A LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018) E O DIREITO DO CONSUMIDOR

Revista dos Tribunais | vol. 1009/2019 | Nov / 2019
DTR\2019\40668

Bruno Miragem
Professor da Universidade Federal do Rio Grande do Sul (UFRGS), em seus cursos de graduação e no Programa de Pós-Graduação em Direito. Advogado e parecerista.
bmiragem@uol.com.br

Área do Direito: Consumidor; Digital
Resumo: O presente artigo tem por objetivo examinar a repercussão da Lei Geral de Proteção de Dados sobre as relações de consumo e os direitos do consumidor no Brasil, em especial, considerando sua harmonia com o Código de Defesa do Consumidor.

Palavras-chave: Proteção de dados – Direitos do consumidor – Lei Geral de Proteção de Dados – Código de Defesa do Consumidor
Abstract: This article aims to examine the impact of the General Data Protection Law on consumer relations and consumer rights in Brazil, in particular, considering its harmony with the Consumer Protection Code.

Keywords: Data protection – Consumer rights – General Data Protection Law – Consumer Protection Code

Sumário:

1 Introdução

O acesso e utilização dos dados pessoais compreende um dos principais ativos empresariais na sociedade contemporânea e, ao mesmo tempo expressão dos riscos à privacidade frente às novas tecnologias da informação,[1] repercutindo por isso, amplamente, no mercado de consumo e, consequentemente, sobre o direito do consumidor.[2] O desenvolvimento da tecnologia da informação e a capacidade de processamento de imenso volume de dados variados (Big data), permite o refinamento das informações de modo a permitir uma série de utilidades, como a segmentação dos consumidores para quem se dirige uma oferta, maior precisão na análise dos riscos de contratação (seleção de risco), formação de bancos de dados com maior exatidão e eficiência do uso das informações coletadas, de modo a tornar a capacidade de acesso a tratamento de dados um dos valores mais relevantes atualmente.

Esta nova capacidade de tratamento de dados permite a identificação de tendências, não mais baseadas em amostragens, mas no processamento da universalidade dos dados. Deste modo, aumenta a precisão e as possibilidades de resultados a serem obtidos, permitindo, dentre outros resultados, identificar padrões de consumo, conforme o comportamento de compra dos consumidores, sua localização (e.g. as discutidas técnicas de geopricing, pelas quais a determinação do preço de produtos ou serviços se dá conforme o lugar em que esteja o consumidor), a interação em redes sociais, ou a personalização da negociação com consumidores mediante uso de regras pré-determinadas ou de inteligência artificial (os denominados Chatbots).

A rigor, o acesso e tratamento de dados pessoais da população em geral dá causa a repercussões não apenas econômicas, mas afeta também, profundamente, relações

sociais e políticas, dado suas interações com temas aparentemente distintos entre si, com a qualidade do debate público, a liberdade de manifestação, a proteção da reserva pessoal e da privacidade, dentre outros temas fundamentais para o desenvolvimento humano.

Daí a decisão político-jurídica de diversos sistemas jurídicos no sentido de disciplinar a coleta e, sobretudo, o tratamento de dados pessoais por intermédio de legislação específica sobre o tema. O Brasil associou-se a este esforço de disciplina legislativa da proteção de dados pessoais com a edição, em 2018, da Lei 13.709, de 14 de agosto de 2018 (LGL\2018\7222) – denominada Lei Geral de Proteção de Dados (LGPD). Fundamenta-se a LGPD no propósito de garantia dos direitos do cidadão, oferecendo bases para o desenvolvimento econômico a partir da definição de marcos para utilização econômica da informação decorrente dos dados pessoais.[3]

São reconhecidas diferentes influências à LGPD, dentre as quais tem especial relevância as normas que definem o modelo europeu de proteção de dados, em especial o Regulamento Geral de Proteção de Dados (Regulamento 2016/679), que substituiu a Diretiva 46/95/CE, sobre tratamento de dados pessoais, e a Convenção 108, do Conselho da Europa, que já em 1981 buscava dispor sobre a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. Sem prejuízo da influência reconhecida de outros sistemas jurídicos, e mesmo de outras leis brasileiras.[4]

Dentre os fundamentos da LGPD está relacionada a defesa do consumidor (art. 2º, VI), que também prevê, expressamente, a competência dos órgãos de defesa do consumidor para atuar, mediante requerimento do titular dos dados, no caso de infração aos seus direitos pelo controlador (art. 18, § 8º) e o dever de articulação entre a Autoridade Nacional de Proteção de Dados e outros órgãos titulares de competência afeta a proteção e dados, como é o caso dos órgãos de defesa do consumidor (art. 55-K, parágrafo único). Da mesma forma, a exemplo do que dispõe o CDC (LGL\1990\40) em matéria de não exclusão (e cumulação) dos direitos e princípios que consagra em relação àqueles estabelecidos em outras leis, o art. 64 da LGPD, expressamente, consigna: "Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

Trata-se da adoção expressa da interpretação sistemática segundo a técnica do diálogo das fontes, ademais desenvolvida no próprio direito do consumidor.[5]

