados pessoais, estejam eles em ambiente físico ou digital³.

Dados pessoais nos termos do art. 5º da LGPD (lei geral de proteção de dados) são todas as informações que permitem a identificação de pessoas naturais, de forma direta ou indireta, como o nome, CPF, e-mail, entre outras.

Para facilitar o entendimento sobre a definição de dados pessoais, pode-se dividi-la em 03 (três) elementos: (i) informação – podem ser objetivas, p.ex. o nome, bem como subjetiva, p.ex. avaliação do empregador sobre um de seus empregados; (ii) relacionada a pessoa natural: inclui-se, aqui, a informação relacionada ao nascituro e ao falecido, desde que, desse último, seja coletada em vida; (iii) identificada ou identificável: algumas informações tornam a pessoa natural imediatamente ou facilmente identificada, como o nome ou CPF, e outras informações tornam a pessoa identificável quando aliadas a outras (Maldonado, 2021, p. 94 e 95).

Como um dos fundamentos da LGPD é o respeito à privacidade e a inviolabilidade da intimidade, honra e imagem, a lei considerou determinadas informações como

³ Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

sensíveis, pois, estas revelam aspectos delicados da pessoa, capazes de gerar algum tipo de discriminação ou exposição, conforme prevê o art. 5º, II, da LGPD⁴.

A lei visa gerar proteção aos dados pessoais por meio da criação de regras e mitigação de riscos dos tratamentos de dados pessoais e, portanto, se aplica a toda pessoa física ou jurídica, de direito pública ou privado, que realize qualquer operação de tratamento de dados pessoais.

Basicamente, qualquer pessoa, em qualquer circunstância, pode tratar dado pessoal, haja vista que a LGPD define como operação de tratamento de dados pessoais todas as possibilidades de manuseio destes dados, independente do meio utilizado, partindo da coleta e findando na eliminação dos dados pessoais, vide art. 5º, X, da LGPD⁵.

Em que pese qualquer pessoa possa tratar dados pessoais, a LGPD traz dois personagens, com atribuições e responsabilidades distintas, denominando-os como controlador e operador, considerados pela lei como agentes de tratamento.

O controlador é a pessoa que está no comando dos dados pessoais, ou seja, as operações de tratamento são realizadas em seu nome, atendendo a uma finalidade imposta por ele, mesmo que não as faça diretamente, pois, basta tomar as principais decisões e deter maior influência sobre estas para ser considerado como controlador.

Já o operador é aquele que realiza as operações de tratamento em nome do controlador. Para ostentar essa posição, deve fazer aquilo que for determinado pelo controlador, mesmo que tome algumas decisões simples sobre aquela operação. Contudo, não se deve confundir o empregado (CLT) como operador, pois, os atos que pratica pela empresa, dentro das suas atribuições, são considerados como atos do próprio controlador, em função desta subordinação direta que possui do empregador (ANPD, 2022, p. 18).

A distinção de controlador e operador é de suma importância em uma operação de tratamento de dados pessoais, uma vez que a LGPD traz atribuições e

⁴ II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

⁵ X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

responsabilidades distintas para cada um, até porque um deles está no comando e o outro atua em seu nome, o que não o isenta de responsabilidade.

Os agentes de tratamento devem observar uma porção de regras e diretrizes para tratar dados pessoais, a começar pelos princípios previstos na lei. A base principiológica introduzida pela LGPD, mas que já podia ser observada em outras legislações, como mencionado no tópico anterior, é aplicável a tudo o que envolve uma operação de tratamento.

A LGPD prevê no art. 6^o, a base principiológica que contém 10 princípios a ser seguidos como um mantra em toda e qualquer atividade de tratamento de dados pessoais, dentre os quais, podemos destacar os da finalidade, necessidade e transparência, que visam limitar o tratamento de dados pessoais para a finalidade pela qual está sendo realizado e com os dados pessoais estritamente necessários, devendo os agentes de tratamento sempre transparecerem a finalidade e a necessidade pela qual estão realizando esta atividade.

