DADOS SENSÍVEIS E CONSENTIMENTO: UM PANORAMA NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

SENSITIVE DATA AND CONSENT: AN OVERVIEW OF THE BRAZILIAN GENERAL DATA PROTECTION LAW

Maria Regina Detoni Cavalcanti Rigolon Korkmaz*

RESUMO: *A contemporaneidade lança novos desafios no cenário dos progressivos avanços tecnológicos e da digitalização de múltiplos aspectos da vida humana, no qual a proteção de dados pessoais, sobretudo de dados sensíveis, representa importante chave para a garantia de diversos direitos fundamentais. A partir de uma perspectiva exploratória e qualitativa, o presente estudo teve por fim investigar o debate que se apresenta na interseção entre a proteção de dados sensíveis e o consentimento na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 de 2018). Partindo da premissa de que os dados sensíveis apresentam, em sua ontologia, uma potencialidade discriminatória acima da média dos demais dados pessoais, o presente artigo pretendeu analisar os limites do consentimento, tal como ele está delineado na regulação brasileira. Em última análise, o estudo apresentou parâmetros da interface entre o legítimo exercício da autodeterminação informativa, no que se relaciona ao tratamento de dados sensíveis, e o arcabouço protetivo estabelecido na lei, que prevê critérios de proteção da pessoa humana para além da esfera meramente individual.*
Palavras-chave: *Lei Geral de Proteção de Dados Pessoais; dados sensíveis; proteção de dados; discriminação.*

ABSTRACT: *Contemporaneity presents society with new challenges within the scenario of progressive technological advances and the digitization of multiple aspects of human life, in which the protection of personal data, especially sensitive data, represents an important key for the enforcement of several fundamental rights. From an exploratory and qualitative perspective, the study aims to investigate the debate that presents itself at the intersection of the protection of sensitive data and the consent in the Brazilian General Data Protection Law (Law No. 13,709 of 2018). Based on the assumption that sensitive data presents, in its ontology, a discriminatory potential above the average of other personal data, this article intends to analyze the limits of consent, as it is outlined in the Brazilian regulation. Ultimately, the study presents parameters of the interface between the legitimate exercise of informational self-determination, regarding sensitive data processing, and the protective framework established in the law, which provides criteria for the protection of the human person beyond the individual sphere.*
Keywords: *Brazilian General Data Protection Law; sensitive data; data protection; discrimination.*

SUMÁRIO: 1 INTRODUÇÃO. 2 DA PRIVACIDADE À PROTEÇÃO DE DADOS SENSÍVEIS. 3 NOTAS SOBRE O CONSENTIMENTO NO ÂMBITO DA PROTEÇÃO DE DADOS PESSOAIS. 4 O CONSENTIMENTO PARA O TRATAMENTO DE DADOS SENSÍVEIS NA LGPD. 5 CONCLUSÃO. REFERÊNCIAS.

1 INTRODUÇÃO

A relevância assumida pelos dados pessoais na contemporaneidade lança-nos a necessidade de equilibrar a sua utilidade para os valores compartilhados socialmente e a proteção da pessoa a partir dos seus dados, que assume a natureza de direito fundamental. A ubiquidade e as crescentes potencialidades do fenômeno de processamento de dados redimensionam esse desafio.

Para além da privacidade e da proteção de dados pessoais, ganha relevância a tutela dos dados pessoais sensíveis como a defesa do princípio da igualdade material, na medida em que está em questão não somente a esfera privada da pessoa, mas a sua posição na organização social, política e econômica (RODOTÀ, 2008). Os dados sensíveis se referem

* Universidade Federal de Juiz de Fora, Faculdade de Direito, Departamento de Direito Privado, Juiz de Fora, MG, Brasil.
https://orcid.org/0000-0002-3838-464X

às opções e características fundamentais da pessoa e são, portanto, dotados de uma "potencial inclinação para serem utilizados com finalidades discriminatórias", como esclarece Rodotà (2008, p. 96).

Historicamente, a ontologia dos dados sensíveis tem a capacidade de fundamentar um regime jurídico específico nas normas sobre proteção de dados pessoais, o que se verificou no caso do Regulamento Europeu de Proteção de Dados 2016/679 (*General Data Protection Regulation,* sigla em inglês GDPR) e da regulação brasileira: a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709 de 2018 – sigla LGPD).

Especificamente, em princípio previsto nesses diplomas como uma das hipóteses legais que podem autorizar o tratamento dos dados sensíveis, o consentimento deve ser analisado com maior profundidade, porque, embora figure como um instrumento para a construção da esfera privada, apresenta limitações quando confrontado com a natureza de direito fundamental da proteção de dados pessoais e com os riscos subjacentes ao tratamento de dados, não raro majorados em face de dados sensíveis.