2 A proteção de dados pessoais e sua repercussão no mercado de consumo

A proteção de dados pessoais é projeção de direitos fundamentais consagrados. Relaciona-se com a proteção da vida privada e da intimidade (art. 5º, X, da CF (LGL\1988\3)), da dignidade da pessoa humana (art. 1º, III, da CF (LGL\1988\3)) e contra a discriminação (art. 3º, IV), como expressões da liberdade e da igualdade da pessoa. A Constituição da República, igualmente, assegura como direito fundamental a inviolabilidade do sigilo de dados (art. 5º, XII). Por tais razões sustenta-se a autonomia da proteção de dados pessoais, como direito da personalidade,[6] ou a especialização da proteção constitucional à vida privada e à intimidade dando origem a um direito fundamental à proteção de dados pessoais.[7] A Lei Geral de Proteção de Dados, nesta linha, define em seu art. 1º, seu objetivo de proteção dos "direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

Mesmo antes da edição da LGPD construiu-se, no direito brasileiro, por influência do direito comparado,[8] a noção de autodeterminação informativa,[9] colocando sob a égide da decisão livre e racional da pessoa a quem os dados digam respeito (titular dos dados), o poder jurídico para determinar a possibilidade e finalidade de sua utilização, assim como seus limites. O exercício deste poder se define, sobretudo a partir da noção de consentimento do titular. No direito brasileiro, a exemplo de vários sistemas jurídicos

estrangeiros, o consentimento para uso dos dados polariza a disciplina da proteção dos dados pessoais.[10]

Neste particular, registre-se que consente que responde afirmativamente a pedido ou proposta. Expressa estar de acordo com algo que se lhe apresenta. Esta noção de consentimento para coleta e uso dos dados é a regra que imediatamente se deduz do reconhecimento da autodeterminação informativa,[11] de modo que se deva admitir o uso dos dados apenas na hipótese de autorização legal ou da concordância do titular dos dados. Neste particular, é relevante a referência do Regulamento Geral de Proteção de Dados europeu, que se refere à "manifestação de vontade livre, específica, informada e inequívoca" (art. 7º).

Na perspectiva econômica, a posse de dados pessoais adquire crescente valor. Observa-se no mercado de consumo a transição entre a economia de produção em massa, mediante oferta de produtos de consumo massificados, que deu origem e sentido à noção de sociedade de consumo, a partir do final da Segunda Grande Guerra (1945), para uma economia da especialização flexível,[12] marcada por diferentes características em relação ao modelo que o precede,[13] deslocando a competição exclusivamente baseada em preços pela especialização do produto, pelo qual os fornecedores buscam a diferenciação de seus produtos e serviços em relação a seus concorrentes, frente aos consumidores.[14]

Isso implica em mudanças decisivas no mercado de consumo e novos riscos.[15] Os fornecedores cada vez mais ocupam-se não apenas de atrair consumidores pela publicidade, mas a sua fidelização, buscando identificá-los com determinado produto ou serviço a partir de sua customização (de modo que não mais se mire os consumidores em geral, mas certo grupo de modo individualizado).[16] Para tanto, é necessário aos fornecedores terem informações precisas sobre os consumidores de modo que possam realizar sua segmentação de acordo com características comuns, no que se insere a importância dos dados pessoais.

É conhecido o exemplo de uma grande empresa varejista norte-americana que, mediante uso do Big Data, passou a inferir a probabilidade de gravidez de suas consumidoras, inclusive o estágio em que se encontra, mediante verificação da lista de produtos que é habitualmente adquiriam. Deste modo utilizou-se a informação para direcionar produtos de acordo com sua fase da gravidez. Este exemplo permite identificar o modo como se utilizam os dados pessoais no mercado de consumo, de modo que a partir da correlação entre vários dados faz com que se determine um padrão, de modo a prever sua repetição no futuro, direcionando-se ações de publicidade em favor de um grupo segmentado de consumidores.[17]

Há diferentes informações que interessam aos fornecedores. Tradicionalmente, os bancos de dados organizaram-se sobretudo para permitir a mensuração do risco de crédito no mercado. Ou seja, para avaliação da capacidade de pagamento do consumidor e seu comportamento pretérito em relação a dívidas constituídas. Não por acaso, será sobre esta espécie que recairá a disciplina específica do CDC (LGL\1990\40) (art. 43) e cujos métodos até hoje são continuamente aperfeiçoados (assim o "cadastro positivo de crédito" e os sistemas de pontuação que se examinam em outro item), e normalmente contam com previsão de regras próprias.

Porém, para a formação de perfis e segmentação de consumidores, interessam dados relativos as suas transações comerciais (tais como o histórico de transações, frequência e valores envolvidos), estilo de vida e preferências pessoais, interesses e hábitos, obtidos por questionários diretos (como os que envolvem há décadas, a participação em prêmios e sorteios comerciais), ou análise de comportamento, mediante pesquisas ou coleta de informações específicas, como é o caso do itinerário de navegação na internet, utilização de dispositivos associados à internet das coisas,[18] ou as diferentes manifestações e reações em redes sociais e outros espaços virtuais de interação.