Os princípios devem ser respeitados por todo o ciclo de vida do tratamento dos dados pessoais, senão a operação será considerada ilegal. Além do dever de segui-los à risca, é necessário que o controlador justifique a operação de tratamento em alguma das hipóteses legais previstas no art. 7^o, da LGPD.

Ao justificar o tratamento em alguma destas hipóteses, os agentes de tratamento devem seguir outras regras previstas na LGPD, principalmente quando tratam dados pessoais sensíveis e dados de crianças e adolescentes, até porque a lei traz seções específicas para estes dois últimos grupos de dados pessoais.

De forma eficaz e acertada, a LGPD, além de estabelecer regras, obrigações e responsabilidades para as operações de tratamento de dados pessoais, criou a Autoridade Nacional de Proteção de Dados (ANPD), inicialmente órgão da administração pública vinculado à Presidência da República, e atualmente Autarquia de Natureza Especial, com

⁶ Art. 6^o As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade [...] II - adequação [...] III - necessidade [...] IV - livre acesso [...] V - qualidade dos dados [...] VI - transparência [...] VII - segurança [...] VIII - prevenção [...] IX - não discriminação [...] X - responsabilização e prestação de contas [...].

a vigência Medida Provisória n. 1124/2022, tratando-se de importante mudança de sua natureza jurídica.

A ANPD é responsável por zelar, fiscalizar o cumprimento da LGPD e aplicar sanções pelo descumprimento desta, detendo autonomia técnica e decisória, ainda mais com a sua transformação para autarquia de natureza especial. O seu papel é de suma importância para a consolidação da cultura de proteção de dados no Brasil, e no gozo de suas atribuições, já elaborou um guia orientativo para definições de agentes de tratamento e uma regulação específica para micro e pequenas empresas, através da Resolução CD/ANPD n. 2.

Por fim, a LGPD esteve integralmente vigente após 03 (três) marcos temporais. O primeiro, em 28/12/2018, quando os artigos referentes à criação da ANPD entraram em vigor. O segundo, em 18/09/2020, quando a maior parte da LGPD entrou em vigor. O último, em 1º/08/2021, quando as sanções administrativas previstas na LGPD entraram em vigor.

A partir deste resumo dos conceitos, regras e obrigações introduzidas pela LGPD, passa-se ao objeto principal deste estudo: a análise da hipótese legal do consentimento, avaliando a complexidade e formalidade da sua utilização para justificar uma operação de tratamento, a fim de demonstrar o risco empresarial e à governança de dados quando utilizada pelo empresário de forma genérica.

3 CONSENTIMENTO DO TITULAR DE DADOS PESSOAIS E A PREVISÃO DA LGPD

Neste tópico, será abordado o conceito de consentimento na legislação brasileira, a sua previsão na Lei Geral de Proteção de Dados como hipótese legal de tratamento de dados pessoais e como se deu a sua evolução nas legislações de proteção de dados, por meio da análise do seu papel e importância ao longo do tempo e nas regulamentações sobre esta matéria.

3.1 Evolução do consentimento até a regulamentação na LGPD

O consentimento pode ser definido como “a anuência válida do sujeito a respeito do entabulamento de uma relação jurídica sobre determinado objeto” (França *apud* Diniz, 2022, p. 173).

Na brilhante exposição de Bruno Bioni expõe as quatro gerações de leis de proteção de dados pessoais, dentre as quais a segunda e a terceira gerações visaram conferir ao indivíduo maior protagonismo em todos os movimentos dos seus dados pessoais, tendo o consentimento como vetor central, o que consagrou a autodeterminação informativa. Contudo, a quarta geração relativizou a centralidade do consentimento nos tratamentos de dados pessoais, muito embora não tenha eliminado o seu protagonismo, pois, até os dias de hoje a construção e a interpretação das normas relacionadas a proteção de dados seguem este norte regulatório.

