Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)

Caitlin Mulholland[1]

Sumário. Introdução. 1. O que são dados sensíveis, para além da expressa previsão da Lei Geral de Proteção de Dados? 2. Dados sensíveis e direitos fundamentais: uma identificação necessária. 3. Âmbito de aplicação do artigo 11, da LGPD: análise do parágrafo primeiro, do artigo 11, da LGPD, e o elemento danoso. 4. A responsabilidade civil dos agentes de tratamento de dados pessoais sensíveis é subjetiva ou objetiva? 5.Tratamento irregular e artigo 44, LGPD e seu confronto com o artigo 42, LGPD. 6. Conclusão. 7. Referências bibliográficas.

1. O que são dados sensíveis, para além da expressa previsão da Lei Geral de Proteção de Dados?

Para fins de regulação das atividades de tratamento de dados, a Lei Geral de Proteção de Dados Brasileira (LGPD) - Lei 13.709/18 - categoriza e tutela de forma diferenciada os dados pessoais e os dados pessoais sensíveis. Dado pessoal é composto por informações relacionadas à 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).[2]

Apesar da LGPD ter trazido um conteúdo ampliado de dados pessoais sensíveis - referindo-se tanto a aspectos existenciais, como sociais - 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

---

[1] Professora Associada do Departamento de Direito da PUC-Rio. Doutora em Direito Civil pela UERJ.

[2] Em relação aos dados genéticos, no âmbito do direito penal destacam-se duas leis: a Lei 12.654/12 - que prevê a coleta de perfil genético como forma de identificação criminal - e a Lei 12.037/09 - que dispõe sobre a identificação criminal do civilmente identificado. Ambas as leis permitem o tratamento de dados genéticos, desde que dentro limites especificados em lei, tais como o respeito a prazos de manutenção dos dados na base e a proibição de revelação de traços somáticos ou comportamentais do titular dos dados.

convicções políticas, religiosas e filosóficas". Significa dizer que para fins de análise de concessão de crédito - fundamentado no 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 - fundamentado no princípio da não discriminação. Este princípio, por sua vez, é dos mais relevantes no que diz respeito ao tratamento de dados sensíveis, constituindo-se a justificativa basilar para a sua tutela rigorosa. A vedação ao tratamento discriminatório e abusivo é o ponto essencial para identificar os limites ao uso de dados sensíveis. Desta forma, quando diante da utilização de dados que seja potencialmente lesiva, em decorrência de sua capacidade discriminatória, seja por entes privados - i.e. fornecedoras de produtos e serviços - seja por entes públicos, as regras restritivas ao tratamento de dados se aplicarão, restando vedada ou limitada a sua utilização.

Consideradas essas premissas, conceituam-se dados sensíveis como "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação" (BIONI, 2018, p. 84). De acordo com esse conceito, mais importante do que identificar a natureza própria ou conteúdo do dado - conforme o rol do artigo 5o. II, LGPD - é constatar a potencialidade discriminatória no tratamento de dados pessoais. Isto é, a limitação para o tratamento de dados se concretizaria na proibição de seu uso de maneira a gerar uma discriminação, um uso abusivo e não igualitário de dados.

De maneira semelhante, Doneda entende que os dados sensíveis "seriam determinados tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva" (DONEDA, 2003, 160-161). Doneda assume a posição de que esta categoria de dados é determinada de acordo com o efeito de seu tratamento em relação aos demais dados pessoais. Isto porque, o valor tutelado, nesse caso, seria a igualdade material, acima do conteúdo tradicional da privacidade, e a liberdade, que permitiria ao titular dos dados o exercício de direitos de maneira autônoma, sem limitações abusivas ou indevidas. Ou seja, os conteúdos dos dados sensíveis trazidos no artigo 5o. II, da LGPD, são opções realizadas pelo legislador motivadas pelo efeito potencialmente lesivo do seu tratamento.