2.1.1 Princípios da Lei Geral de Proteção de Dados e o direito do consumidor

A edição da Lei Geral de Proteção de Dados incrementa a tutela dos direitos do consumidor prevista no CDC (LGL\1990\40). O regime previsto pela LGPD não exclui aquele definido pelo CDC (LGL\1990\40). A incidência em comum dos arts. 7º do CDC (LGL\1990\40) e 64 da LGPD firmam a conclusão de que os direitos dos titulares dos dados previstos nas respectivas normas devem ser cumulados e compatibilizados pelo intérprete.

Isso repercute tanto na coleta de informações e formação dos bancos de dados, quanto no tratamento destes mesmos dados e seu compartilhamento entre diferentes gestores de bancos de dados e fornecedores. Conforme já foi mencionado, o CDC (LGL\1990\40) ao disciplinar os bancos de dados o fez de modo restrito, com atenção aos bancos de dados restritivos de crédito (art. 43). A ausência de normas relativas a outras espécies de bancos de dados no CDC (LGL\1990\40) e, originalmente, no restante da legislação, por um lado expandiu o âmbito de aplicação do art. 43 do CDC (LGL\1990\40), assim como permitiu o exame da questão para além do expressamente previsto em lei.

Por outro lado, a tendência do direito brasileiro, consagrada inicialmente no art. 43 do CDC (LGL\1990\40) e depois pela Lei 12.414/2011 (LGL\2011\1883), foi a de disciplinar especialmente os bancos de dados relativos a informações de crédito, não se ocupando, em um primeiro momento, com outras variantes de coleta e tratamento de dados.

Apenas com a edição da Lei 12.965/2014 (LGL\2014\3339) – o Marco Civil da Internet – é que serão definidas regras gerais sobre proteção de dados, ainda que aplicáveis apenas em relação ao fluxo de informações na internet. A proteção de dados pessoais é fixada como princípio da disciplina do uso da internet (art. 3º, III). Da mesma forma, é previsto o consentimento expresso para "coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" (art. 7º, IX) e o direito à "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei" (art. 7º, X). Da mesma forma, assegura a aplicação da lei brasileira a quaisquer situações em que pelo menos um dos atos de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet ocorra em território nacional (art. 11).

Deste modo, o tratamento de dados realizados com a finalidade direta ou indireta de fomentar a atividade econômica do fornecedor no mercado de consumo, submete-se à incidência, em comum, do CDC (LGL\1990\40) e da LGPD. Neste particular, registre-se que a LGPD estabelece uma definição ampla de tratamento de dados, como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, X).

Da mesma forma, quando tais operações se realizem por intermédio da internet, incidirá também o Marco Civil da Internet, devendo ser compatibilizadas as normas das respectivas legislações.

Ao incidir sobra a formação de bancos de dados de consumidores e a consequente utilização das informações neles arquivadas para fomentar a atividade negocial do fornecedor no mercado de consumo, a LGPD deve ser compreendida tanto a partir dos princípios que delineia para a coleta e tratamento de dados em geral, quanto dos direitos do titular dos dados e procedimentos para a regular coleta e tratamento dos dados.

A LGPD, ao definir disciplina específica e detalhada para a coleta e tratamento de dados, abrangente, inclusive daqueles que digam respeito aos consumidores no mercado de consumo, vai definir e articular uma série de princípios que informam esta atividade. A

adequada compreensão destes princípios é relevante para o exame da disciplina de proteção de dados e seu uso permitido segundo os critérios definidos na legislação.

2.1.1.1 Boa-fé

O art. 6º, caput, da LGPD, define que as atividades de tratamento de dados pessoais deverão observar a boa-fé. Trata-se a boa-fé de princípio que disciplina amplamente relações jurídicas de direito público e privada. Tem por conteúdo essencial, a par das diversas funções que desempenha no sistema jurídico, a eficácia criadora de deveres anexos àqueles que decorrem da lei ou do conteúdo expresso da relação jurídica. É comum que a ela se associem os deveres de cooperação e lealdade, assim como o respeito às legítimas expectativas das partes. No caso do tratamento de dados pessoais, a boa-fé fundamenta a tutela das legítimas expectativas do titular dos dados frente ao controlador (art. 10, II, da LGPD), o que se delineia, sempre a partir das circunstâncias concretas em que se deu o consentimento, a finalidade de uso e tratamento dos dados que foi indicada na ocasião e o modo como foram compreendidas as informações prévias oferecidas. A tutela da confiança do consumidor, neste caso, abrange tanto a crença nas informações prestadas quando de que aquele que tenha acesso aos seus dados, por força do consentimento dado, não se comporte de modo contraditório a elas e respeite a vinculação à finalidade de utilização informada originalmente.

Neste particular, recorde-se que a proteção dos dados pessoais se justifica pela proteção à privacidade do titular dos dados. Privacidade é conceito objetivo, mas também contextual, uma vez que se vincula à expectativa legítima do titular do direito em ter preservada, sob certas condições, informações a seu respeito da exposição pública. Dos termos do consentimento resulta esta expectativa, de modo que não poderá o fornecedor ou o controlador dos dados, dando uso diverso da finalidade que motivou o consentimento do consumidor, tal qual foi compreendida por ele, defender a utilização a partir de critérios outros que não aquele que caracterizou o efetivo entendimento do titular dos dados. São relevantes aqui para a correta compreensão desta expectativa legítima do consumidor, tanto as informações e esclarecimentos prestados na ocasião da obtenção do consentimento, quanto a situação específica de vulnerabilidade do consumidor, decorrente da lei, ou de situação concreta que acentue esta característica (vulnerabilidade agravada).