Com fulcro nesta construção regulatória exposta por Bruno Bioni, ensina Laura Schertel Mendes que a maneira pela qual o indivíduo exerce a autodeterminação informacional é pelo mecanismo do consentimento (Mendes, 2014, p. 60):

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.

Nos dizeres de Danilo Doneda (2006, p. 372):

no tratamento reservado à disciplina do consentimento, desnuda-se o próprio caráter de um sistema de proteção de dados pessoais. Em um sistema de índole patrimonialista, o consentimento assumirá uma função predominantemente legitimadora, ao servir como instrumento para colocar os dados pessoais no mercado e proporcionar, se levarmos a um efeito extremo, a chamada *commodification* dos dados pessoais - sua transformação em uma *commodity*. Em um sistema que privilegie a privacidade como uma liberdade negativa e se confia ao indivíduo a autodeterminação de sua esfera privada, o consentimento é o instrumento por excelência do exercício deste poder

Assim, é evidente que o consentimento, durante a evolução regulatória no cenário internacional, exerceu papel fundamental para a construção da privacidade e proteção de dados pessoais, justamente por instrumentalizar a autodeterminação informativa.

No Brasil, os marcos regulatórios não se diferenciaram do cenário europeu quando o assunto é o protagonismo do consentimento em proteção de dados. No direito brasileiro, o consentimento sempre foi abordado como um dos principais pilares da proteção de dados pessoais (Feigelson, 2019, p. 60).

O Código Civil de 2002, de maneira indireta, prevê três formas de manifestação de vontade: expressa, tácita e presumida. Dentre elas, a manifestação expressa é a que mais se aproxima do consentimento em proteção de dados pessoais. Isso porque, desde o advento da Diretiva de Proteção de Dados Pessoais 96/46/EC, o consentimento já se traduzia em “qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento.”

A criação do conceito específico de consentimento para a proteção de dados pessoais, é consequência do papel fundamental que detém. Principalmente nas relações de consumo, as organizações utilizam o consentimento como “uma ficção” (p.ex. cláusulas padrões), em que este deixa de exercer o seu papel de proteção aos direitos fundamentais, surgindo, daí, a necessidade de considerar um consentimento específico para o tratamento de dados pessoais, a ser manejado uniformemente em todas as situações (Doneda, 2006).

Este consentimento específico ao tratamento de dados pessoais, consagra, indubitavelmente, dois importantes princípios, o da finalidade e informação, pois, como mencionado, o consentimento deve ser específico (à uma finalidade) e informado.

No Brasil, a partir desta ideia de o indivíduo cada vez mais ter controle⁷ sobre os seus dados pessoais, podemos citar a inovação legislativa consistente no Marco Civil da Internet (Lei n. 12.965/2014), que, muito embora não tivesse como objetivo suprir uma

⁷ Isto porque o princípio da autodeterminação informativa consagrou este importante marco nas regulamentações sobre proteção dados, conferindo ao indivíduo o poder de controlar o fluxo dos seus dados pessoais.

lei específica de proteção de dados, vários dispositivos da lei asseguraram o consentimento como norte regulatório, conforme explica Bruno Bioni (2021, p. 129):

Pela combinatória de tais dispositivos, verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação.

No entanto, após anos de discussões e debates, o Brasil aprovou uma Lei Geral de Proteção de Dados Pessoais, a qual também seguiria o mesmo caminho de legislações anteriores, tendo o consentimento como via única para legitimar o tratamento de dados pessoais (BIONI, 2021). Ocorre que após inúmeras consultas públicas o consentimento, por esta nova lei brasileira, deixou de ser a única hipótese legal para tratar dados pessoais, conforme se expõe a seguir.

3.2 A Hipótese legal do consentimento previsto na LGPD

A Lei Geral de Proteção de Dados tem ainda como vetor principal o consentimento, haja vista que um de seus fundamentos é a autodeterminação informativa (art. 2º, II), em que pese não seja mais a única forma de legitimar um tratamento de dados pessoais, mas sim uma das dez hipóteses previstas no rol taxativo do art. 7º.