Críticas ao desenvolvimento do conceito e conteúdo de dados sensíveis existem, especialmente quando se considera que até mesmo dados que não são qualificados na

LGPD como sensíveis podem transformar-se em sensíveis se submetidos a um determinado tratamento, revelando aspectos da personalidade de uma pessoa, que, por sua vez, poderia levar a práticas de natureza discriminatórias. De acordo com Doneda, portanto, "um dado, em si, não é perigoso ou discriminatório - mas o uso que dele se faz, pode sê-lo" (DONEDA, 2003, 162). Daí poder se concluir que o conceito de dados sensíveis deve ser funcionalizado de acordo com o tratamento que é concedido a eles. Significa sustentar que dados sensíveis são qualificados como tais não só por conta de sua natureza intrinsecamente personalíssima, de forma apriorística, mas devido ao uso e finalidade que é concedido a esse dado por meio de um tratamento que pode gerar uma potencialidade discriminatória abusiva. Nesse mesmo sentido, entende Bioni que "um dado "trivial" pode também se transmudar em um dado sensível; particularmente, quando se têm disponíveis tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos" (BIONI, 2018, p. 84). Continua o autor, exemplificando essa transformação de dados no conhecido estudo que utilizou o Facebook como laboratório. De acordo com o estudo, levado a cabo pela Universidade de Cambridge, com base na análise de "curtidas" em determinados posts, seria possível identificar de forma fidedigna aspectos existenciais e sensíveis dos usuários da rede social, tais como a orientação sexual, a raça e a tendência político-partidária (BIONI, 2018, p. 85). Isto é, os dados coletados de "curtidas" que, por si só, não representam conteúdo sensível, foram tratados de forma a identificar dados sensíveis, de natureza personalíssima, e potencialmente discriminatórios.

Verifica-se, portanto, que 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, enfati-

zando-se, no caso de dados sensíveis, o uso dos mesmos de maneira que atenda 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, "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" (BODIN, TEFFÉ, 2016, 21).

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".[3] 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 ca-

---

[3] 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/. Consultado em 15 de novembro de 2019.

racterísticas 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, 70). Em complementação, Cohen relata alguns exemplos de 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).

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). Em posição crítica quanto a uma posição central ou preferencial do consentimento para o tratamento de dados - sejam sensíveis ou não -, Bruno Bioni afirma que é questionável a "efetividade de um quadro normativo focado no poder de escolha dos indivíduos" (BIONI, 2018, p. 114). Ainda que se considere que o consentimento seja o protagonista para a abordagem regulatória da proteção de dados, a sua centralidade abre espaço para hipóteses concretas que independem do consentimen-

to e que se encontram, de acordo com Bioni, numa posição de igualdade umas em relação às outras (BIONI, 2018, p. 115 e 116). Esta afirmação pode ser corroborada, inclusive, pela constatação de que tanto a hipótese de tratamento de dados sensíveis por meio do consentimento do titular, quanto aquelas que se referem às demais situações que independem desta manifestação de autonomia, previstas nos incisos I e II, do artigo 11, da LGPD, reconhece-se na técnica legislativa utilizada uma posição de igualdade entre estas hipóteses, e não a de prevalência do consentimento.

Assim, a LGPD permite, por exemplo, 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 e a interesses do titular de dados. Essas hipóteses serão analisadas em itens a seguir. 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.

2. Dados sensíveis e direitos fundamentais: uma identificação necessária.

De acordo com a Carta de Direitos Fundamentais da Comunidade Europeia (2000/C 364/01)[4], a proteção de dados deve ser caracterizada como um direito fundamental. A convenção reconhece que "todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito" (artigo 8º). O reconhecimento da proteção de dados está inscrito no Capítulo II da Carta, que trata das Liberdades, constatando-se que o conteúdo desse direito se aproxima da noção de auto-determinação informativa, tão cara a Stefano Rodotà (RODOTÀ, 2008). De maneira semelhante, reconhecendo sua