Esta compreensão quanto à expectativa legítima do consumidor titular dos dados no fornecimento do consentimento, igualmente, revela-se pela definição do dever de informar do fornecedor na fase pré-contratual, conforme define o art. 9º, § 3º, da LGPD, ao dispor que "quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei." Trata-se de regra de grande importância nas relações de consumo, sobretudo ao regular as denominadas políticas de tudo ou nada, (take-it-or-leave-it-choice),[19] submetendo o consumidor a opção de aceitar integralmente as disposições ou termos de serviço como condição para sua utilização.

O art. 18, de sua vez, estabelece o direito do titular dos dados de obter do controlador, a qualquer momento e mediante requisição, a adoção das seguintes providências: I – confirmação da existência de tratamento; II – acesso aos dados existentes; III – correção de dados incompletos, inexatos ou desatualizados; IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas na lei; VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX – revogação do consentimento.

A operacionalização da boa-fé no tratamento de dados do consumidor pode servir-se, igualmente, do disposto no art. 30 do CDC (LGL\1990\40) que respeita à eficácia vinculativa da oferta e à preservação da integridade da informação pré-negocial do fornecedor. Refere a norma do CDC (LGL\1990\40) que "toda informação ou publicidade, suficientemente precisa, veiculada por qualquer forma ou meio de comunicação com relação a produtos e serviços oferecidos ou apresentados, obriga o fornecedor que a fizer veicular ou dela se utilizar e integra o contrato que vier a ser celebrado." A rigor, é possível, com fundamento na boa-fé, considerar informações vinculantes aquelas que geram expectativa legítima do consumidor, independentemente de terem sido prestadas antes da contratação ou contradigam o próprio instrumento escrito (como pode ocorrer com o consentimento para uso de dados, no qual informação pré-contratual seja contradita pelos termos de cláusula ou termo de consentimento escrito), assim como a possibilidade da interpretação mais favorável ao consumidor nos termos do art. 47 do CDC (LGL\1990\40).

2.1.1.2 Finalidade

O princípio da finalidade é central na disciplina da proteção de dados pessoais. A finalidade da utilização dos dados é requisito do consentimento. O titular dos dados pessoais ao consentir o faz para que sejam utilizados para certa e determinada finalidade, que deve ser expressa. No direito europeu, os dados pessoais "recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais (...)" (art. 5º, I, b, do Regulamento Geral de Proteção de Dados da UE).

O art. 6º, I, da LGPD define o conteúdo do princípio da finalidade vinculando-o à "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Trata-se de princípio que, conforme assinala a doutrina, tem grande relevância prática, afinal, "com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)".[20] Aquele que pretende obter o consentimento do titular dos dados, obriga-se a declinar expressamente as finalidades para as quais pretende utilizar os dados e, nestes termos, vincula-se aos termos desta sua manifestação pré-negocial. A utilização dos dados, seja para tratamento ou compartilhamento desviada das finalidades expressas quando da obtenção do consentimento, torna-o ineficaz e ilícita a conduta, ensejando responsabilidade, bem como todos os meios de tutela efetiva do direito do titular dos dados. Nasce tanto a pretensão de reparação dos danos causados pela utilização indevida dos dados pessoais do titular, quanto pretensão inibitória, para impedir ou fazer cessar o ilícito, sem prejuízo do exercício da polícia administrativa, que no caso das relações de consumo será exercido tanto pela Autoridade Nacional de Proteção de Dados quanto pelos integrantes do Sistema Nacional de Defesa do Consumidor, sem prejuízo da atuação do outro órgão ou entidade da Administração com competência regulatória ou de supervisão específica sobre o setor econômico a que se vincule o fornecedor.

O art. 7º da LGPD define as finalidades legítimas para o tratamento de dados pessoais.[21] Em relação aos dados pessoais sensíveis, tais finalidades são definidas, de modo mais estrito, no art. 11 da LGPD.[22] Nas relações de consumo, tem relevância o exame, sobretudo, dos incisos I, II, VI, VIII, IX e X do art. 7º da LGPD. Em relação aos dados sensíveis, ainda, além da atenção estrita às finalidades previstas no art. 11 da LGPD, o §3º do mesmo artigo permite que a quando a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores tenham por objetivo obter vantagem econômica, este poderá ser objeto de vedação ou regulamentação por parte da Autoridade Nacional de Proteção de Dados, segundo procedimento de que define.[23] Em

tais casos sempre estarão em tensão o exercício da livre-iniciativa, da privacidade e da defesa do consumidor, sendo reconhecida por lei a competência regulamentar que dever promover, em qualquer intervenção que venha a proceder, a concordância prática entre estes três direitos fundamentais assegurados pela ordem constitucional.