Embora os agentes de tratamento possam justificar as operações de tratamento por meio das demais hipóteses legais, não há como dizer que o consentimento deixou de ser o seu vetor principal, como explica Bruno Bioni (2021, p. 131):

Por outro lado, também é possível dizer que o consentimento não deixou de ser o seu vetor principal. Isso porque uma análise detida dos princípios e a maneira pela qual a LGPD dissecou tal elemento ao longo do seu corpo normativo acabam por revelar uma forte preocupação, mais uma vez, sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações pessoais.

A grande demonstração disto é a previsão do § 6º, do art. 7º, da LGPD, que prevê a obrigatoriedade da observância dos princípios gerais e garantia dos direitos do titular, uma vez que todo o regime de direitos criado pela LGPD tem como vetor central a autonomia privada, visando a participação do indivíduo no fluxo de seus dados pessoais:

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

O art. 5º, XII, da LGPD, traz como consentimento a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Esse conceito, sobremaneira, vai de frente com o previsto na legislação europeia, que diferente da LGPD, explica o significado de “livre, informado e inequívoco”.

É de suma importância entender o significado desta expressão que conceitua o consentimento na LGPD, pois tratam de requisitos que devem ser observados pelos agentes de tratamento. Extrai-se do General Data Protection Regulation (GDPR) o entendimento a respeito destes conceitos, em especial a Guideline 05/2020, do European Data Protection Board (EDPB), conforme expõe Maldonado e Ópice Blum (2021, p. 192 e 193).

Tem-se como livre, a livre escolha que o titular dos dados pessoais sobre quais tipos de dados serão tratados em cada operação, e o consentimento informado é atingido quando o titular é informado a respeito de todo o ciclo de vida do tratamento dos seus dados pessoais, e por último, tem-se como inequívoco a prova de que o titular autorizou o tratamento dos seus dados pessoais, por ação positiva, como marcar a opção em caixa de texto (Maldonado, Ópice Blum, 2021).

Em que pese esses conceitos não estarem previstos de forma direta na LGPD, é possível identificá-los no art. 8º:

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (INEQUÍVOCO).

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. (LIVRE e INFORMADO)

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. (consentimento INEQUÍVOCO)

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento. (LIVRE)

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (INFORMADO)

Trata-se até aqui apenas sobre o conceito da hipótese legal do consentimento que pode ser utilizada como justificativa para tratamento de dados pessoais, conforme o art. 7º, I, da LGPD, entretanto, a lei confere uma série de outras formalidades que devem ser observadas para que o consentimento seja utilizado para legitimar estas operações.

Para que o controlador dos dados pessoais compartilhe os dados obtidos com o consentimento do titular, deverá obter consentimento específico para esse fim (art. 7º, § 5º). Aqui já se observa o cuidado que há com essa operação de tratamento, muito corriqueira no mundo atual, onde se observa grandes corporações que possuem bases de dados que valem mais que petróleo⁸.

A ideia da obtenção de um consentimento específico para compartilhar os dados pessoais, é, novamente, trazer o indivíduo ao controle das suas informações pessoais, exercendo a autodeterminação informativa através da escolha ou não de autorizar o controlador dos seus dados pessoais compartilhar suas informações com terceiros.

A LGPD criou diversos mecanismos para tornar o consentimento a forma mais rígida de tratar dados pessoais, pois facilmente anulável, e a maneira mais simples de o titular dos dados pessoais encerrar qualquer operação de tratamento, o que contribui, sobremaneira, ao presente estudo. Os §§ 5º e 6º, do art. 8º e os §§ 1º, 2º, do art. 9º, principalmente, demonstram esta situação:

⁸ Em 2006, o matemático britânico Clive Humby disse a famosa frase “Data is the new oil”, que passou a ser utilizada em todo o mundo, tornando-se um jargão da matéria de privacidade e proteção de dados.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

§ 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. (g.n.)