[4] A Carta consagra no direito comunitário um conjunto de direitos de natureza pessoal e política, além dos que representam aspectos de proteção econômica e social de todos cidadãos da União Europeia, incluindo também seus residentes. A Carta reafirma os direitos e garantias previstos na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 1950.

natureza fundamental, o artigo 1º do Regulamento Geral de Proteção de Dados da Comunidade Europeia, identifica como finalidade da lei a defesa dos "direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais". Contudo, apesar da natureza de direitos fundamentais, de acordo com Rodotà, "exigências de segurança interna e internacional, interesses de mercado e a reorganização da administração pública estão levando à diminuição de salvaguardas importantes, ou ao desaparecimento de garantias essenciais". Por consequência, "a privacidade, além de não ser mais vista como um direito fundamental, é, de fato, freqüentemente considerada um obstáculo à segurança, sendo superada por legislações de emergência" (RODOTÀ, 2007, 11).

Considerando que a coleta de dados sensíveis e a criação de perfis sociais pode levar à discriminação, a proteção de dados 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). Em sentido semelhante, Bioni conclui que "a proteção dos dados pessoais tem um papel de fundamental importância para que o indivíduo se realize e se relacione na sociedade, o que é um traço marcante dos direitos da personalidade (BIONI, 2018, p. 85). Conclui-se que a proteção de dados pessoais - enquanto decorrência da cláusula geral de tutela da pessoa humana e do direito à privacidade - é um requisito essencial para o exercício democrático.

A tutela jurídica de dados pessoais como um corolário do direito à privacidade (ou, eventualmente, 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.[5] O reconhecimento do direito fundamental à igualdade no artigo 5º, *caput*, da Constituição Federal tutela também o direito ao tratamento de dados sem distinções de qualquer natureza. Ao mesmo tempo, dentre os objetivos fun-

---

[5] Em sentido contrário, entende Bioni que os dados pessoais devem ser tratados como categoria autônoma de direitos da personalidade, afastando-se a noção de que a tutela desses dados seria consequência lógica da proteção da privacidade. Para o autor, "o direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana" (BIONI, 2018, p. 99).

damentais 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. Por estes motivos, a tutela dos dados pessoais sensíveis enquanto direito fundamental mostra-se essencial, especialmente se consideradas as características inerentes à proteção desses dados como instrumento para o exercício concreto do princípio da igualdade e da solidariedade social.

A falta de previsão constitucional da proteção de dados pessoais, contudo, parece estar perto do fim. Em fevereiro de 2019, o Senador Eduardo Gomes encaminhou ao Senado Proposta de Emenda à Constituição - PEC 17/2019 - que pretende acrescentar "o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria". Aguarda-se, desta forma, que o reconhecimento de direito fundamental aos dados pessoais possa permitir que os mesmos sejam garantidos de maneira prioritária em nosso ordenamento jurídico, visando a plena tutela da pessoa humana e sua proteção contra usos discriminatórios que possam comprometer o direito à igualdade, também reconhecido como direito fundamental em nossa Carta Magna.

3. Âmbito de aplicação do artigo 11, da LGPD: análise do parágrafo primeiro, do artigo 11, da LGPD, e o elemento danoso.

O âmbito de aplicação do artigo 11, da LGPD, vem delimitado em seu parágrafo primeiro, indicando que este deverá ser aplicado a qualquer tratamento de dados pessoais que revele dados sensíveis, conforme exposto nos itens anteriores. Com essa locução, parece ficar claro que se aplica o art. 11 a todas as hipóteses em que os dados tratados são considerados sensíveis, e também às hipóteses em que os dados pessoais não tem a característica de sensíveis, mas podem "revelar" dados sensíveis. Em análise da decisão do Tribunal Constitucional Alemão que reconheceu o direito à autodeterminação informativa, Bioni reconhece que "deslocou-se, por exemplo, a discussão sobre se um dado é sensível ou se esconderia algo íntimo da pessoa para se considerar que qualquer dado pessoal pode angariar um efeito lesivo" (BIONI, 2018, ps. 102-103).