A primeira hipótese de finalidade legítima permitida para tratamento dos dados pela legislação, é a do consentimento do titular dos dados (art. 7º, I, da LGPD). Porém também se admite o tratamento de dados para "o cumprimento de obrigação legal ou regulatória pelo controlador" (art. 7º, II, da LGPD). Pode o fornecedor ter de utilizar os dados dos seus consumidores inclusive em seu próprio benefício, quando por exemplo, conforme certas informações se lhe ofereçam preços ou tarifas mais vantajosas segundo regras definidas pelo regulador (p.ex. tarifa dos serviços de energia elétrica de consumidores de baixa renda).

Da mesma forma, admite-se o tratamento dos dados pessoais "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados" (art. 7º, V). Trata-se de finalidade recorrente na utilização de dados do consumidor nas relações de consumo. Abrange os procedimentos necessários à execução do contrato (fase de execução) e seus procedimentos preliminares à contratação (fase pré-contratual). Há situações em que o fornecedor, para determinar as condições de uma determinada contratação necessita de dados do consumidor, seja para delimitar a prestação ou para formação do preço. É o que ocorre, por exemplo, com o consumidor que indica o endereço residencial para entrega do produto, que é tomado para cálculo do frete ou taxa de entrega; ou daquele que indica determinadas informações pessoais para registro de sua identidade junto a um determinado fornecedor de serviços (e.g., para abertura de uma conta bancária). Porém, há situações em que o conteúdo das informações serve também para formação do preço, ou ainda para a própria decisão de contratação. Um dos exemplos mais evidentes são as informações prestadas pelo consumidor ao segurador para determinação do risco segurado (declaração inicial do risco); ou ainda as informações prestadas ao operador do plano de saúde, para efeito de viabilizar a contratação. São situações que se colocam em evidência, sobretudo, em vista do risco de discriminação do consumidor, uma vez que resultem na negativa da possibilidade de contratar, ou fazendo com que se dê em condições que, na prática, em razão da sua onerosidade, impeçam, de fato, que possa arcar com a contraprestação pecuniária correspondente.

Por vezes, tratando-se de dados relativos à saúde do consumidor, vão se tratar de dados sensíveis, ou seja, aqueles "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II, da LGPD). Neste caso, incide o art. 11 da LGPD, que dispõe em termos mais estritos sobre o tratamento dos dados sensíveis em relação aos demais dados. Alteração recente na redação do § 4º deste art. 11 da LGPD, todavia, mantendo a vedação à possibilidade de comunicação do uso compartilhado relativo a dados pessoais sensíveis referentes à saúde, com objetivo de obter vantagem econômica, acrescentou a exceção originalmente prevista, que previa a possibilidade de compartilhamento em razão da "portabilidade de dados quando consentido pelo titular" (inciso I), também uma segunda hipótese, quando havia "necessidade de comunicação para a adequada prestação de serviços de saúde suplementar"(inciso II).[24] Neste caso, note-se que o compartilhamento de dados também se admite vinculado a estrita atenção à finalidade de viabilizar a adequada prestação de serviços de saúde suplementar, o que pode se dar tanto na fase pré-contratual, quanto na fase contratual, porém não podem servir para impedir a contratação dos respectivos serviços de saúde suplementar, tampouco limitar sua utilização ou frustrar sua finalidade de assegurar os meios necessários à manutenção ou reestabelecimento das condições de saúde do consumidor.

Outra finalidade admitida ao uso de dados pessoais que repercute nas relações de consumo é a que sirva para "o exercício regular de direitos em processo judicial, administrativo ou arbitral" (art. 7º, VI). Neste caso, os dados de que disponha o

fornecedor sobre o consumidor podem ser utilizados para exercício de pretensão de que seja titular, por intermédio de processo judicial, administrativo ou arbitral, ou nas mesmas condições, defesa de pretensão deduzida contra si, por consumidor ou terceiros. Trata-se de finalidade admitida em relação à utilização de dados pessoais, inclusive dos dados pessoais sensíveis (art. 11, II, "d", da LGPD). Assim, por exemplo, dentre várias outras situações, tanto poderá o fornecedor utilizar o endereço informado pelo consumidor para endereçar-lhe a citação do processo, quanto verificar sua condição de crédito em bancos de dados específicos trazendo tais informações ao processo judicial, se pertinentes; ou ainda quando requerido a informar a relação de contratantes que atendem as condições objeto de certo litígio.

Os dados pessoais podem ser objeto de tratamento, ainda, no âmbito das relações de consumo, "para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias" (art. 7º, VIII, da LGPD). A finalidade de tutela a saúde do consumidor individual, ou ainda da coletividade de consumidores justifica o tratamento de dados. Note-se que este tratamento de dados sempre se dá no interesse pressuposto da preservação e promoção da saúde do consumidor ou da coletividade, como ocorre quando há interação entre mais de um profissional da mesma ou de diferentes especialidades no tratamento de saúde do consumidor, os quais, necessariamente, precisam compartilhar informações sobre seu estado de saúde. Da mesma forma, por exemplo, se fazem necessárias, cotidianamente, informações sobre o histórico de saúde e eventuais intercorrências, para adequado tratamento da saúde do consumidor (p.ex. o resultado de exames laboratoriais que sejam informados ao profissional que os requereu ao respectivo paciente), ou para prevenir riscos (p.ex. a informação sobre certa doença contagiosa relativa a determinado paciente e que deva ser informado às autoridades sanitárias).