Portanto, com a referência teórica de Rodotà (2008, 2019), aliada ao propósito de investigação exploratória e qualitativa sobre o consentimento para o tratamento dos dados sensíveis na LGPD, o presente trabalho tem por objetivo lançar considerações sobre os seus contornos e limites na regulação. Em caráter complementar para a investigação, determinados pontos do GDPR sobre o tema foram apresentados, tendo em vista a influência do modelo europeu na regulação brasileira.

Para tanto, após a presente introdução, será endereçada, em linhas centrais, a evolução da noção de privacidade até o debate sobre proteção de dados pessoais, no qual se situa a categoria dos dados sensíveis. Após, serão apresentadas notas sobre o instituto do consentimento, sobretudo no âmbito da proteção de dados pessoais. Posteriormente, será realizada uma análise do consentimento para o tratamento dos dados sensíveis no paradigma da LGPD, seguida da conclusão do presente artigo.

2 DA PRIVACIDADE À PROTEÇÃO DE DADOS SENSÍVEIS

A privacidade é uma noção cultural induzida no curso do tempo e dependente de bases sociais, culturais e políticas (DONEDA, 2006). O célebre artigo "The right to privacy" , de Warren e Brandeis (1890), apresentado no contexto tecnológico da câmera fotográfica portátil e do avanço da imprensa, trouxe a defesa da esfera intangível da pessoa, com a percepção de que a proteção integral da pessoa e da propriedade, na referência do *common law*, não era alheia ao momento em que se situava. Os autores apresentaram, então, que a privacidade seria parte de um direito mais geral de imunidade da pessoa (WARREN; BRANDEIS, 1890), deslocando-a para uma perspectiva pessoal, embora ainda fosse marcada por uma lógica proprietária.

Com os avanços tecnológicos, o conceito de informação pessoal passou de algo pressuposto, enquanto meio para a proteção da privacidade diante de informações e documentos privados, para progressivamente definir-se como um conceito central para esse direito (MACHADO; DONEDA, 2018). É a partir desse cenário que a privacidade, como direito complexo e ampliado que comportou a progressiva inclusão de novos aspectos de liberdade no seu âmago, passa a abranger a noção de autodeterminação informativa, definida por Rodotà (2008, p. 15) como o "direito de manter controle sobre as suas informações e de determinar a maneira de construir sua esfera particular".

Com efeito, a partir de L. M. Friedman e J. Rosen, Rodotà (2008, p. 15) reconhece que a coleta de dados e a aptidão de gerar perfis sociais e individuais discriminatórios indicam para a privacidade como "a proteção de escolhas de vida contra qualquer forma de controle público e estigma social", a implicar a necessária "reivindicação de limites que protegem o indivíduo do direito de não ser simplificado, objetivado e avaliado fora de

contexto". A categoria dos dados sensíveis estaria situada no "núcleo duro" da privacidade (RODOTÀ, 2008, p. 95-96).

Para além de uma definição baseada no direito individual de controlar as próprias informações[1], a proteção de dados pessoais se desdobra da privacidade e assume paradigmas próprios (DONEDA, 2006). Apesar de compartilhar com a privacidade o mesmo fundamento ontológico que é a dignidade da pessoa humana, a proteção de dados passa a ostentar uma dimensão coletiva, essencialmente dinâmica e com um caráter significativamente objetivo (RODOTÀ, 2008, p. 85-88). Tanto é assim que as normas sobre proteção de dados pessoais elencam diversas hipóteses que autorizam o seu tratamento independente da vontade da pessoa quando estiverem em jogo outros valores merecedores de tutela, extrapolando, assim, o critério da vontade meramente individual.

Spiros Simitis evidencia que a evolução histórica da proteção de dados pessoais foi acompanhada da discussão sobre os dados sensíveis. A primeira legislação nacional a respeito do tema na Suécia, em 1973, abordou a categoria dos dados sensíveis, assim como as normas que a seguiram na França, Dinamarca, Noruega e Luxemburgo (SIMITIS, 1990 *apud* MENDES, 2014), tendo sido definitivamente consagrada na Convenção 108, editado pelo Conselho da Europa, em 1981.

A previsão dessa categoria nas primeiras leis sobre proteção de dados era acompanhada de disposições mais severas que o regime dos dados pessoais não sensíveis. Esse *standard* protetivo maior dos dados sensíveis se refletia nos seguintes aspectos: (i) ampliação das exigências legais com relação ao consentimento; (ii) ampliação de exigências legais para o tratamento desses dados pelo responsável, como a intensificação das medidas de segurança; e (iii) aumento do controle por parte da autoridade administrativa para a autorização de armazenamento, processamento e circulação dos dados (MENDES, 2014).

