ISSN 2175-6058
http://dx.doi.org/10.18759/rdgf.v19i3.1603

DADOS PESSOAIS SENSÍVEIS E A TUTELA DE DIREITOS FUNDAMENTAIS: UMA ANÁLISE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/18)

SENSITIVE PERSONAL DATA AND THE PROTECTION OF FUNDAMENTAL RIGHTS: AN ANALYSIS IN LIGHT OF THE GENERAL DATA PROTECTION LAW (LAW 13.709/18)

Caitlin Sampaio Mulholland

RESUMO

O presente artigo pretende aproximar o conceito de dados pessoais sensíveis de uma teoria de direitos fundamentais, por meio de uma interpretação dos princípios e valores constitucionais que justificam a proteção do direito à privacidade. Pretende-se investigar a Lei Geral de Proteção de Dados - Lei 13.709/2018 - e as políticas por ela assumidas no que diz respeito ao tratamento de dados pessoais sensíveis tanto pelo Estado, quanto pelo Mercado. Sustenta-se a necessidade de um tratamento restrito dos dados pessoais sensíveis como forma de proteção contra o seu uso discriminatório, visando a promoção plena do exercício democrático.

Palavras-chave: Dados pessoais sensíveis. Direitos Fundamentais. Lei Geral de Proteção de Dados.

ABSTRACT

The present paper intends to approximate the concept of sensitive personal data of a theory of fundamental rights, through an interpretation of the principles and constitutional values that justify the protection of the right to privacy. The aim is to investigate the General Data Protection Law - Law 13.709/2018 - and the policies it has adopted with regard to the processing of sensitive personal data by both the State and the Market. I support the need for a restricted treatment of sensitive personal data as a form of protection against its discriminatory use for the full promotion of democratic exercise.

Keywords: Sensitive personal data. Fundamental Rights. General Data Protection Law.

INTRODUÇÃO: TRÊS CASOS EXEMPLARES

Em 2016, uma prestadora de serviços de coleta e doação de sangue na Austrália, a *Red Cross Blood Service*, sofreu um duro golpe em seu sistema de segurança de dados, quando informações referentes a 550.000 doadores de sangue vieram a público devido à transferência de um arquivo contendo informações desses doadores a um ambiente computacional não seguro, acessível por pessoas sem a devida autorização para manejar aqueles dados. Os dados se referiam a coletas de sangue realizadas entre os anos de 2010 e 2016.

O fato, por si só, já seria grave, considerando a natureza pessoal dos dados que foram disponibilizados publicamente em *site* na Internet, quais sejam: nome, gênero, endereço e data de nascimento. Contudo, para trazer tons mais dramáticos à situação, dentre as informações contidas na base de dados, uma era especialmente sigilosa, qual seja, a que especificava que determinado doador seria "pessoa com comportamento sexual de risco".[1] Essa categorização era determinada por meio de questionário do tipo "verdadeiro-falso" disponibilizado ao doador no momento da coleta de sangue, em que se perguntava se o mesmo havia participado de atividades sexuais de risco nos últimos 12 meses. Tanto as perguntas realizadas no questionário, como as respostas, compunham a base de dados e estabeleciam a conexão com o doador, individualizado por seu

nome e pelas demais informações pessoais. A *Red Cross* pediu desculpas formais aos doadores e disponibilizou todo um aparato de atendimento às pessoas que tiveram seus dados violados.

Em 2017, num segundo caso, no Canadá, uma empresa de produtos sexuais, a *Standard Innovation*, disponibilizou no mercado de consumo um vibrador denominado *We-Vibe 4 Plus* que possuía uma característica incomum: o aparelho conectava-se por rede (*bluetooth ou wi-fi)* ao celular, por meio de um aplicativo, que permitia o seu acesso remoto. O usuário - ou seu/sua companheiro(a) definia por meio do aplicativo preferências relacionadas ao ritmo e tipo da vibração. Contudo, descobriu-se que o aparelho enviava para os servidores da empresa os dados relacionados ao seu uso, inclusive no exato momento em que estava sendo utilizado. Os dados coletados continham informações sobre a temperatura corporal, o ritmo de vibrações, a intensidade das mesmas, tempo de uso, início e término do uso, etc. Evidentemente, a justificativa da empresa para a coleta de tais dados era a de que com eles poderia melhorar o produto. No entanto, nem os termos de uso do produto ou do aplicativo indicavam a coleta dos dados, nem existia um sistema de segurança das informações adequado que permitisse a sua guarda eficiente. Os consumidores do vibrador ingressaram com uma ação coletiva contra a empresa, que foi levada a realizar um acordo no valor de US$ 2,9 milhões e obrigou-se a não mais coletar dados sigilosos de seus usuários.[2]