Admite-se o tratamento de dados ainda, "quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais" (art. 7º, IX, da LGPD). O Regulamento Geral de Proteção de Dados europeu dá o exemplo em que se aplica a figura nas situações em que o titular dos dados é cliente do responsável pelo tratamento. Assim se consideram os dados pessoais do consumidor utilizados para efeito de organização interna do próprio fornecedor ou na sua relação com parceiros negociais, assim como, com relação ao uso de dados sensíveis com a finalidade de garantir a "prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos" (art. 11, II, "g", da LGPD), hipótese em que igualmente são resguardados os direitos do titular e serão restritos nos casos em que prevaleçam "direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Neste particular, por exemplo, cada vez mais vem sendo desenvolvido para identificação pessoal do consumidor em variada sorte de serviços, o reconhecimento facial, da impressão digital, da íris, ou de outras características personalíssimas, que exigem uma estrita vinculação do uso da tecnologia e dos dados que dispõe para esta finalidade específica. O mesmo se diga em relação a meios tradicionais de identificação, como o número de registro, identidade, do cartão de crédito ou outros que permitam a identificação do consumidor. Nestes casos, a estrita vinculação à finalidade específica permitida por lei, quando não haja consentimento do consumidor (que é a primeira hipótese admitida para uso dos dados, art. 7º, I, da LGPD), é condição essencial para a preservação de sua privacidade e segurança, em especial para evitar a utilização indevida dos dados para outros fins não autorizados pelo próprio titular, e tampouco pela legislação.

A preocupação com a definição precisa do que caracteriza o legítimo interesse do controlador dos dados remonta à discussão estabelecida tanto no âmbito europeu – no contexto do Regulamento Geral de Proteção de Dados em vigor e da Diretiva 46/95/CE, que veio a revogar – quanto nas discussões que antecederam a aprovação da LGPD no Brasil.[25] Nestes termos é que o art. 10 da LGPD vai procurar definir o que se dava considerar "legítimo interesse do controlador" como fundamento do tratamento de dados

pessoais com finalidades legítimas, nos seguintes termos: "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I – apoio e promoção de atividades do controlador; e II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei."

Alguns aspectos resultam da interpretação do art. 10 da LGPD: primeiro, que o interesse legítimo do controlador no tratamento de dados não se admite em vista de critérios genéricos, senão em acordo com o exame de situações concretas; segundo, que abrange somente os dados pessoais estritamente necessários para a finalidade pretendida (art. 10, §1º); terceiro, que devem ser respeitadas, em qualquer caso, as legítimas expectativas do titular dos dados (art. 10, II), o que se deve considerar em vista tanto da informação prestada no caso de ter havido consentimento, ou ainda a proteção de sua privacidade, considerada nos termos em que acredita, de modo legítimo, resguardar certas informações sobre si do conhecimento de terceiros. Além destas situações, devem ser mencionadas as exigências de transparência do uso dos dados sob a justificativa do legítimo interesse do controlador (art. 10, § 2º), de modo a permitir, inclusive, que o titular dos dados se oponha a esta utilização, sem prejuízo da mitigação dos riscos que deve perseguir.

De grande relevância para as relações de consumo, ainda, será o tratamento dos dados pessoais com a finalidade de proteção do crédito (art. 7º, X, da LGPD). Trata-se de hipótese de tratamento de dados com maior tradição no mercado de consumo, sobre a qual dispõe legislação específica, como é o caso do art. 43 do CDC (LGL\1990\40) e, mais adiante, a Lei 12.414/2011 (LGL\2011\1883). Os dados pessoais do consumidor relativo a seu comportamento de crédito compreendem informações diversas relativas ao nível de comprometimento atual da sua renda com dívidas, eventuais situações de inadimplemento e sua duração, o histórico de pagamento, dentre outras informações relevantes. Todas estas informações são relevantes para a análise do risco de crédito e, neste contexto, da própria capacidade de endividamento do consumidor. Por sua relevância, tais informações podem implicar no impedimento de contratação pelo consumidor, ou ainda, sua submissão a certas condições, razão pela qual o tratamento das informações de crédito deve observar critérios objetivos na análise dos dados, de modo a evitar restrições excessivas ou discriminatórias.

2.1.1.3 Adequação

O atendimento ao princípio da adequação no tratamento de dados pessoais é definido pela "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (art. 6º, II, da LGPD). Neste sentido, visa preservar a vinculação necessária entre a finalidade de utilização dos dados informada ao titular e seu efetivo atendimento na realização concreta do tratamento de dados. Neste sentido, a adequação vincula-se diretamente ao consentimento dado pelo titular para o tratamento dos dados ou as demais finalidades legais admitidas que deverão ser informadas, e a situação de confiança que se cria do estrito atendimento dos termos da informação prévia ao consentimento ou do uso informado.