A percepção de que o armazenamento, o processamento e a circulação de certos tipos de dados acarretariam maior risco à personalidade, especialmente diante de práticas discriminatórias, explicam a conformação jurídica mais rigorosa dos dados sensíveis (MENDES, 2014). Em decorrência, emergiu a necessidade de exorbitar os cânones tradicionais então relacionados à privacidade, em prol de outro valor digno de tutela: a igualdade material (DONEDA, 2006). Assim, quando a privacidade era compreendida em termos de autonomia e liberdade, os dados sensíveis elevaram o debate para termos de igualdade (MENDES, 2014). Na síntese de Rodotà (2019, p. 36, tradução nossa):

> É necessário enfatizar, de fato, que os dados sensíveis são aqueles relativos a saúde e vida sexual, as opiniões e ao pertencimento étnico ou racial, com uma lista semelhante às encontradas nas normas relativas a casos de discriminações. Assim, somos confrontados com algo que vai além da simples proteção da vida privada e se apresenta como defensor da mesma igualdade entre as pessoas[2].

[1] O "dado" assume uma conotação primitiva, como uma informação em estado potencial antes de ser transmitida, enquanto a "informação" se refere a algo além da representação contida no dado, chegando ao limiar da cognição (DONEDA, 2011, p. 94).

[2] No original: "È necessario sottolineare, infatti, che i dati sensibile sono quelli che riguardano la salute e la vita sessuale, le opinioni e l'appartenenza etnica o razziale, con una elencazione analoga a quella che si trova nelle norme riguardanti i casi di discriminazione. Siamo così di fronte a qualcosa che eccede la semplice tutela della vita privata e si pone come presidio della stessa eguaglianza tra le persone".

Embora qualquer dado pessoal possa ser tratado com finalidades discriminatórias[3], o potencial lesivo do tratamento dos dados sensíveis apresenta maior risco que a média, seja para a pessoa, seja para a coletividade (DONEDA, 2006). A rigor, a categoria dos dados sensíveis é fruto de uma observação pragmática desse desnível de potencialidade lesiva entre os dados considerados sensíveis e os demais dados pessoais.

Com fundamento na possibilidade de discriminação, os dados sensíveis se associam a conjunturas em que podem estar presentes potenciais violações de direitos fundamentais, de forma que protegê-los permite a efetivação de diversos direitos como saúde, liberdades comunicativas, religiosa, de associação, entre outros (MULHOLLAND, 2018).

Com efeito, a LGPD normatizou a categoria[4] dos dados sensíveis como aquelas informações "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" (BRASIL, 2018).[5] Por outro lado, adotou-se na norma um conceito amplo de dado pessoal, como sendo qualquer "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

Na regulação brasileira, uma vez qualificado o dado pessoal como sensível, atrai-se um regime jurídico particularizado, com um *standard* protetivo significativamente acima do reservado aos demais dados pessoais. Em específico, como dito, a maior qualificação do consentimento representou um eixo estratégico para a ampliação da proteção conferida à pessoa a partir dos dados sensíveis, instituto esse que deve ser endereçado.

3 NOTAS SOBRE O CONSENTIMENTO NO ÂMBITO DA PROTEÇÃO DE DADOS PESSOAIS

Como já advertia Rodotà (2008), as correntes noções de privacidade não são suficientes para solucionar o problema da circulação de informações e cada vez mais surgem casos complexos nos quais não está em questão apenas o poder da pessoa em determinar a sua esfera privada. Embora a privacidade tenha evoluído para além de uma concepção patrimonial, com a inserção no seu conteúdo da autodeterminação informativa, o seu exercício ainda é marcado por forte componente subjetivo, de forma que cada individualidade, em última análise, determinará a sua exposição no tecido social.

Em outros termos, de forma geral para a proteção dos dados pessoais, porém mais profundamente para os dados sensíveis, a prevalência do subjetivismo do titular pode se concretizar em fatores limitadores do livre desenvolvimento da personalidade, além de comprometer a própria esfera coletiva e o atendimento a interesses socialmente relevantes. Primeiro, com eventual uso indiscriminado dos dados pessoais, no paradigma do *big data* e do avanço de sistemas cada vez mais complexos, não raro estaremos diante da falta de compreensão pela pessoa à qual os dados se referem dos riscos subjacentes à circulação de um dado sensível, que poderá prejudicá-la, ainda que acobertada pela opacidade do tratamento dos dados. Segundo, em atenção à perspectiva solidarista, não é defensável o

[3] A propósito, especialmente sobre a prática de *clustering*, a partir da qual a discriminação se baseia a partir da criação de categorias socialmente invisíveis, cf. Rouvroy (2016).

[4] Sobre uma leitura ampliada da categoria dos dados sensíveis na LGPD, cf. Negri e Korkmaz (2019) e Mulholland (2020).

[5] É possível identificar um paralelismo entre os dados considerados sensíveis na LGPD e no GDPR. Nesse sentido, o artigo 9º, item 1, do GDPR dispõe que: "É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa" (UNIÃO..., 2016, p. 38).

império da vontade individual, ainda mais se considerada a vulnerabilidade da pessoa frente ao mercado e ao Estado em razão da forte assimetria informacional.

Assim, a princípio, o consentimento é um poder conferido à pessoa para modificar a sua esfera jurídica, podendo ser compreendido como síntese da atuação da autonomia privada e como instrumento por excelência para a manifestação da escolha individual, inclusive no campo das diversas configurações da personalidade (DONEDA, 2006).