Há, em continuidade, a complementação desse parágrafo primeiro, em que se indica o dano como elemento da aplicação das regras referentes a dados sensíveis. Ao estatuir que se aplica o artigo 11, da LGPD, a qualquer tratamento de dados pessoais que revele de forma abusiva ou ilícita dados pessoais sensíveis, causando dano ao seu titular, parece que o legislador quis vincular esta hipótese à geração de um dano. Isto é, a aplicação do artigo 11, da LGPD, somente estaria legitimada se o tratamento de dados pessoais que revela dados sensíveis gerar algum dano ao titular dos dados. Esta interpretação, contudo, limitaria sobremaneira a aplicação do artigo 11, da LGPD. Primeiro, porque a prova do dano concreto, por vezes, seria de difícil realização. Segundo, porque as consequências danosas são, em grande medida, refletidas na coletividade e não na subjetividade de cada titular de dados. Significa dizer que quando estamos diante de um dano causado pelo tratamento de dados pessoais sensíveis, ele se revela na coletividade com maior relevância, através, por exemplo, do perfilamento de pessoas, com base em análises estatísticas em que se presume uma realidade que, eventualmente, não reflete as características de uma pessoa concretamente considerada, gerando uma discriminação abusiva. Isso não significa dizer que a pessoa, em sua subjetividade, fica afastada da possibilidade de arguir a existência de um dano concreto que a atingiu particularmente. Esse direito estará resguardado. Contudo, parece que a conexão que é realizada nesse parágrafo entre o tratamento de dados sensíveis e os danos ocasionados por essa atividade foge do escopo de tutela pretendida pela lei, que deve ser a mais ampla possível.

Mais correto seria, portanto, interpretar o parágrafo primeiro do artigo 11, considerando que a menção a dano ali prevista complementa o entendimento de que o tratamento de dados pessoais sensíveis gerará sempre danos de natureza personalíssima por violação dos direitos de privacidade, liberdade ou identidade, fundamentos da proteção de dados. Portanto, opina-se no sentido de que toda a vez que houver tratamento de dados pessoais sensíveis realizado fora das hipóteses previstas no artigo 11, I e II, da LGPD, haverá dano presumido por violação dos direitos fundamentais acima elencados. O dano seria, assim, in *re ipsa*, configurado pelo mero tratamento irregular ou inade-

quado, sem a necessidade de provar-se a existência de outras consequências jurídicas, tais como um desvalor patrimonial.[6]

4. A responsabilidade civil dos agentes de tratamento de dados pessoais sensíveis é subjetiva ou objetiva?

Conforme abordado nos itens anteriores, apesar do artigo 5º, II, da LGPD, trazer o conceito de dados sensíveis - exemplificado por um rol não taxativo, frise-se - deve-se considerar que o tratamento de dados que não estejam categorizados na lei como tal pode conduzir a resultados práticos discriminatórios, cujos efeitos a LGPD visa impedir justamente ao reconhecer e tutelar esta categoria de dados sensíveis. Isto é, a categoria de dados sensíveis não deve ser considerada como estruturalmente diversa da categoria de dados não sensíveis, na medida em que tanto uma, quanto outra estão sujeitas à potencialidade de tratamentos discriminatórios e geradores de danos a seus titulares. Sendo assim, não deve haver uma diferenciação de regimes de responsabilidade civil, baseada numa classificação dos dados como sensíveis ou não. Ou seja, o regime de responsabilidade civil adotado pela Lei Geral de Proteção de Dados Pessoais é único, independentemente da natureza do dado tutelado, se sensível ou não, pois a consequência de sua violação - o dano patrimonial ou moral, individual ou coletivo - independerá dessa categorização, devendo ser integralmente reparado.