No terceiro caso, na China, em 2014, foi anunciado o que está sendo chamado de sistema de crédito social ("social scoring"), que será implementado até 2020 no país. Por meio de tal sistema mantido pelo Estado chinês pretende-se verificar a "fidelidade" dos 1,3 bilhão de cidadãos chineses aos princípios e valores do Estado.[3] Por esse sistema será possível categorizar e taxar os comportamentos dos cidadãos como positivos ou negativos (na visão do Estado), indicando uma classificação única e pública daquela pessoa, que servirá para determinar se um cidadão terá direito ao acesso a determinadas políticas públicas, que incluem desde a prestação de serviços médico-hospitalares até a indicação de escolas em que os filhos devem ser matriculados. De acordo com o documento público de planejamento do sistema de crédito social, tal proposta "forjará um ambiente de opinião pública em que

manter a confiança é gloriosa. Fortalecerá a sinceridade nos assuntos do governo, a sinceridade comercial, a sinceridade social e a construção da credibilidade judicial". Por enquanto, a participação do cidadão chinês em tal sistema é voluntária, mas ,em 2020, ela será obrigatória para todos, inclusive para as pessoas jurídicas que tenham sede na China.

Apesar de cada um dos três casos apresentados se referirem a temas diversos sexualidade, hábitos sócio-culturais e sistemas de controle social o ponto comum é o tratamento e violação de dados sensíveis, isto é, a utilização ampla e não consentida por terceiros de dados pessoais que tenham características fortemente marcadas pela capacidade de seu uso discriminatório tanto pelo Estado, quanto pelo mercado. Tratam-se, portanto, de situações em que podem estar presentes potenciais violações de direitos fundamentais, dadas as características e a natureza desses dados sensíveis. Para a compreensão do conceito de dados sensíveis e a motivação de sua tutela, é importante investigar a Lei Geral de Proteção de Dados Pessoais brasileira, seus conceitos, princípios e seu âmbito de aplicação.

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS BRASILEIRA: ÂMBITO DE APLICAÇÃO E PRINCÍPIOS.

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/18) dispõe sobre tratamento de dados de pessoas naturais, tanto por meio físico, quanto por meio digital, reconhecendo a finalidade da tutela desses dados/informações para a proteção de direitos, como os da liberdade de expressão e de comunicação, privacidade, honra, imagem, autodeterminação informativa e livre desenvolvimento da personalidade (art. 2º). Ademais, a lei reconhece a efetivação e promoção de Direitos Humanos Fundamentais como justificativa para a tutela dos dados pessoais (art. 2º, VII).

A lei protege situações que concernem exclusivamente a operações de tratamento de dados, isto é, aquelas "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" (art. 5º, X). Percebe-se pelo rol descritivo do que se entende por tratamento de dados, que inúmeras atividades que envolvem dados pessoais sofrerão a limitação e escrutínio da lei.

Há, contudo, algumas exceções relevantes à aplicação da LGPD, enumeradas taxativamente no artigo 4º, quais sejam: (i) tratamento por pessoas naturais para fins particulares e não econômicos; (ii) tratamento para fins exclusivamente jornalísticos, artísticos ou acadêmicos; (iii) tratamento para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais[4]; e (iv) tratamento de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.[5]

Em relação à hipótese prevista no item (iii), a LGPD faz remissão à necessidade de aprovação de legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, devendo ser respeitados o princípio do devido processo legal e os demais princípios previstos na LGPD. Espera-se que a legislação vindoura seja ainda mais rigorosa na proteção dos dados sensíveis das pessoas que a ela estarão sujeitas, considerando que o tratamento desses dados está relacionado em grande medida aos objetivos de proteção do próprio Estado e dos interesses públicos. Deve-se visar a um tratamento limitado desses dados, para evitar o seu eventual uso para propósitos que não atendam aos fundamentos republicanos do Estado Democrático de Direito.[6]

Em relação aos princípios aplicáveis ao tratamento de dados pessoais, a sua previsão é reconhecida no artigo 6º, da LGPD, com o objetivo de restringir a atividade de tratamento de dados pessoais, exigindo-se que haja o seu cumprimento para que seja reconhecida a licitude da atividade, legitimanda. São os seguintes princípios previstos na lei: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação,

responsabilização e prestação de contas.[7] Dos princípios previstos, dois são de especial relevância quando do tratamento de dados sensíveis, quais sejam, o princípio da finalidade e o princípio da não discriminação.

Pelo princípio da finalidade, os dados devem ser tratados para determinados propósitos, que devem ser informados ao titular de dados previamente, de maneira explícita e sem que seja possível a sua utilização posterior para outra aplicação. Para Doneda, "este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)" (DONEDA, 2005, 216). Ainda com base no princípio da finalidade, Maria Celina Bodin de Moraes, em apresentação à obra de Stefano Rodotà, entende que o tratamento de dados e especialmente a sua coleta "não pode ser tomada como uma "rede jogada ao mar para pescar qualquer peixe". Ao contrário, as razões de coleta, principalmente quando se tratarem de "dados sensíveis", devem ser objetivas e limitadas" (MORAES, 2008, p. 9). A medida dessa objetividade e limitação será determinada justamente pela finalidade legítima do tratamento, que fica condicionada "à comunicação preventiva ao interessado sobre como serão usadas as informações coletadas; e para algumas categorias de dados especialmente sensíveis estabelece que a única finalidade admissível é o interesse da pessoa considerada" (RODOTÀ, 2008, p. 87).