No entanto, são recorrentes os debates no campo da proteção de dados pessoais sobre a fragilidade do consentimento enquanto instrumento de tutela. Embora seja um caminho entre a *regulation* e a *deregulation*, são múltiplos os perigos de erigir o consentimento como um pilar para a proteção de dados (RODOTÀ, 2008). De plano, é evidente o risco de transpor o instituto do consentimento do seu contexto tradicional dos mecanismos negociais para o âmbito da proteção de dados sem proceder a uma adequação, especialmente porque a adaptação de uma estrutura formal a uma realidade que apresenta com o seu meio de origem uma semelhança enganosa pode compreender uma escolha ideológica (DONEDA, 2006). Eventual leitura do consentimento, através de uma matriz negocial, acabaria por reforçar o sinalagma entre o consentimento para o tratamento dos dados pessoais e uma vantagem econômica por parte daquele que consente, fortalecendo um esquema proprietário para os dados pessoais (TEPEDINO; TEFFÉ, 2019).

Nesse sentido, com base na regulação reservada ao consentimento é possível identificar a natureza do sistema de proteção de dados pessoais. Se o sistema assumir uma índole patrimonialista, o consentimento terá uma função predominantemente "legitimadora" para colocar os dados no mercado e, em um arranjo extremo, conduzir estes dados a um processo de *commodification*, isto é, transformá-los em *commodity,* como aponta Doneda (2006). Compreendida a privacidade como uma liberdade negativa – com a atribuição de autodeterminação ao indivíduo sobre a sua esfera privada –, o consentimento é constituído como elemento essencial do exercício deste poder (DONEDA, 2006).

Todavia, a falsa premissa de conceder o consentimento como instrumento para determinar livremente a utilização dos dados pessoais poderia, por parte do Estado, representar um "falso álibi" para não interferir em situação que demandaria a sua atuação positiva na defesa de direitos fundamentais[6]. Além disso, a relação de dependência verificada entre o consentimento e a fruição de bens e serviços muitas vezes acrescenta à sua concessão a autorização para o uso secundário de dados (RODOTÀ, 2008).

Vale dizer, a análise do consentimento deve ser situada no paradigma de que a proteção de dados diz respeito à personalidade, e não à propriedade (RODOTÀ, 2008), o que se apresenta como critério interpretativo e integrativo fundamental de marcos regulatórios com essa matriz, como é o caso brasileiro. A rigor, o papel do consentimento para a proteção de dados pessoais deve ser ponderado, sob pena de, amparado na estrita tecnicidade, neutralizar a atuação de direitos fundamentais (DONEDA, 2006).

[6] Como destaca Rodotà (2008, p. 37): "a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejoso de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de jogo do qual somente poderá sair como perdedor. A atenção, consequentemente, deve deslocar-se dos meios de reação individual para instrumentos de controle social: e poderá ocorrer que, seguindo esse caminho, alguns meios que estavam tradicionalmente à disposição do indivíduo venham ser perdidos; perda, no entanto, que pode ser compensada pela criação, em nível coletivo, de um aparato de controle globalmente mais incisivo e vigilante do que o atual".

4 O CONSENTIMENTO PARA O TRATAMENTO DE DADOS SENSÍVEIS NA LGPD

A possibilidade de desmembrar o consentimento em espécies com requisitos próprios, de acordo com a natureza dos interesses em um certo perfil de tratamento de dados pessoais, é o que estabelece um regime diferenciado para o consentimento relativo ao tratamento de dados sensíveis, aproximando-o do seu campo de interesses (DONEDA, 2006).

Assim, no regime comum de proteção de dados pessoais, a LGPD define o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". De outra parte, para o tratamento dos dados sensíveis, a normativa estabelece *adicionalmente* uma qualificação do consentimento para exigir que seja fornecido "de forma específica e destacada, para finalidades específicas", de acordo com o art. 11, inciso I (BRASIL, 2018).

A rigor, por detrás de toda adjetivação ou qualificação do consentimento está uma modulação da carga participativa exigida de cada pessoa para o tratamento dos seus dados (BIONI, 2019). Em face da potencialidade lesiva subjacente ao tratamento dos dados sensíveis, portanto, a carga participativa deve ser máxima, o que se relaciona com o grau de consciência a respeito do tratamento por parte do titular, como verdadeira advertência dos riscos anormais daquela prática, na observação de Bioni (2019).

No regime geral do consentimento na LGPD – extensível aos dados sensíveis –, é exigida a sua caracterização como livre. Ao se referir ao consentimento livre, quer-se assegurar o poder de o titular escolher entre aceitar ou não a utilização dos seus dados, sem quaisquer intervenções ou situações que viciem o seu consentimento, com o imperativo de averiguar a assimetria entre as partes envolvidas (TEPEDINO; TEFFÉ, 2019).