Isso ainda é consagrado, especificamente, como direitos do titular dos dados pessoais, conforme observa-se dos incisos VI, VIII e IX, do art. 18, da LGPD:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Além destas exigências gerais que a LGPD impõe aos agentes de tratamento, para qualquer operação de tratamento que utilize o consentimento como justificativa, há na lei a exigência de que esta hipótese legal seja obrigatoriamente utilizada no tratamento de dados pessoais sensíveis (art. 11) e de crianças e adolescentes (art. 14), o que não será objeto do presente estudo, pois, o objetivo é demonstrar o risco empresarial e à governança de dados ao justificar de forma genérica qualquer tratamento de dados pessoais através do consentimento.

O consentimento, ainda, é uma das quatro hipóteses legais que autorizam o controlador a fazer transferência internacional dos dados pessoais que tiver posse, conforme o art. 33, VIII, da LGPD, desde que “em destaque para a transferência, com

informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades”.

Pode-se concluir, portanto, que o consentimento, embora seja uma das dez hipóteses legais de tratamento de dados pessoais, sem hierarquia alguma em relação aos demais, é abordada como ponto central da LGPD, seja pela obrigatoriedade da sua coleta no tratamento de dados pessoais em específico, seja pelas formas de nulidade através da configuração de vícios ao consentimento, e, também, a existência de várias hipóteses de revogação.

Assim sendo, é importante que os empresários sejam criteriosos em suas atividades empresariais que envolvam operações de tratamento, para que o consentimento não seja o vetor central de suas operações, tendo em vista que isto pode trazer consigo um grande risco de estas serem inviabilizadas com a revogação por parte dos titulares, ou ainda cometer algum vício de consentimento, em razão das inúmeras formalidades que devem ser observadas.

Como será abordado no tópico a seguir, a gestão do consentimento que deve ser feita pelos empresários, pode ser custosa e problemática, implicando em sérios riscos, principalmente quando se utiliza o consentimento de modo genérico, em discrepância com o previsto na LGPD.

4 USO DO CONSENTIMENTO GENÉRICO COMO RISCO EMPRESARIAL E A GOVERNANÇA DE DADOS

O presente estudo é voltado às operações de tratamento no âmbito empresarial, ou seja, destina-se aos empresários que tratem dados pessoais em suas atividades empresariais, embora a Lei Geral de Proteção de Dados abarque todas as atividades de tratamento, independentemente se realizadas ou não no âmbito empresarial, estatal, se feitas por pessoas físicas ou jurídicas.

No cenário atual, em que as organizações estão inseridas na famigerada “Sociedade da Informação”, na qual os dados pessoais são considerados como “novo petróleo” e são utilizados para o desenvolvimento de novas tecnologias e soluções

empresariais, é cada vez mais frequente que certas atividades empresariais dependam, quase que exclusivamente, do tratamento de dados pessoais, seja em meio físico ou digital.

Aliás, neste contexto da sociedade informacional, não há como visualizar atividade empresarial que não realize tratamento de dados, seja na relação com clientes, fornecedores, dos quais ainda que se tratar de pessoa jurídica haverá representantes pessoa natural e suas informações, ou mesmo diante dos seus colaboradores. O correto é que sempre haverá tratamentos de dados pessoais.

Nesse contexto, como mencionado anteriormente, a terceira geração de leis de proteção de dados pessoais se concentrou na criação de mecanismos para conferir ao indivíduo o controle do fluxo das suas informações, e o principal meio criado foi o consentimento, ato em que ficaria a cargo do indivíduo autorizar ou não as organizações utilizarem os seus dados pessoais.