A LGPD, em seus artigos 42 a 45, estabelece as regras referentes à responsabilidade civil dos agentes de tratamento de dados pessoais, inaugurando um debate doutrinário a respeito da natureza da obrigação de indenizar, se subjetiva - baseada na conduta culposa do agente de tratamento - ou objetiva - fundamentada no risco da atividade desenvolvida pelos agentes.[7] Estas normas, por sua vez, são justificadas por três princípios da Lei Geral de Tratamento de Dados Pessoais, quais sejam, os princípios da

---

[6] Em sentido semelhante ao que se adota nesse entendimento, o Superior Tribunal de Justiça, em consolidação de entendimento de julgamentos, promulgou a Súmula 403, que expõe que "independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais". Sugere a súmula que a só divulgação da imagem, sem consentimento da pessoa retratada, já configuraria, por si só, um dano de natureza extrapatrimonial.

[7] O Regulamento Europeu de Proteção de Dados Pessoais possui regras semelhantes a adotadas em nossa legislação, reconhecendo no Artigo 82 e Considerando 146, RGPD, a obrigação de indenizar danos causados quando houver violação do regulamento.

segurança[8], da prevenção[9] e da responsabilização e prestação de contas[10]. Complementa o debate, os artigos 46 e seguintes, da LGPD[11], que tratam da segurança de dados, governança e sanções administrativas adequadas em caso de incidentes de segurança. Reconhece este artigo, portanto, as boas práticas aplicáveis ao tratamento de dados pessoais, indicando a necessidade de adoção de medidas que previnam e evitem danos aos titulares de dados.

De acordo com Gisela Sampaio da Cruz Guedes e Rose Melo Vencelau Meireles (GUEDES, MEIRELES, 2019, p. 231), a LGPD adotou claramente a teoria subjetiva da responsabilidade civil, devendo haver a prova da culpa do agente de tratamento na ocasião do dano, por sua vez fundamentada (i) na omissão na adoção de medidas de segurança para o tratamento adequado dos dados ("quando não fornecer a segurança que o titular dele pode esperar,"); (ii) no descumprimento das obrigações impostas na lei ("em violação à legislação de proteção de dados pessoais" ou "quando deixar de observar a legislação"). Para as autoras, "o legislador criou uma série de deveres de cuidado que devem ser seguidos pelo controlador e pelo operador, sob pena de virem a ser responsabilizados". As autoras indicam que o Capítulo VI da LGPD (artigos 46 a 54) - que trata de *standards* de conduta (culpa normativa)[12] a serem seguidos pelos agentes de tratamento de dados para a segurança, sigilo, boas práticas e governança de dados - seria o fundamento para o reconhecimento da responsabilidade subjetiva. Em complementação, na análise das excludentes de responsabilidade do artigo 43, da LGPD, o inciso II pareceria indicar a adoção de uma excludente tipicamente relacionada às hipóteses de res-

---

[8] Art. 6, VII, LGPD - 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.

[9] Art. 6, VIII, LGPD - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[10] Art. 6, X, LGPD - 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.

[11] Art. 46, LGPD. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

[12] Para Maria Celina Bodin de Moraes, "a noção normativa de culpa, como inobservância de uma norma objetiva de conduta, praticamente substitui a noção psicológica, com vistas a permitir que se apure o grau de reprovação social representado pelo comportamento concreto do ofensor, isto é, a correspondência, ou não, do fato a um padrão (standard) objetivo de adequação, sem que se dê relevância à sua boa ou má intenção. (...) a figura do ilícito permanece ancorada no fato "culposo", o qual, porém, foi redefinido, através dessa concepção da culpa, como sendo um fato avaliado negativamente em relação a parâmetros objetivos de diligência". Moraes, Maria Celina Bodin de. Danos à pessoa humana. Renovar: Rio de Janeiro, 2003, p. 212.