Com fundamento na liberdade das escolhas pessoais, o seu exercício livre manifesta-se menos no momento do consentimento em si, do que na possibilidade de concedê-lo ou não, e reside justamente neste poder que se limitado pela estrutura negocial perderia a sua razão de ser (DONEDA, 2006). Nesse sentido, de acordo com o relatório de maio de 2020 do Comitê Europeu de Proteção de Dados (em inglês European Data Protection Board, sigla EDPB), foi sustentado que o consentimento não é livre quando existir qualquer elemento de coação, pressão ou inabilidade de exercer livremente a vontade (EUROPEAN..., 2020).

Como expressamente destacado no Considerando 42 do GDPR, não há consentimento livre se o titular dos dados não dispuser de uma "escolha verdadeira ou livre", ou se não puder recusar ou retirar o consentimento sem prejuízo próprio, o que deve ser demonstrável pelo controlador, de acordo com o European Data Protection Board (2020, p. 13). Em decorrência, o Considerando 43 destaca:

> [...] Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução (UNIÃO..., 2016, p. 8).

Na LGPD, por sua vez, foi estabelecido que se o tratamento de dados pessoais for apresentado como condição para o fornecimento de produto ou serviço ou para exercício de direito, o titular deverá ser informado com destaque sobre esse fato, bem como sobre os meios dos quais poderá se valer para o exercício dos direitos elencados no art. 18, de acordo com o art. 9º, § 3º (BRASIL, 2018). Como apontam Tepedino e Teffé (2019, p.

300), é possível ler esse dispositivo como uma proposta de regulação da lógica binária das políticas chamadas de tudo ou nada (*take-it-or-leave-it-choice*), nas quais, para ter acesso a um determinado serviço ou produto, o indivíduo deve aceitar todas as condições apresentadas. Contudo, é de se questionar a suficiência da informação em destaque sobre o condicionamento do titular dos dados, quando está em questão a real possibilidade de não consentir para o tratamento dos dados pessoais. Aliás, o direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, previsto no inciso VIII, do art. 18, embora funcione como um instrumento de transparência, não parece significativo em termos de liberdade no ato de consentir.

Com o propósito de garantir uma autodeterminação por parte do indivíduo de quais dados pessoais poderão ser utilizados, para quais finalidades e sob quais termos, ganha relevância o chamado "consentimento granular" como forma de permitir uma oxigenação dos processos de tomada de decisão, através do qual a pessoa pode emitir autorizações fragmentadas no tocante ao fluxo de seus dados, de acordo com Bioni (2019). Nessa perspectiva, abre-se margem "para que o controle dos dados seja fatiado de acordo com cada uma das funcionalidades que são ofertadas e se deseja ter e que demandam, respectivamente, tipos diferentes de dados" (BIONI, 2019, p. 197-198). Essa granularidade é apontada como um fator caracterizante da própria liberdade no ato de consentir, como pode ser extraído do citado Considerando 43, do GDPR.

A propósito, é possível inferir a fragilidade do consentimento como instrumento legitimador do tratamento de dados sensíveis em vista do princípio da não discriminação, elencado na LGPD[7], que poderia deslegitimar um tratamento de dados consentido, mas que pudesse gerar uma discriminação ilícita ou abusiva em desfavor da pessoa. Vale dizer, está em debate quais são os contornos de um consentimento livre, quando não raro a pessoa não tem consciência da potencialidade lesiva do uso daquele dado, sobretudo diante dos exponenciais avanços tecnológicos. A questão da assimetria informacional e da vulnerabilidade do titular dos dados nesse cenário valoriza o papel do qualificador "informado" do consentimento, como a seguir será endereçado. Particularmente nessa interface, ressalte-se que a autonomia humana pode ser limitada pela inabilidade de a pessoa compreender informações ou fazer decisões adequadas (TSAMADOS *et al.*, 2021).

Na realidade, Rodotà (2008) já sustentava a impossibilidade de operar o consentimento em todas as situações, bem como de fundar no consentimento a própria definição de privacidade. Diante de fortes desníveis de poder, o consentimento individual é profundamente limitado, a exemplo do recolhimento pelo empregador de convicções políticas e sindicais do empregado, do requerimento de exames de doenças como HIV, informações genéticas, entre outros, qualificados como dados sensíveis.

Tendo em vista a frequente fragilidade do qualificador "livre" do consentimento no âmbito da proteção de dados pessoais, o aumento ou a redução do papel decisional do titular se erige como mecanismo de proteção da pessoa, como sustenta Doneda (2006). Isso porque determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no mais elevado alto grau, que não pode ser atendido exclusivamente por uma decisão individual (DONEDA, 2006). Nessa direção, a alínea "a" do item 2 do art. 9 do GDPR estabelece que o direito da União ou de um Estado-Membro na União Europeia pode afastar o consentimento como hipótese legitimadora do tratamento de um dado sensível (UNIÃO..., 2016). No entanto, não há uma previsão análoga na LGPD.