Não obstante a sua importância para a consolidação da disciplina relacionada à proteção de dados, atualmente, as conjecturas que envolvem o paradigma do consentimento, no cenário atual, demonstraram que são insuficientes para, de fato, garantir ao indivíduo o controle sobre o fluxo dos seus dados pessoais. (SCHERTEL e FONSECA, 2020, p. 528)

Por esta razão, a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), inspirada no *General Data Protection Regulation*, o regulamento geral de proteção de dados da Europa, trouxe outras hipóteses que possibilitam as empresas justificarem as operações de tratamento de dados pessoais de suas atividades empresariais, todas previstas no art. 7º, da lei brasileira.

Como já mencionado alhures, a hipótese legal consentimento é apenas uma das 10 (dez) hipóteses legais, dentre as quais não há hierarquia. Não obstante, o consentimento ainda é a hipótese que tende a trazer maior segurança jurídica ao controlador dos dados pessoais, o qual detém a incumbência de provar que o obteve em consonância com a LGPD.

Isso porque a LGPD estabelece uma série de requisitos e formalidades para que esta hipótese legal seja legítima, conforme exposto no tópico anterior. Dito isso, é

importante que o empresário tenha em mente que a utilização do consentimento não consistirá em uma autorização genérica, pois, isto torna o consentimento nulo, e conseqüentemente, o tratamento de dados pessoais deve ser encerrado.

Assim, no caso de uma operação de tratamento justificada pela coleta do consentimento de forma genérica, leia-se, em discrepância com a LGPD, seja pela ausência de manifestação livre, informada ou inequívoca, sendo esta essencial e necessária para a continuidade de determinada atividade empresarial, tal irregularidade cometida pelo empresário traz sérios danos ao seu negócio, fazendo com que enfrente problemas jurídicos, financeiros ou sociais.

Este exemplo retrata apenas um dos riscos que o empresário corre ao justificar as atividades de tratamento vinculadas ao seu negócio, pela hipótese legal do consentimento, de forma genérica. Pode-se citar, ainda, as sanções administrativas que a Autoridade Nacional de Proteção de Dados pode aplicar ao empresário que infringir alguma norma prevista na LGPD.

Dispostas no art. 52, da LGPD, uma das principais e mais noticiadas sanções, é a multa (inc. I e II), de até 2% (dois por cento) do faturamento da empresa, limitada a cinquenta milhões. Outrossim, engana-se o empresário que pensa ser esta a sanção mais severa, uma vez que as demais estão relacionadas à suspensão, paralização e bloqueio da operação de tratamento irregular ou dos dados pessoais tratados, podendo, no pior cenário, o empresário ser proibido de tratar dados pessoais (inc. XII) o que implicaria na não atividade empresarial, desencadeando uma crise gerencial que poderia resultar em encerramento da atividade.

Evidente que a utilização genérica do consentimento para justificar as operações de tratamento não gerará, a princípio, a aplicação da sanção mais severa prevista nos incisos do art. 52, da LGPD. Por outro lado, é outro risco que adiciona ao negócio do empresário que faz disto uma prática recorrente, pois, pode ter sua atividade paralisada, caso esta dependa deste tratamento de dados pessoais irregular.

De forma a endossar este entendimento de que o consentimento utilizado de forma genérica pelo empresário traz riscos à sua atividade empresarial, importante trazer a baila os tratamentos de dados pessoais dos colaboradores. À medida que o empregador

necessita tratar os dados pessoais de seu empregado, seja no momento da contratação, seja pelos atos rotineiros do setor de Recursos Humanos, seja por alguma necessidade em específico de coletar e compartilhar os dados destes, a opção pelo consentimento para justificar estas operações de tratamento pode ser considerada nula.

Isso porque o consentimento, na grande parte das vezes, não será “livre”, em razão da subordinação que existe na relação entre empregado e empregador, motivo pelo qual o empresário deve ficar atento a qualquer atividade de tratamento que envolva seus colaboradores, tendo em vista que o empresário poderá ser responsabilizado pela atividade de tratamento que o empregado alegar ter causado danos, pois, “consentiu” com aquele tratamento dos seus dados pessoais por ter o receio de sofrer alguma punição ou a própria demissão.