Em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. O legislador, ao relacionar o uso discriminatório às qualidades de ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo. Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. Assim, por exemplo, seria legítimo a um operador de dados que esteja realizando a precificação de um serviço de seguros de automóveis, tratar de maneira diferenciada os dados de mulheres entre 35 e 45 anos e mães, com a finalidade de oferecimento de um valor que reflita os riscos de danos usualmente ocasionados ou sofridos

por esse grupo determinado de pessoas. Ou seja, há a possibilidade de tratamentos discriminatórios de dados, desde que não se caracterizem pela ilicitude ou abusividade, o que será determinado segundo critérios definidos tanto pelas regras expressas de direito civil[8] e penal, quanto por princípios como o da boa-fé objetiva[9]. O que se questiona é se esse tratamento segregado - desde que lícito e não abusivo - pode ser realizado também quando considerados os dados pessoais sensíveis, na medida em que eles possuem características personalíssimas, que devem ser tuteladas prioritariamente. Considerando que

> [...] coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como "a proteção de escolhas de vida contra qualquer forma de controle público e estigma social" (L. M. Friedman), como a "reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto" (J. Rosen)" (RODOTÀ, 2008, p.12).

Necessário se faz, portanto, conceituar dados sensíveis e verificar as restrições impostas na lei para seu tratamento.

TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS: CONCEITO, RESTRIÇÕES E TUTELA

Para fins de regulação das atividades de tratamento de dados, a Lei Geral de Proteção de Dados Brasileira (LGPD) categoriza e tutela de forma diferenciada os dados pessoais e os dados pessoais sensíveis. Para os fins da LGPD, dado pessoal é composto por informações relacionadas a pessoa natural identificada ou identificável (artigo 5º, I) e dado pessoal sensível se refere à "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" (art. 5º, II). Apesar dessa lei específica ter trazido um conceito ampliado de dados pessoais sensíveis, o seu tratamento jurídico já é conhecido da legislação brasileira desde a promulgação da Lei de Cadastro Positivo - Lei 12.414/11 - que em seu artigo 3º, § 3º, II, proíbe anotações em bancos

de dados usados para análise de crédito de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas". Significa dizer que para fins de análise de concessão de crédito - princípio da finalidade - estão vedadas inclusões nas bases de dados de quaisquer informações de natureza personalíssima e que não se relacione à finalidade almejada com a análise de crédito, com o objetivo de evitar o tratamento discriminatório - princípio da não discriminação.[10]

Este princípio não discriminação é dos mais relevantes, no que diz respeito ao tratamento de dados sensíveis. É esse o ponto fundamental quando diante do uso de dados sensíveis potencialmente lesivo, em decorrência de sua capacidade discriminatória, seja por entes privados - *i.e*. fornecedoras de produtos e serviços - seja por entes públicos. Alguns casos emblemáticos expõem a enorme dificuldade que se enfrenta relativamente ao tratamento indevido desses dados sensíveis. Cohen relata alguns o tratamento inadequado de dados sensíveis que geram discriminação e segregação abusiva no âmbito das relações de consumo. Segundo a autora,

> "consumer data can be used for many purposes to which consumers might not so blithely agree: employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical "have--nots"; employment or housing decisions based on perceived personality risks; employment or housing decisions based on sexual or religious preferences; and so on" (COHEN, 2000, p. 27).

Em sentido semelhante, Rodotà sustenta que a formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação [...] seja porque dados pessoais, aparentemente não "sensíveis", podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas" (RODOTÀ; 2008, p. 56). Para o autor italiano, "(...) para garantir plenitude à esfera pública, determinam-se rigorosas condições de circulação destas informações, que recebem um fortíssimo estatuto "privado",

que se manifesta sobretudo pela proibição de sua coleta por parte de determinados sujeitos (por exemplo, empregadores) e pela exclusão de legitimidade de certas formas de coleta e circulação" (RODOTÀ: 2008, p. 64). A Lei Geral de Proteção de Dados brasileira segue esta tendência, ao estabelecer limitações específicas para o tratamento de dados sensíveis.