Em outro eixo, a LGPD exige no regime jurídico geral do consentimento que este seja *informado*. O objetivo da previsão é o de prover o titular dos dados das informações que se façam necessárias ao entendimento das circunstâncias adjacentes ao tratamento dos seus

[7] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018).

dados pessoais. Em última análise, como destacado no relatório do European Data Protection Board, se o controlador não apresenta informação acessível, o controle pelo titular dos dados se torna ilusório, tornando inválido, por consequência, o consentimento[8].

A exigência de que o consentimento seja realmente informado toma por premissa, no mínimo, a leitura dos termos de consentimento para tratamento de dados, os quais devem ser fidedignos às práticas pertinentes ao tratamento. Ocorre que a forma de apresentação dos usuais termos de consentimento se dá de maneira não atrativa para o titular dos dados: não raro, são textos extensos que se valem de uma linguagem elaborada e que visualmente não estimulam a leitura do seu conteúdo[9].

O consentimento deve estar inscrito em uma constelação de circunstâncias para ser pleno e válido, demandando "uma temporalidade estrita ao uso previamente informado e esclarecido, o qual tenha sido ampla e livremente objeto de deliberação de pessoa autônoma" (SARLET; CALDEIRA, 2019, p. 23). Contudo, na conjuntura brasileira são múltiplos os desafios para que essas circunstâncias sejam concretamente verificadas[10].

Nessa direção, o consentimento deve ser avaliado de forma realista diante dos limites gerados pela assimetria informativa e de poder entre aquele que consente e o responsável pelo tratamento dos dados, tendo em vista uma efetiva compreensão das suas implicações[11].

Sarlet e Caldeira (2019) se referem à natureza processual do consentimento, a demandar a garantia de todas as condições, inclusive as temporais e as informacionais, para a livre tomada de decisão em um paradigma de responsabilidade. O princípio da transparência estabelecido na LGPD interfere nesse processo, na medida em que assegura à pessoa "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" (BRASIL, 2018). Segundo Frazão (2018), "o direito à informação está intrinsecamente relacionado ao princípio da transparência e prestação de contas e somente não é absoluto em razão da ressalva mencionada no inciso II, em relação aos segredos comercial e industrial".

---

[8] O European Data Protection Board (2020) sustenta que, no mínimo, para que o consentimento seja considerado informado o titular dos dados deve ter acesso às seguintes informações: identidade do controlador dos dados; finalidade de cada operação de processamento para as quais os dados são requeridos; quais tipos de dados serão coletados e utilizados; a possibilidade de retirar o consentimento; informações sobre o uso dos dados para fins de tomada de decisões automatizadas, quando relevante; possíveis riscos de transferência de dados devido à ausência de uma decisão de adequação e de salvaguardas adequadas. O European Data Protection Board (2020) acrescenta que, a depender das circunstâncias e do contexto do tratamento dos dados, mais informações podem ser necessárias para que o titular genuinamente compreenda o processamento.

[9] Madrigal (2012) relata uma pesquisa realizada no ano de 2008 por Lorrie Faith Cranor e Aleecia McDonald, à época no Carnegie Mellon, identificando que se o titular dos dados fosse ler todos os termos de consentimento a respeito dos seus dados pessoais ao ano gastaria 76 dias de trabalho. Ao calcular um custo hipotético de oportunidade a partir de balizas econômicas, o "custo da privacidade", de acordo com as pesquisadoras, seria de 781 bilhões de dólares no contexto pesquisado dos Estados Unidos, com tendência de crescimento nos dias atuais.

[10] "Três em cada dez jovens e adultos de 15 a 64 anos no País – 29% do total, o equivalente a cerca de 38 milhões de pessoas – são considerados analfabetos funcionais. Esse grupo tem muita dificuldade de entender e se expressar por meio de letras e números em situações cotidianas, como fazer contas de uma pequena compra ou identificar as principais informações em um cartaz de vacinação. Há dez anos, a taxa de brasileiros nessa situação está estagnada, como mostram os dados do Indicador do Alfabetismo Funcional (Inaf) 2018" (Disponível em: https://epocanegocios.globo.com/Brasil/noticia/2018/08/epoca-negocios-tres-em-cada-10-sao-analfabetos-funcionais-no-pais-aponta-estudo.html. Acesso em: 9 ago. 2019).

[11] Nesse sentido, o European Data Protection Board (2020, p. 16) destaca : "A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors".

Um outro ponto que deve ser assinalado na LGPD é que em seu regime comum o consentimento deve ser inequívoco, ao passo que em se tratando de dados sensíveis deve ser específico e destacado. Determinadas imprecisões são apontadas com relação a essa redação da lei. É relevante verificarmos o modelo europeu. De acordo com o item 1 do art. 4 do GDPR, "o consentimento consiste em uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados, aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (UNIÃO..., 2016, p. 34). No regime jurídico dos dados sensíveis, o GDPR prescreve na alínea "a" do item 2 do art. 9 a exigência de que o consentimento seja explícito e para uma ou mais finalidades específicas[12]. Além disso, no Considerando 51 do GDPR, que trata dos dados sensíveis, é feita uma referência ao consentimento *expresso*.