No caso do consentimento dado ao tratamento de dados pessoais sensíveis, anote-se que esta vinculação à finalidade é ainda mais estrita, inclusive pelos requisitos que lhe são determinados, nos termos do art. 11, I, da LGPD, a exigir, em tais situações, que ele deva ser dado "de forma específica e destacada, para finalidades específicas".

2.1.1.4 Necessidade

O princípio da necessidade, segundo a definição legal, compreende 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" (art. 6º, III, da LGPD). Uma vez que o tratamento dos dados pessoais se vincula diretamente a um direito fundamental que assegura sua proteção, assim como supõe o consentimento do titular e hipóteses de atendimento a finalidade legítima, resulta daí a limitação de seu uso ao mínimo necessário para que atenda a tais fins. Associa-se, neste caso, a noção amplamente desenvolvida pelo direito de proporcionalidade, como adequação entre meios e fins. Neste particular, o tratamento dos dados deve estender-se ao mínimo necessário para atendimento das finalidades propostas. Daí referir, a definição legal, a dados pertinentes, proporcionais e não excessivos.

Dada a crescente capacidade de processamento de volumes cada vez mais expressivos de dados, um desafio regulatório importante em relação à proteção de dados é o equilíbrio entre a pretensão de maior precisão na análise dos dados e a limitação do seu uso em face do princípio da necessidade. Em especial frente às várias possibilidades de correlações que podem ser realizadas em termos estatísticos entre dados que aparentemente não tenham uma vinculação direta entre si. A precisão do que se deva considerar o mínimo necessário para a realização das finalidades do tratamento de dados tensiona com o volume ou qualidade dos dados necessários para a melhor consecução destas finalidades.

2.1.1.5 Livre acesso

O princípio do livre acesso compreende a "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" (art. 6º, IV, da LGPD). A participação dos titulares dos dados no seu tratamento se expressa, especialmente pela exigência de consentimento e na possibilidade efetiva de que tenham conhecimento sobre a forma e extensão em que se desenvolvem. Abrange a possibilidade de obter cópia dos registros existentes, de modo, tendo a pretensão, inclusive, de corrigir informações incorretas ou imprecisas, ou conforme seu interesse, mesmo, acrescentar dados verdadeiros que possam favorecer seu interesse.

O art. 9º da LGPD concretiza o princípio assegurando o direito do titular dos dados "ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I – finalidade específica do tratamento; II – forma e duração do tratamento, observados os segredos comercial e industrial; III – identificação do controlador; IV – informações de contato do controlador; V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI – responsabilidades dos agentes que realizarão o tratamento; e VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei." O mesmo direito de acesso é consagrado no rol dos direitos do titular dos dados, enunciado no art. 18, II, da LGPD. Há, neste ponto, clara inspiração na regra do art. 15 do Regulamento Geral de Proteção de Dados europeu (Regulamento 2016/679), que dispõe, que enuncia, com pequenas variações, os direitos subjetivos previstos na LGPD brasileira.

A violação do direito de acesso aos dados, que se pode caracterizar pela simples recusa, mas, sobretudo na dinâmica atual do mercado de consumo, pela imposição de obstáculos ao acesso, exigindo que o consumidor reporte-se a diferentes pessoas ou setores distintos para acesso a estas informações, retardando-o injustificadamente[26] e deixando de facilitar o exercício do direito, configura infração aos direitos do consumidor passível de sanção, em comum, pela LGPD e pelo CDC (LGL\1990\40), sem prejuízo de eventual responsabilização por danos.

2.1.1.6 Qualidade dos dados

É assegurado pela LGPD a "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" (art. 6º, V). A rigor, é inerente a formação de banco de dados e toda e qualquer atividade de tratamento de dados pessoais que possam repercutir de qualquer modo sobre os direitos do titular das informações arquivadas a exatidão dos dados. Esta noção de exatidão abrange sua atualidade e clareza, como pretendeu bem explicitar a definição legal de qualidade dos dados, o que é especialmente importante se for considerado o caráter permanente e contínuo do tratamento de dados, seu compartilhamento e consulta pelos interessados, o que leva a que na medida em que as informações se modifiquem, pelo que é natural e ordinário no cotidiano da vida, seja identificado um ônus do controlador dos dados de mantê-los atualizados.

Há quase duas décadas Simsel Garfinkel já registrava os embaraços causados pelas estratégias de marketing baseadas em dados desatualizados, como os que desconsideravam a morte de um determinado consumidor e permanecia a expor massivamente seus familiares com publicidade direcionada à pessoa falecida.[27] Isso pode se reproduzir hoje, em situações distintas, nas redes sociais, no envio de correspondências ou outros meios de mensagens publicitárias a pessoas cuja situação pessoal tenha se alterado, ou mesmo se utilizando de critérios para direcionamento de mensagens, precificação ou análise de riscos que já não correspondem a uma situação real, mas pertença ao passado. Nestes termos, informação desatualizada é inexata, portanto, incorreta, e viola o direito do titular dos dados na exata medida em que o vincula a uma circunstância, característica ou fato que não lhe corresponde.