Importa reconhecer que a referida lei recebeu uma forte influência do direito comunitário europeu, desde a Diretiva de Proteção de Dados de 1995 até o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em vigor a partir de maio de 2018. No que diz respeito ao tratamento de dados sensíveis, a LGPD conceituou de forma semelhante, senão idêntica, ao GDPR, o conceito de dados pessoais sensíveis, sendo certo que a lei brasileira é bastante inspirada no regulamento europeu. Em seu artigo 9(1) e (2), o GDPR estabelece um regime bastante estrito, proibindo, via de regra, o processamento desse tipo de dado pessoal. No entanto, excetua essa proibição em dez circunstâncias, que passam desde a proteção de interesses vitais do indivíduo até razões de substancial interesse público, sem, contudo, exemplificar ou especificar quais seriam essas hipóteses concretamente consideradas.

Como forma de proteger mais intensamente os titulares dos dados sensíveis, o GDPR qualificou de maneira mais restrita o consentimento do titular dos dados sensíveis, passando a exigir que, além de expresso, a manifestação consentida deve ser livre, explícita, inequívoca, informada e específica. Nos "considerandos" do GDPR, a explicação (51) estatui que "merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais". Ademais, no comentário (71) do GDPR, fica consignado que "(…) o responsável pelo tratamento deverá (…) proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos".

De início, a LGPD adota uma forte fundamentação no consentimento do titular de dados para admitir o tratamento dos dados pessoais. Significa dizer que será permitido o tratamento de dados pessoais em havendo manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII). Em complementação, a LGPD estabelece restrições importantes quando diante do tratamento de dados sensíveis, e em relação ao consentimento, estabelece a necessidade de que ele seja realizado de forma específica e destacada, para finalidades singulares também (artigo 11, I, LGPD). Assim, e de acordo com Rodotà, reconhece-se que o consentimento do titular de dados sensíveis deve ser qualificado, na medida em que estamos diante de um "contratante vulnerável", caracterizado justamente pela ausência de liberdade substancial no momento da determinação da vontade (RODOTÀ, 2008, p. 90).

Contudo, a LGPD permite que haja tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados, quando for indispensável para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (artigo 11, II, b, LGPD), além de outras hipóteses que se referem, em grande medida, a interesses públicos. Neste último caso, o consentimento do titular dos dados sensíveis, seja genérico, seja específico, ficaria dispensado em decorrência de uma ponderação de interesses realizada pela lei, aprioristicamente, que considera mais relevantes e preponderantes os interesses de natureza pública frente aos interesses do titular, ainda que estes tenham qualidade de Direito Fundamental. No entanto, críticas devem ser feitas a este posicionamento legislativo, especialmente se considerarmos que a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de Direitos Fundamentais, tais como os da igualdade, liberdade e privacidade.

OS DIREITOS FUNDAMENTAIS E SUA APLICAÇÃO AO DIREITO PRIVADO: UMA ANÁLISE BASEADA NO PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA

Os Direitos Fundamentais, previstos em nossa Constituição Federal de 1988, formam, conforme salienta Ingo Sarlet, "um conjunto complexo e extremamente heterogêneo de posições jurídicas" (SARLET, 2008, p.118), representados desde os direitos subjetivos de resistência ou oposição perante o Estado, até os direitos ao exercício democrático plural. Conforme ensinamentos de Konrad Hesse, os Direitos Fundamentais cumprem a função de "criar e manter os pressupostos elementares de uma vida na liberdade e na dignidade humana" (HESSE *apud* BONAVIDES, 2001, p.514). Para Bonavides, "a vinculação essencial dos direitos fundamentais à liberdade e à dignidade humana, enquanto valores históricos e filosóficos, nos conduzirá sem óbices ao significado de universalidade inerente a esses direitos como ideal da pessoa humana" (BONAVIDES, 2001, p. 516).

O reconhecimento da dignidade humana, alçada constitucionalmente a fundamento do Estado Democrático de Direito, é hoje a base valorativa de sustentação de toda e qualquer situação jurídica de Direito Privado. Sua inclusão no texto constitucional representou a escolha sócio-cultural-jurídica por uma sociedade solidária e justa, proporcionadora do livre desenvolvimento pessoal de seus cidadãos (MULHOLLAND, 2014, p. 14)

Este princípio possui duas acepções: uma no sentido de garantir a todas as pessoas um tratamento humano, não degradante, e, portanto, protetivo da integridade psicofísica de cada um; e outra, no sentido de realizar projetos e propostas que possibilitem a cada pessoa a concretização de sua humanidade, por meio de ações visíveis.

Tendo em vista esta caracterização da pessoa como um fim em si mesmo, toda e qualquer manifestação legislativa deve ter como finalidade a promoção do homem e de seus valores. E é nesta finalidade promocional que se encontra a maior dificuldade por parte do jurista. Se for possível dizer que a dignidade da pessoa humana, por se erigir como fundamento do Estado Democrático de Direito, deve alcançar todas as esferas do ordenamento jurídico – incluído aí os institutos de Direito

Privado –, é também possível concluir que a limitação interpretativa do conteúdo deste valor constitucional será difícil de se alcançar. Nesta dificuldade se encontram as barreiras para a aplicação consciente do princípio da dignidade humana, pois "corre-se o risco da generalização, indicando-a como *ratio* jurídica de todo e qualquer direito fundamental" (MORAES, 2003, p.54). Segundo Maria Celina Bodin de Moraes, "levada ao extremo, essa postura hermenêutica acaba por atribuir ao princípio um grau de abstração tão intenso que torna impossível sua aplicação" (MORAES, 2003, p. 84).