Neste aspecto, na prática ao empresário cumpriria analisar se o consentimento é a melhor e mais adequada base legal para o referido tratamento e não outra listada no art. 7º da LGPD.

Portanto, são vários os riscos que a utilização do consentimento de forma genérica traz ao empresário. Passado esse ponto, ressalta-se que o empresário deve levar em conta todo o ciclo de vida dos dados pessoais, de modo que quando se utiliza o consentimento como justificativa de um tratamento, é preciso ser feita a sua gestão, como exige a LGPD.

A generalidade do consentimento não é levada em conta apenas no início do ciclo de vida dos dados pessoais, como na coleta, transmissão e compartilhamento, mas também ao final deste ciclo, seja pelo armazenamento, eliminação ou modificação dos dados pessoais, principalmente com o que se faz após a utilização dos dados pessoais quando a finalidade precípua para qual se obteve o consentimento se esvaiu-se.

Avaliar o ciclo de vida dos dados pessoais das atividades empresariais relaciona-se diretamente à Governança dos dados pessoais, e mapear quais as hipóteses legais que justificam os tratamentos de dados pessoais que ocorrem na empresa faz parte desta Governança. Assim, há também riscos à Governança a utilização do consentimento de

forma genérica, principalmente em relação às boas práticas de governança, definidas pelo art. 50^o, da LGPD.

A utilização de forma genérica do consentimento, faz com que o titular de dados pessoais não tenha consciência de como os seus dados serão tratados pelo controlador. Em outras palavras, é como outorgassem poderes ao controlador fazer o que bem entender com seus dados pessoais, em dissonância ao que prevê a LGPD, razão pela qual as sanções administrativas foram criadas, a fim de mitigar tal prática (art. 52).

Por isso a LGPD estabelece que as organizações implementem uma Governança dos dados pessoais, com o objetivo de fornecer mecanismos aos titulares continuarem no controle do fluxo de seus dados, de maneira a gerar transparência a estes, através da informação das finalidades e maneiras pelas quais são tratados os dados pessoais.

Isso posto, conclui-se, então, que a autodeterminação-informativa foi evoluindo ao longo do tempo. Inicialmente, o consentimento foi a ferramenta criada. Posteriormente, à medida em que este consentimento foi perdendo força com os avanços tecnológicos, a autodeterminação informacional se perdeu em meio às assimetrias do mercado informacional (Bioni, 2019), motivo pelo qual foi necessário a criação de um conjunto de regras que seja aplicado a qualquer operação de tratamento, independente da hipótese legal utilizada para justificá-la.

Nessa linha, diante deste conjunto de regras, no Brasil materializada pela LGPD, a Governança de dados pessoais exige que o empresário estabeleça uma série de regramentos internos e externos, observando cada uma das fases do ciclo de vida dos dados pessoais, bem como deve estabelecer uma relação de transparência no relacionamento com o titular dos dados pessoais (Maldonado, 2021, p. 183).

No entanto, esta exigência trazida pela LGPD não é observada pelo empresário que justifica os tratamentos de dados pessoais por meio do consentimento, de forma

⁹ Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

genérica, sem observar todas as suas formalidades legais. Assim, isto se traduz em um risco à Governança dos dados pessoais, além de trazer riscos à própria atividade empresarial.

Portanto, o empresário que pratica esta irregularidade em suas atividades empresariais está sujeito a riscos que podem, no pior cenário, inviabilizar a sua operação. Assim como tal incompatibilidade com a LGPD pode violar gravemente a personalidade destes indivíduos sujeitos às operações de tratamento irregulares, seja pela inadequada divulgação ou utilização de informações armazenadas a seu respeito, por isso os dados merecem tutela jurídica de modo a assegurar a sua liberdade e igualdade (Schertel Mendes, 2014).

Por fim, as considerações acima, além de serem imprescindíveis aos controladores dos dados pessoais, devem ser observadas com muita cautela pelos operadores dos dados pessoais, pois atribui-se parte dos riscos a ambos os papéis, haja vista que o empresário pode figurar como qualquer dos agentes de tratamento de dados pessoais.