Do ponto de vista da técnica legislativa seria redundante exigir que o consentimento seja específico, na medida em que o princípio da finalidade previsto na LGPD demanda que o tratamento de dados pessoais atenda a propósitos específicos e explícitos, a demandar um direcionamento do próprio consentimento que não pode ser, portanto, genérico (BIONI, 2019). A rigor, a ideia de um consentimento genérico é incompatível com a própria compreensão dos dados pessoais como representação da personalidade.

Apesar da diferença semântica entre a qualificação do consentimento como específico ou expresso e deste último representar melhor o nível de participação pretendido da pessoa com relação ao fluxo dos seus dados, a consequência normativa deve ser a mesma, na medida em que o propósito da qualificação é reservar uma autorização singular por parte da pessoa à qual os dados se referem (BIONI, 2019). Esse consentimento especial deve ser compreendido como um vetor para que haja uma maior assertividade do titular com relação aos movimentos específicos dos seus dados (BIONI, 2019).

Anote-se que a maior assertividade do titular avulta em importância na medida em que se consideram características comuns a processamentos automatizados no atual estado da arte da tecnologia e as ostensivas potencialidades de coleta de dados no cenário de hiperconectividade, como denunciado por Pasquale (2015) na metáfora da *black box.*[13]

Uma outra questão é a qualificação do consentimento como inequívoco no regime comum dos dados pessoais na LGPD[14]. De acordo com Bioni (2019, p. 199-200), por inequívoco entende-se que o consentimento não pode ser ambíguo, mas sim evidente e se dar uma forma clara, ou seja, deve-se verificar um comportamento concludente por parte

[12] É relevante citar o Considerando 32 a respeito do consentimento no GDPR: "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. [...] O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. [...]" (UNIÃO..., 2016, p. 6).

[13] A metáfora apresentada por Pasquale (2015) tem significado dúplice: como monitoramento de dados e como um sistema que trabalha de forma misteriosa, sabemos o *input* e o *output*, mas não se compreende como um se transformou no outro. Deparamo-nos na atualidade com os dois significados, na medida em que somos progressivamente rastreados por empresas e pelo governo, sem que seja assinalado o uso das informações, onde ela pode chegar e as suas consequências, processo permeado de estratégias para a manutenção das *black boxes* que agrava a assimetria informacional.

[14] Sobre a referência de um "ato positivo inequívoco" no GDPR, para um cotejo com a previsão de *consentimento inequívoco* na LGPD, o European Data Protection Board (2020, p. 18-19) pondera que: "The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration. [...] Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice. [...] In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR".

da pessoa à qual os dados se referem, compreendido como uma "ação afirmativa que não deixe dúvidas sobre a intenção do cidadão".

Para os dados sensíveis, não basta que o consentimento seja inequívoco como no regime comum, devendo também ser *expresso*, como visto, e *destacado*, como se depreende do art. 11, inciso I, da LGPD (BRASIL, 2018). É fundamental, portanto, que a pessoa tenha plena ciência de que está consentindo separadamente para o tratamento de dados sensíveis, de forma que a qualificação do consentimento como destacado contribui para uma maior carga participativa da pessoa no contexto da manifestação da vontade.

No que toca à exigência da *finalidade específica*, nos termos do inciso I do art. 11 da LGPD, é importante, novamente, remeter ao princípio da finalidade. A exigência de que o tratamento de dados se dê para propósitos específicos já é estabelecida por este princípio e aplicável ao tratamento de qualquer dado pessoal, seja ele sensível ou não. Entretanto, é possível compreender essa previsão em especial para os dados sensíveis como uma ênfase para uma especificidade no seu tratamento, sobretudo diante da sua potencialidade lesiva.

É necessário remetermos a um aspecto do regime geral do consentimento na LGPD, mas que ganha particular atenção em se tratando de dados sensíveis. Como ato jurídico unilateral, o consentimento para o tratamento de dados pessoais é revogável de forma incondicional, o que se coaduna com a caracterização dos dados pessoais como representação da personalidade, que são, em última análise, indisponíveis (DONEDA, 2006). Nessa direção, a LGPD estabelece a revogabilidade facilitada a qualquer tempo do consentimento fornecido pelo titular, de acordo com o art. 8, §5º.

Por fim, como importante referência para o Brasil, o European Data Protection Board (2020) enfatizou, no âmbito do GDPR, que a obtenção do consentimento não nega e nem diminui as obrigações dos controladores de dados no sentido de observar a principiologia de proteção de dados pessoais disposta na regulação europeia, em especial no que diz respeito aos princípios da lealdade, da necessidade, da proporcionalidade e da qualidade dos dados.