O Direito civil é chamado a dar concretude a este princípio por meio de uma atuação protetiva. É por meio da específica caracterização da pessoa e da consideração de suas qualidades que se dará a verdadeira – no sentido de justa e equitativa – tutela da pessoa em suas relações privadas. Diferentemente do conceito de indivíduo, igual ao outro em todos os seus aspectos e, portanto, devendo ser tratado de maneira igualitária, o conceito de pessoa permite ao ordenamento, por meio de normatização ou de trabalho hermenêutico desempenhado pela doutrina e magistratura, a possibilidade de estabelecer tratamentos desiguais de acordo com a qualidade que cada pessoa desempenha numa relação privada (MULHOLLAND, 2009, p. 67-68).

O princípio da dignidade da pessoa humana será identificado em cada uma das situações reais em que se possa verificar a concretização dos princípios da liberdade, da igualdade, da integridade ou da solidariedade social. Perfaz-se, assim, o princípio em uma cláusula geral de tutela da pessoa, servindo como princípio "prevalente no momento da concretização normativa e [n]a ponderação de princípios" (RUZYK, 2002, p.131). Significa isto dizer que para toda e qualquer situação em que esteja em jogo ou discussão a situação jurídica existencial, esta deverá prevalecer sobre aquelas patrimoniais se com elas incompatíveis (MULHOLLAND, 2009, p. 69). A análise do princípio da dignidade da pessoa humana se realiza, portanto, e com razão, considerando-se sempre a plena tutela da pessoa, seja considerando aspectos relacionados à sua liberdade, seja à sua identidade e privacidade, como no caso dos dados pessoais.

Uma primeira análise da estrutura constitucional dos Direitos Fundamentais leva ao reconhecimento de que a proteção de dados pessoais ainda que não prevista constitucionalmente pode ser feito tanto da proteção à intimidade (art. 5º, X), quanto do direito à informação (art. 5º, XIV), ou do direito ao sigilo de comunicações e dados (art. 5º, XII), assim como da garantia individual ao conhecimento e correção de informações sobre si pelo *habeas data* (art. 5º, LXXII). Para Rodotà,

> estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito fundamental autônomo (o autor refere-se à Carta de Direitos Fundamentais da União Europeia)[11], mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio (RODOTÀ, 2008, p. 14).

Percebe-se assim que, apesar de não haver a previsão constitucional no Brasil do direito aos dados pessoais como uma categoria de Direitos Fundamentais, pode-se compreender, por meio de uma leitura funcionalizada da Constituição Federal e de seus princípios e valores, que a tutela da privacidade é o *locus* constitucional da proteção dos dados pessoais, conforme esclareceremos adiante. Parte-se da ideia de que os dados são elemento constituinte da identidade da pessoa e que devem ser protegidos na medida em que compõem parte fundamental de sua personalidade, que deve ter seu desenvolvimento privilegiado, por meio do reconhecimento de sua dignidade.

DO DIREITO À PRIVACIDADE: PROTEÇÃO DA INTIMIDADE DESDE O PRINCÍPIO "THE RIGHT TO BE LET ALONE" AO DIREITO DE CONTROLAR SEUS PRÓPRIOS DADOS

Em nosso ordenamento, o artigo 5º, X, da Constituição Federal[12], e o artigo 21, do Código Civil[13], fundamentam a proteção da esfera privada de uma pessoa, referindo-se tanto à vida privada, quanto à intimidade da pessoa humana. O direito à privacidade, e mais especificamente, o direito

à intimidade, alude à proteção da esfera privada ou íntima de uma pessoa, sendo esta abrigada contra ingerências externas, alheias e não requisitadas, e tutelada na medida em que não se permite, sem autorização do titular da informação ou dado, a sua divulgação no meio social.

Este conceito habitual de privacidade está, contudo, superado. Se, tradicionalmente, o direito à privacidade (*right to privacy*) está associado ao direito de ser deixado só, contemporaneamente pode-se afirmar que a privacidade evoluiu para incluir em seu conteúdo situações de tutela de dados sensíveis**,** de seu controle pelo titular e, especialmente, de "respeito à liberdade das escolhas pessoais de caráter existencial" (LEWICKI, 2003, p. 9). Para Stefano Rodotà, "a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações" sendo a esfera privada "aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo" (RODOTÀ, 2008, p. 92). Para Solove, "*privacy is a fundamental right, essential for freedom, democracy, psychological well-being, individuality, and creativity*" (SOLOVE, 2008, p. 5).