5 CONSIDERAÇÕES FINAIS

O consentimento sempre foi o ponto central de legislações relacionadas à proteção de dados, como visto no presente estudo, e era enxergado como a principal ou única ferramenta de efetivação da autodeterminação informativa. Com o advento da Lei Geral de Proteção de Dados, inspirada na legislação europeia, foram criadas ferramentas para o exercício da autodeterminação informativa e o consentimento passou apenas uma de dez hipóteses legais que justificam os tratamentos de dados pessoais.

Em que pese estas inovações trazidas pela LGPD, o consentimento ainda desempenha importante papel no cenário de privacidade e proteção de dados, pois ainda é o mecanismo mais forte para o indivíduo ter controle do fluxo dos seus dados pessoais, razão pela qual a legislação brasileira criou uma série de requisitos para que a coleta do consentimento seja feita.

Muito embora exista atualmente dez hipóteses legais para as organizações justificarem as suas operações de tratamento de dados pessoais, criou-se uma cultura,

antes do advento da LGPD, de que a única maneira de se fazer isto era por meio da coleta do consentimento, fazendo com que tal hipótese legal fosse banalizada, sendo efetuada de maneira genérica, em total discrepância com a LGPD.

Tal prática generalizada entre os empresários faz com que assumam riscos desnecessários, como destacado no tópico anterior. Assim sendo, o presente estudo chegou à conclusão de que os empresários que utilizarem-se do consentimento como única forma de legalizar as operações de tratamento das suas atividades, tendem a sofrer graves consequências, ligadas à governança de dados e ao próprio negócio em si, motivo pelo qual é recomendável a adequação dos fluxos de dados pessoais da empresa à LGPD.

REFERÊNCIAS

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

BIONI, Bruno Ricardo. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 20 out. 2023.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. v. 2. abril. 2022.

BRASIL. CONSTITUIÇÃO FEDERAL DA REPÚBLICA DO BRASIL DE 1988. Promulgada pelo Congresso Nacional. **Diário Oficial da União**, Brasília em 5 de outubro de 1998.

BRASIL. LEI Nº 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD). Decretada pelo Congresso Nacional e sancionada pela Presidência da República. **Diário Oficial da União**, Brasília em 15 de agosto de 2018.

BRASIL. LEI Nº 12.414/2011. Lei do Cadastro Positivo. Decretada pelo Congresso Nacional e sancionada pela Presidência da República. **Diário Oficial da União**, Brasília em 10 de junho de 2011.

BRASIL. LEI Nº 8.078/1990. Código de Defesa do Consumidor. Decretada pelo Congresso Nacional e sancionada pela Presidência da República. **Diário Oficial da União**, Brasília em 12 de setembro de 1990.

BRASIL. LEI Nº 12.965. Marco Civil da Internet. Decretada pelo Congresso Nacional e sancionada pela Presidência da República. **Diário Oficial da União**, Brasília em 23 de abril de 2014.

DINIZ, Maria Helena. **Curso de direito civil brasileiro: teoria geral do direito civil**. v.1. São Paulo: Editora Saraiva, 2022. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598698/>. Acesso em: 21 out. 2023.

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 novo direito fundamental**. São Paulo: Saraiva, 2014.

MENDES, L. S.; FONSECA, G. C. S. **Proteção de Dados Para Além do Consentimento: tendências contemporâneas de materialização**. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2022.

FEIGELSON, B.; SIQUEIRA, A. H. A. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega. **LGPD: Lei Geral de Proteção de Dados Pessoais: Manual de Implementação**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

MALDONADO, V. N.; BLUM, R. O. **LGPD: Lei Geral de Proteção de Dados Pessoais comentada**. 3.ed. São Paulo: Thomson Reuters Brasil, 2021.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 3.ed. São Paulo: Saraiva Educação, 2021.