5 CONCLUSÃO

A contemporânea repercussão do ubíquo processamento de dados pessoais em múltiplos direitos fundamentais não tem precedentes. A existência pregressa do fenômeno informacional se contrapõe ao desenvolvimento de sistemas automatizados com progressivas funcionalidades, e os dados pessoais, nesse campo, representam um eixo estratégico de interesses de organizações, do mercado e do Estado.

Entre os dados pessoais é situada a categoria dos dados sensíveis, qualificados por extrapolar o tema da proteção de dados, alçando-o diretamente a termos de igualdade material. A ontologia dos dados sensíveis é associada à sua potencialidade de discriminar e estigmatizar, razão pela qual, historicamente, a esses dados costuma ser reservado um maior *standard* de proteção se comparado ao dos dados pessoais não sensíveis.

Como um dos instrumentos para esse propósito está uma maior qualificação do consentimento da pessoa à qual os dados se referem para o tratamento de dados sensíveis, o que foi identificado no marco regulatório brasileiro geral de proteção de dados pessoais. Apesar de o instituto do consentimento ser permeado por desafios como a assimetria informacional e de poder entre a pessoa e o responsável pelo tratamento, inegável é a sua importância como instrumento para a autodeterminação informativa, desde que situado em um paradigma de tutela da pessoa, o que o presente trabalho buscou endereçar.

De forma progressiva, a proteção de dados pessoais se apresenta como chave para o pleno exercício de diversos direitos fundamentais no paradigma de hiperconectividade. Em especial, a tutela dos dados sensíveis, nesse cenário, assume importância ainda maior para que a pessoa, em suas múltiplas expressões, seja efetivamente protegida na era da informação.

REFERÊNCIAS

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

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 abr. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658. Acesso em: 1 set. 2017.

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

ESTADÃO. Três em cada dez jovens e adultos de 15 a 64 anos no País - 29% do total, o equivalente a cerca de 38 milhões de pessoas - são considerados analfabetos funcionais. **Estadão,** 6 ago. 2018. Disponível em: https://epocanegocios.globo.com/Brasil/noticia/2018/08/epoca-negocios-tres-em-cada-10-sao-analfabetos-funcionais-no-pais-aponta-estudo.html. Acesso em: 09 ago. 2019

EUROPEAN DATA PROTECTION BOARD (União Europeia). **Guidelines 05/2020 on consent under Regulation 2016/679.** 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en. Acesso em: 14 maio 2020.

FRAZÃO, Ana. Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais. **Jota,** 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em: 1 jul. 2019.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais,** São Paulo, v. 998, cad. esp. p. 99-128, dez. 2018.

MADRIGAL, Alexis C. Reading the privacy policies you encounter in a year would take 76 work days. **The Atlantic,** 2012. Disponível em: https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/. Acesso em: 2 jun. 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva Educação, 2014. (Série IDP: linha de pesquisa acadêmica).

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais,** v. 19, p. 159-180, 2018.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Migalhas,** 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 20 jul. 2020.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. **Revista de Direito, Governança e Novas Tecnologias,** Goiânia, v. 5, n. 1, p. 63-85, jan./jun. 2019. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 9 out. 2019.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano**. Il mondo nella rete**: quali i diritti, quali i vincoli. Roma: Laterza & Figli – Gruppo Editoriale L'Espresso, 2019.

ROUVROY, Antoinette. "'Of Data and Men'. Fundamental Rights and Freedoms in a World of Big Data." **Council of Europe, Directorate General of Human Rights and Rule of Law,** Strasbourg, v. T- PD-BUR(2015)09REV, p. 1-37, 11 jan. 2016.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Civilistica.com,** Rio de Janeiro, ano 8, n. 1, 2019. Disponível em: http://civilistica.com/o-consentimento-informado-e-a-protecao/. Acesso em: 9 abr. 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 287-322.

TSAMADOS, Andreas; AGGARWAL, Nikita; COWLS, Josh; MORLEY, Jessica; ROBERTS, Huw; TADDEO, Mariarosaria; FLORIDI, Luciano. The ethics of algorithms: key problems and solutions. **AI & Society**, 20 fev. 2021. DOI: http://dx.doi.org/10.1007/s00146-021-01154-8.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**: general regulation data protection (regulamento geral sobre a proteção de dados). Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 8 ago. 2018.

WARREN, Samuel; BRANDEIS, Louis.The Right to Privacy. **Harvard Law Review,** Boston, v. 4, n. 5, p. 193-220, dez., 1890.

Recebido: 18/5/2021.
Aprovado: 25/10/2023.

Maria Regina Detoni Cavalcanti Rigolon Korkmaz
Doutora em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ).
Mestre em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF).
Professora de Direito Civil e Novas Tecnologias da Universidade Federal de Juiz de Fora (UFJF).
Professora convidada da pós-Graduação *lato sensu* em Direito Digital do ITS Rio, em parceria com a UERJ e com o CEPED e da pós-Graduação em Direito Privado, Tecnologia e Inovação da EBRADI.
Advogada.
E-mail: mariaregina.korkmaz@ufjf.br