Foi com base naquele primeiro conteúdo que em 1890, os *Justices* da *Supreme Court* americana, Warren e Brandeis, determinaram a necessidade de tutela dessa esfera existencial. À época, a interpretação que se dava ao direito à privacidade era restrita e se aplicava a casos em que existia a atuação de terceiros contra aquela esfera. Isto é, a interpretação que se dava a este direito restringia-se a tutelar a esfera privada de uma pessoa, impedindo que outros pudessem nela ingressar sem sua autorização. Associada à ideia de casa, moradia, este princípio foi primeiramente utilizado para proteger a vida privada das pessoas, dentro de seu próprio lar (MULHOLLAND, 2012, p. 2).

A ampliação do conceito de *privacy* se deu, em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, consequentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a

facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada (MULHOLLAND, 2012, p.3).

Seriam, assim, três as concepções sobre o direito à privacidade acima apresentadas, quais sejam, (i) o direito de ser deixado só, (ii) o direito de ter controle sobre a circulação dos dados pessoais, e (iii) o direito à liberdade das escolhas pessoais de caráter existencial (MULHOLLAND, 2012, p.3). Assim, "a privacidade deve ser considerada também como o "direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular", reconhecendo-se às pessoas "auto-determinação informativa" (RODOTÀ, 2008, p.15) e a realização plena de sua liberdade existencial (RODOTÀ, 2008, p. 92).

A PROTEÇÃO CONSTITUCIONAL DOS DADOS SENSÍVEIS COMO EXERCÍCIO DEMOCRÁTICO DE IGUALDADE E NÃO DISCRIMINAÇÃO

A proteção de dados pessoais enquanto decorrência da cláusula geral de tutela da pessoa humana e do direito à privacidade é um requisito essencial da democracia. A capacidade de tratamento de dados pessoais das mais diversas ordens vem aumentando exponencialmente, principalmente devido ao advento de tecnologias avançadas de inteligência artificial, com o uso de algoritmos sofisticados e com a possibilidade de aprendizado por máquinas (*machine learning*). Significa dizer que o tratamento de "*big data*" literalmente, grandes bases de dados por meio de técnicas computacionais cada vez mais desenvolvidas pode levar a análises probabilísticas e resultados que, ao mesmo tempo que atingem os interesses de uma parcela específica da população, retiram a capacidade de autonomia do indivíduo e o seu direito de acesso ao consumo de bens e serviços e a determinadas políticas públicas, por exemplo.

Por isto que a regulação da coleta, uso, tratamento e compartilhamento de dados pela Lei Geral de Proteção de Dados torna-se de suma importância, devendo tais atividades serem realizadas de tal forma a respeitar os princípios previstos na mesma, enfatizando-se, no caso de dados sensíveis, o uso dos mesmos de maneira que atente ao princípio da igualdade e não gere uma discriminação. O princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequitativos. Esse princípio deve servir como base de sustentação da tutela dos dados sensíveis, especialmente quando estamos diante do exercício democrático e do acesso a direitos sociais, tais como o direito ao trabalho, à saúde e à moradia.

De acordo com Celina Bodin e Chiara de Teffé (2016, p.21), "uma vez munidas de tais informações (dados pessoais), entidades privadas e governamentais tornam-se capazes de "rotular" e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode favorecer inclusive graves discriminações, principalmente se analisados dados sensíveis".

> Em continuidade, as autoras sustentam que "[...] um acervo suficientemente amplo de informações permite a elaboração de perfis de consumo, o que se, de um lado, pode ser utilizado para incrementar e personalizar a venda de produtos e serviços, de outro, pode aumentar o controle sobre a pessoa, desconsiderando sua autonomia e dificultando a participação do indivíduo no processo decisório relativo ao tratamento de seus dados pessoais, de seu patrimônio informativo.

A título de ilustração, dois casos relatam os malefícios do perfilamento (*profiling*), com uso de dados pessoais que geraram tratamento discriminatório. Os casos ocorreram nos EUA e se referiram à contratação de serviços médicos e de seguridade. No primeiro caso, algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez. Em outro caso, relacionado

a dados de saúde, "quando uma pessoa tem um derrame, alguns bancos, ao descobrir tal fato, começam a cobrar o pagamento dos empréstimos realizados".[14] Em outro exemplo trazido por Rodotà sobre o uso de dados pessoais sensíveis,

> Não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado (RODOTÀ, 2008, p. 70).