ponsabilidade civil subjetiva. Estabelece este inciso que os agentes de tratamento de dados só não serão responsabilizados se, ainda que exista o dano, não houver violação da legislação de proteção de dados. A violação da lei, para as autoras, seria elemento subjetivo da obrigação de indenizar e indicaria a conduta culposa do agente de tratamento de dados. Assim, não haverá obrigação de indenizar quando o agente de tratamento de dados tiver demonstrado que "(…) observou o *standard* esperado e, se o incidente ocorreu, não foi em razão de sua conduta culposa" (GUEDES, MEIRELES, 2019, p. 236). Em resumo, sustentam as autoras que a LGPD adota a teoria subjetiva da responsabilidade civil, calcada em duas "dicas" deixadas pelo legislador: (i) no artigo 42, quando o legislador faz menção a medidas de segurança; (ii) no art. 43, II, quando o legislador estabelece excludente de ilicitude referente ao cumprimento das normas da LGPD.

Em posição diversa, Maria Celina Bodin de Moraes e João Quinelato Queiroz (MORAES, QUEIROZ, 2019) acreditam que a LGPD adota a chamada teoria ativa ou proativa da responsabilidade civil. Esta teoria indica a necessidade de olhar-se a responsabilidade civil de um ponto de vista positivo, sustentado pela necessidade da adoção de posturas pelos agentes de tratamento de dados que tutelem a prevenção de danos, sendo a obrigação de indenizar medida excepcional a ser tomada. De acordo com os autores, "a proteção da intimidade por vias da mera não interferência na esfera individual cede espaço à tutela positiva e proativa, isto é, que garanta ao titular o conhecimento pleno das formas de tratamento, finalidade e destino de seus dados" (MORAES, QUEIROZ, 2019, p. 118). Complementam essa afirmação, indicando que os dados pessoais, por constituirem conteúdo do direito à privacidade, impõem que "a coleta e o tratamento de dados pessoais deve ser precedida de medidas rigorosas e eficazes de proteção, especialmente em relação aos dados sensíveis, núcleo duro da dignidade humana" (MORAES, QUEIROZ, 2019, p. 119). Os autores sustentam que a "responsabilidade proativa" encontra-se justificada no art. 6º, X, da LGPD, que reconhece o princípio da responsabilização e prestação de contas que impõem aos agentes de tratamento de dados pessoais a "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". Para os autores,

> as características peculiares da hipótese de responsabilidade civil em questão – que se expressam principalmente na regulação detalhada das obrigações comportamentais do controlador e do operador de dados, com um novo foco no perfil de gerenci-

> amento de riscos, especialmente relacionado ao uso da inovação tecnológica – possibilita garantir a efetividade do recurso de compensação, adaptando- o às especificidades da atividade de processamento de dados pessoais e aos requisitos de proteção que ele apresenta (MORAES, QUEIROZ, 2019, p. 133-134).

De outro lado, Danilo Doneda e Laura Schertel Mendes (DONEDA, MENDES, 2018) consideram que a atividade de tratamento de dados encerra um risco intrínseco, na medida em que há uma potencialidade danosa considerável em caso de violação desses direitos, que se caracterizam por sua natureza de direito personalíssimo e de direito fundamental. Partem os autores da constatação de que a legislação de proteção de dados tem como um dos seus principais fundamentos a diminuição de riscos de dano. Tanto assim, que a lei adota como princípio, no artigo 6, III, o da necessidade que impõe a "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". Este dever estaria relacionado diretamente ao fator de risco referente ao tratamento de dados. Para eles:

> A consideração da responsabilidade dos agentes leva em conta, em primeiro lugar, a natureza da atividade de tratamento de dados, que a LGPD procura restringir às hipóteses com fundamento legal (art. 7º) e que não compreendam mais dados do que o estritamente necessário (princípio da finalidade, art. 6º, III) nem sejam inadequadas ou desproporcionais em relação à sua finalidade (art. 6º, II). (DONEDA, MENDES, 2018, p. 479).

Estas considerações a respeito da finalidade da lei e dos princípios por ela adotados (necessidade, minimização, responsabilidade e prestação de contas, entre outros), levam Mendes e Doneda a concluir que o legislador optou por um regime de responsabilidade objetiva, vinculando o exercício da atividade de tratamento de dados pessoais a um risco inerente, potencialmente causador de danos a seus titulares.