A tutela jurídica de dados pessoais como um corolário do direito à privacidade (ou do direito à identidade) nos leva a considerar que a autodeterminação informativa, ou o poder de controle sobre os próprios dados, deve ser a tônica quando buscamos a proteção específica dos dados sensíveis, especialmente se tais dados podem gerar tratamentos desiguais. O reconhecimento do direito fundamental à igualdade no artigo 5º, *caput*, da Constituição Federal tutela também o direito ao tratamento sem distinções de qualquer natureza. Ao mesmo tempo, dentre os objetivos fundamentais da República Federativa do Brasil, constantes do artigo 3º, da Constituição Federal, está o de "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação". Soma-se ao reconhecimento constitucional da proteção da igualdade e da não discriminação, a previsão na LGPD da impossibilidade do tratamento para fins discriminatórios ilícitos ou abusivos, conforme já esclarecido em outra oportunidade.

CONSIDERAÇÕES FINAIS

Nos três casos exemplares relatados na introdução deste artigo, pode-se reconhecer o tratamento de dados sensíveis nas atividades realizadas tanto por pessoas jurídicas privadas, quanto pelo Estado. No primeiro caso *Red Cross Blood Services* informações relacionadas a hábitos sexuais de doadores de sangue foram coletadas com a finalidade de realização de análise de riscos relacionados à doação e recebimento

de sangue, sendo posteriormente divulgadas, devido a uma falha de segurança no tratamento dos dados. No segundo caso *Standard Inovation* dados sensíveis relacionados ao uso de vibradores sexuais foram utilizados pela empresa sem o consentimento de seus titulares, com a finalidade de oferecer produtos mais adequados no mercado, o que levou a uma ação coletiva bem sucedida. No terceiro caso sistema de scoring social na China dados das mais diversas naturezas incluídos dados sensíveis são utilizados para fins de pontuação social dos cidadãos, que permitirá a sua qualificação para acessar determinados serviços públicos desenvolvidos por meio de políticas de Estado.

No primeiro caso, temos uma evidente violação no dever de segurança no tratamento de dados, caracterizando um ato ilícito. Nos dois últimos casos por mais diversos que sejam em fundamentos a falha no tratamento de dados sensíveis surge como decorrência da violação do princípio da finalidade. Para cada uma das aplicações envolvidas no tratamento de dados, há uma finalidade que deve servir como parâmetro ou limitação dessas atividades. Considerando que a finalidade deve ser legítima, lícita e não abusiva, podemos concluir que nestas duas hipóteses exemplares, a finalidade de propósitos foi usurpada, seja porque ilícita (no caso da *Standard Inovation*), seja porque abusiva (no caso chinês).

Ademais, no caso do S*coring social* chinês há ainda a violação do princípio da não discriminação, na medida em que os dados coletados, sejam de natureza sensível ou não, são utilizados para finalidades de tratamento diferenciado, excluindo cidadãos do acesso à efetivação de direitos de natureza fundamental, como a igualdade, liberdade, privacidade, saúde, educação, moradia, e impedindo o pleno exercício democrático que, de fato e concretamente, inexiste na China.

Para Rodotà, é fundamental que haja uma tutela rigorosa dos dados sensíveis, pois esses transformaram-se em conteúdo essencial para a concretização do princípio da igualdade e da não discriminação. Mais ainda, a tutela de dados pessoais sensíveis permite a efetivação, a depender de sua natureza, do direito à saúde (dados genéticos ou sanitários), do direito à liberdade de expressão e de comunicação (dados sobre opiniões pessoais), do direito à liberdade religiosa e de associação (dados sobre convicção religiosa). Assim, para o autor italiano, "(...) a

associação entre privacidade e liberdade torna-se cada vez mais forte" (RODOTÀ, 2008, p.153), reconhecendo, desta maneira, a natureza de direitos fundamentais aos dados pessoais sensíveis.

Considerando que se caminha cada vez mais e com maior intensidade para uma sociedade governada por dados, o ambiente social no qual se concretiza a ideia de privacidade informacional passa a ser qualificado pela proteção dos direitos da pessoa de manter o controle sobre seus dados, por meio de sua autodeterminação informativa (liberdade), visando a não discriminação (igualdade). Portanto, o problema da privacidade hoje é causado pelo conflito consequente da assimetria de poderes existente entre os titulares de dados e aqueles que realizam o tratamento dos dados. Esta assimetria gera um desequilíbrio social que, por sua vez, leva à violação dos princípios da igualdade e da liberdade. Proteger de maneira rigorosa os dados pessoais sensíveis se torna, assim, instrumento para a efetivação da igualdade e da liberdade.

NOTAS

1 Disponivel em https://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to--data-breach/7974036 Acesso em: 14 de novembro de 2018.

2 O caso está descrito disponivel em https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits. Acesso em 15 de novembro de 2018.

3 Veja o relato do sistema, disponivel em https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion. Acesso em 15 de novembro de 2018.

4 Rodotà revela que "as formas de limitação mais difundidas, que chegam a sacrificar a tutela da privacidade em prol de outros interesses, considerados temporariamente ou não como prevalecentes, são bem conhecidas e em muitos casos estão previstas na própria legislação sobre bancos de dados. Dizem respeito sobretudo a interesses do Estado (segurança interna ou internacional, polícia, justiça) ou a relevantes direitos individuais e coletivos (tradicionalmente, o direito à informação, sobretudo como liberdade de imprensa; e cada vez mais intensamente o direito à saúde, principalmente em sua dimensão coletiva)" (RODOTÀ: 2008, 70).

5 Art. 4º, Lei 13.709/18 - Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

6 É de se reconhecer que o uso de dados pessoais pelo Estado pode gerar a redução das garantias de proteção de direitos fundamentais. Basta relembrar o caso Edward Snowden e National Security Agency (NSA) e o uso indevido de dados coletados pela própria agência com o objetivo de construção de perfis de pessoas que poderiam estar ligadas a atividades de terrorismo, para

percebermos os usos potencialmente danosos a uma democracia. Sobre o caso Snowden, veja, por todos, Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014.

7 Art. 6º, Lei 13.709/18: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

8 Ver artigos 186 e 187, do Código Civil, que conceituam o ato ilícito.

9 Ver artigo 421, do Código Civil.

10 Em pesquisa realizada em 20/11/18, utilizando-se como parâmetro de busca termos da Lei 12.414/11, há no Superior Tribunal de Justiça 1 Súmula (550), 2 acórdãos de repetitivos e 10 acórdãos que tratam da temática relacionada ao sistema de "credit scoring". As decisões, de uma maneira geral, reconhecem o direito do consumidor de ter o acesso aos dados que foram utilizados pelas financeiras ou bancos para a negativa do direito ao crédito. Ver por todos, nesse sentido, o julgamento do Recurso Especial 1.304.736/RS, Rel. Ministro Luis Felipe Salomão, Segunda Seção, julgado em 24/02/2016.

11 Artigo 8 – Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

12 Artigo 5º, X, CF – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

13 Art. 21, CC - A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

14 Instituto de Tecnologia e Sociedade. Transparência e Governança nos algoritmos: um estudo de caso sobre o setor de birôs de crédito, disponível em: https://itsrio.org/pt/publicacoes/transparencia-e-governanca-nos-algoritmos-um-estudo-de-caso/. Acesso em: 15 de novembro de 2018.

REFERÊNCIAS

MORAES, Maria Celina Bodin de. **Danos** à **pessoa humana**. Rio de Janeiro: Renovar, 2003.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. **Redes sociais virtuais**: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. Revista Pensar, v. 22, n. 1 2017 .

MORAES, Maria Celina Bodin de. Apresentação. In: RODOTÁ, Stefano. **A vida na sociedade de vigilância**: privacidade hoje. Rio de Janeiro: Renovar,2008.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. São Paulo: Malheiros, 2001.

COHEN, Julie. Examined Lives: Informational Privacy and the Subject as Object. 52 Stan. L. Rev. 1373-1438 (2000).

DONEDA, Danilo. **Da privacidade à protecao de dados**. Rio de Janeiro: Editora Renovar, 2005.

LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro:Renovar, 2003.

MULHOLLAND, Caitlin. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2009.

MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. Comentário ao REsp 1.195.995. Civilistica.com - **Revista Eletrônica de Direito Civil**, v. 1, p. 1, 2012.

MULHOLLAND, Caitlin; PIRES, Thula. O reflexo das lutas por reconhecimento no direito civil constitucional. In: Roberto Senise Lisboa; Elcio Nacur Rezende; Ilton Garcia da Costa. (Org.). **Relações privadas e democracia**. Florianópolis: Conpedi, 2014, v. 1, p. 135-153.

RODOTÀ, Stefano. **Il problema della responsabilità civile**. Milano: Giuffrè, 1967.

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

RUZYK, Carlos Eduardo P. A responsabilidade civil por danos produzidos no curso da atividade econômica e a tutela da dignidade da pessoa humana: o critério do dano ineficiente. In: Ramos, C. L S. et al. (Org.). **Diálogos sobre o Direito Civil**: Construindo a racionalidade contemporânea. Rio de Janeiro:Renovar, 2002

SARLET, Ingo W (Org.). **Direitos Fundamentais e Direito Privado**: uma Perspectiva de Direito Comparado. Coimbra: Almedina, 2008.

SOLOVE, Daniel J. **Understanding Privacy**, Cambridge: Harvard University Press, 2008.

Recebido em: 23-11-2018
Aprovado em: 18-12-2018

Caitlin Sampaio Mulholland

Doutorado em direito civil, Universidade do Estado do Rio de Janeiro, 2006. É professora assistente de direito civil do Departamento de Direito da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), coordenadora do curso de graduação em Direito – PUC - RIO. E-mail: http://www.jur.puc-rio.br

R. Marquês de São Vicente, 225, Gávea, Rio de Janeiro - RJ – CEP 22451-045