Analisando os princípios acima indicados, de acordo com o artigo 6º, X, da LGPD, que reconhece o princípio da responsabilização e prestação de contas, os agentes de tratamento devem apresentar medidas de segurança eficazes e capazes de comprovar que o agente de tratamento está em conformidade com a lei. O princípio da prestação de contas estabelece a necessidade, primeiramente, de atender à transparência a ser adotada

pelo agente de tratamento de dados acerca dos procedimentos que são tomados para a segurança no tratamento de dados. Esta transparência - que pode muito bem ser considerada como uma consequência da proteção do princípio da boa-fé objetiva - deve ser considerada como um dever “ativo”. Isto é, aos titulares de dados devem ser comunicadas todas as medidas de segurança que serão tomadas para evitar o dano. A transparência, por sua vez, gera a obrigação ao agente de tratamento de prestar contas, onde serão evidenciadas as medidas que estão sendo tomadas para uma atuação em conformidade com as boas práticas impostas pela lei. Uma das formas, inclusive, de avaliação destas práticas se dá pelo chamado relatório de impacto à proteção de dados pessoais, que se configura como a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (art. 5, XVII, LGPD). O uso deste termo - “mecanismos de mitigação do risco” -, refere-se à capacidade do pretenso ofensor de reconhecer previamente os riscos relacionados à atividade que ele desenvolve e tomar as medidas para evitar o dano, numa antecipação que o controlador ou operador deverá considerar para evitar a obrigação de reparar, por meio da gestão dos riscos relacionados à atividade desenvolvida.

Consideradas as posições opostas levantadas pelos autores citados, afirma-se que a Lei Geral de Proteção de Dados, em seu artigo 42, adota a teoria que impõe a obrigação de indenizar independentemente da análise da culpa dos agentes de tratamento de dados, isto é, a responsabilidade civil é objetiva. Fundamenta esta conclusão o fato de que a atividade desenvolvida pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados. Estes riscos, por sua vez, são intrínsecos, inerentes à própria atividade. Significa dizer que os danos resultantes da atividade habitualmente empenhada pelo agente de tratamento de dados, uma vez concretizados, são quantitativamente elevados - pois atingem um número indeterminado de pessoas - e qualitativamente graves - pois violam direitos que possuem natureza personalíssima, reconhecidos pela doutrina como direitos que merecem a estatura jurídica de direitos fundamentais.

5. Tratamento irregular e artigo 44, LGPD e seu confronto com o artigo 42, LGPD.

Trata o artigo 44 da hipótese em que se reconhece que haverá tratamento irregular de dados quando o agente de tratamento (i) deixar de observar a legislação; ou (ii)

não oferecer a segurança que o titular dele pode esperar (legítima expectativa). Por sua vez, estes dois fundamentos que formam o conceito do tratamento irregular de dados devem ser analisados considerando, dentre outras circunstâncias, o modo como o tratamento é realizado, o resultado e os riscos razoavelmente esperados pelo tratamento e as técnicas de tratamento de dados disponíveis à época em que este foi realizado.[13] Complementa a redação do artigo 44, o seu parágrafo único, que estabelece que o controlador ou o operador será obrigado a indenizar os danos decorrentes da violação da segurança dos dados quando deixarem de adotar as medidas de segurança previstas no art. 46, da LGPD, quais sejam, aquelas "aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".[14]

Com base na redação do artigo 44, LGPD, questiona-se se o legislador inaugurou um regime de responsabilidade civil diverso daquele adotado no artigo 42, LGPD. Essa indagação se deve ao fato de que (i) o artigo 44, LGPD, utiliza a expressão "tratamento irregular", condicionando a hipótese de responsabilidade civil prevista em seu parágrafo único, à qualificação de irregularidade definida no artigo 46, LGPD, e (ii) o artigo 46, LGPD, encontra-se inserido no Capítulo VII, que trata da "Segurança e Boas Práticas", na Seção I, "Da Segurança e Sigilo de Dados", que se refere às medidas de segurança e boas práticas que devem ser adotadas pelo agente de tratamento para a prevenção de danos decorrentes de incidentes de segurança. Assim, enquanto o artigo 42, LGPD, impõe a obrigação de indenizar "em razão do exercício de atividade de tratamento de dados pessoais", o artigo 44 e seu parágrafo único, LGPD, determinam a obrigação de indenizar caso haja tratamento irregular de dados pessoais, identificado como sendo aquele decorrente da "violação da segurança dos dados". Parece que o legislador quis identificar nessa hipótese situações danosas que decorrem especificamente de inci-

---

[13] Em relação a este último fundamento ("riscos razoavelmente esperados pelo tratamento e as técnicas de tratamento de dados disponíveis à época em que este foi realizado"), questiona-se se o legislador reconheceu na hipótese a teoria do risco de desenvolvimento que poderia servir como eventual excludente de responsabilidade civil do agente de tratamento de dados pessoais, por não ser possível a ele técnica e temporalmente conhecer métodos de tratamento de dados que, se aplicados, poderiam ter evitado o dano. Sobre a teoria do risco de desenvolvimento e as consequências de sua adoção para a manutenção ou exclusão da responsabilidade do fornecedor de produtos na seara do Direito do Consumidor, ver, por todos, Calixto, Marcelo Junqueira. A responsabilidade civil do fornecedor de produtos pelos riscos de desenvolvimento. Rio de Janeiro: Renovar, 2004.

[14] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

dentes de segurança que são, por sua vez, acontecimentos que se relacionam ao risco inerente ao desenvolvimento da atividade de tratamento de dados, como vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados. Neste sentido, esses riscos devem ser necessariamente situados como intrínsecos à atividade de tratamento de dados e, portanto, considerados, em última análise, como hipótese de fortuito interno, incapazes de afastar a obrigação dos agentes de tratamento de indenizar os danos causados pelos incidentes.

Conclui-se, portanto, que apesar do uso de expressões diversas em sua redação, tanto o artigo 42, quanto o artigo 44, da LGPD, adotam o fundamento da responsabilidade civil objetiva, impondo aos agentes de tratamento a obrigação de indenizar os dados causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador.

Conclusão.

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, 153).

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. Assim, a adoção de sistema de responsabilidade civil objetiva pela Lei Geral de Proteção de Dados visa proteger de maneira rigorosa os dados pessoais sensíveis e se torna, com isso, instrumento para a tutela e efetivação da igualdade e da liberdade.

Referências bibliográficas.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Forense, 10/2018.

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.

FRAZÃO, Ana. A nova Lei Geral de Proteção de Dados: Repercussões para a atividade empresarial: o tratamento dos dados pessoais sensíveis, Parte V, IN: https://www.jota.info/opiniao-e-analise/colunas/constituicao- empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis- 26092018. Consultado em 14.02.2019.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "Término do tratamento de dados", IN: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoais, Editora RT: São Paulo, 2019, p. 231.

LEONARDI, Marcel. Tutela e privacidade na Internet. 1. ed. São Paulo, Saraiva, 2012. v. 1. 402p.

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

MENDES, Laura Schertel. Habeas data e autodeterminação informativa. Os dois lados de uma mesma moeda. DIREITOS FUNDAMENTAIS & JUSTIÇA, v. 39, p. 350, 2018.

MENDES, Laura Schertel; DONEDA, D. . Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. REVISTA DE DIREITO DO CONSUMIDOR, v. 120, p. 555, 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. REVISTA DE DIREITO DO CONSUMIDOR, v. 120, p. 469-483, 2018.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor, linhas gerais de um novo direito fundamental. 1. ed. São Paulo, Saraiva, 2014.

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.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. IN: Cadernos Adenauer, volume 3, Ano XX, 2019.

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.

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, 2018.

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

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

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.