Refere a lei, também, a relevância dos dados. Talvez esta seja, em termos práticos, o critério de mais difícil precisão quanto à qualidade dos dados. A noção de relevância se define em acordo com a finalidade do tratamento dos dados. Neste sentido, com exceção de situações extremas, nas quais seja praticamente impossível sustentar alguma associação entre informações notoriamente irrelevantes para a finalidade determinada ao tratamento de dados, a correlação de dados em termos estatísticos não se subordina, necessariamente a uma exigência de causalidade, bastando uma demonstração estatística. Nestes termos, não é necessário que o controlador demonstre o modo específico como um determinado dado pessoal repercute em termos causais para um determinado resultado, senão que demonstre uma determinada correlação. Neste particular, registre-se que correlação é a medida da relação entre duas variáveis, que pode ser demonstrada em termos estatísticos e não implica necessariamente em uma relação de causa e efeito (p.ex. a frequência de aquisição de determinados produtos pelos consumidores se dá em determinado horário ou em determinado dia da semana), como ocorre no juízo de causalidade, no qual a relação entre duas variáveis pressupõe que uma é consequência da outra. O estágio atual do tratamento de dados aperfeiçoa a utilização de correlações, por intermédio, sobretudo, do desenvolvimento de algoritmos que permitem a obtenção de resultados precisos não apoiados necessariamente por relações de causalidade. Daí a determinação da relevância dos dados, embora também se configure como um ônus do controlador dos dados, deve ser compreendida a partir destas premissas de tratamento das respectivas informações.

Ao princípio de qualidade dos dados corresponde um direito do titular dos dados de correção dos dados incompletos, inexatos ou desatualizados (art. 18, III, da LGPD), assim como de anonimização, bloqueio e eliminação dos dados considerados desnecessários, excessivos ou tratados em desacordo com a lei (art. 18, IV, da LGPD). Anonimização significa tornar anônimo, ou simplesmente, desidentificar, tornar impossível a associação direta ou indireta entre os dados objeto de tratamento e a pessoa do seu titular. É definida no art. 5º, XI, da LGPD; bloqueio de dados, nos termos da lei (art. 5º, XIII) se caracteriza pela suspensão temporária de qualquer operação de tratamento do dado; eliminação compreende a exclusão de dado ou de conjunto de dados armazenados em banco de dados (art. 5º, XIV). Todas são hipóteses em que se visa preservar o titular dos dados, impedindo que informações em desacordo com a lei possam ser associados a ele, de modo a violar direitos fundamentais (sobretudo no caso de informações desnecessárias ou excessivas)[28], ou ainda seus legítimos interesses, inclusive, para prevenir riscos de dano (em especial no caso de dados incompletos,

inexatos ou desatualizados).

2.1.1.7 Transparência

O princípio da transparência expressa a "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" (art. 6º, VI, da LGPD). A transparência sobre o procedimento de tratamento de dados e os sujeitos envolvidos na atividade é uma marca da legislação sobre proteção de dados em diversos sistemas jurídicos. O Regulamento Geral sobre Proteção de Dados europeu define que "deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados." Prossegue afirmando que "o princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados." (n. 39 do Regulamento 2016/679).

Há, neste particular uma preocupação com o respeito à legítima expectativa do titular dos dados, mas, sobretudo, a determinação do controle do tratamento pelo titular dos dados em relação ao atendimento do compromisso assumido pelo controlador quando da obtenção dos dados.

Tem especial relevância a transparência para controle da temporalidade de tratamento dos dados, e os critérios e procedimentos que devem ser observados quando do seu término. O art. 15 da LGPD refere que o término do tratamento dos dados pessoais ocorrerá nas hipóteses de verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para esta finalidade específica pretendida, o fim do período de tratamento previsto, a comunicação da revogação do consentimento ou a determinação da autoridade nacional, no caso de violação da lei.

O término do tratamento implica, como regra, na obrigação de eliminação dos dados pessoais arquivados. A eliminação deixará de ocorrer apenas em vista das hipóteses previstas no art. 16 da LGPD, a saber: "I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

2.1.1.8 Segurança

Um dos principais objetivos da legislação de proteção de dados é assegurar um arcabouço normativo que assegure o tratamento dos dados pessoais de modo compatível aos direitos dos titulares dos dados, evitando seu tratamento sem observância das exigências legais, assim como a prevenção de riscos inerentes à atividade. Neste cenário, o princípio da segurança é definido pela "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" (art. 6º, VII, da LGPD).

Este princípio associa-se, no tocante às relações de consumo, ao dever geral de qualidade da prestação de serviço do fornecedor, que abrange também o adequado tratamento dos dados pessoais do consumidor, desdobrando-se no dever de segurança em relação a sua pessoa e patrimônio. A violação do dever de segurança, neste

particular, implica na responsabilidade objetiva do fornecedor pelos danos causados, o que será a hipótese em que os dados venham a ser acessados por pessoas ou de modo não autorizado, ou ainda situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Tais hipóteses de acesso não autorizado, acidentes ou atos ilícitos a par do regime de responsabilização previsto na própria LGPD caracterizam espécie de risco inerente à atividade de tratamento de dados, ou seja, fortuito interno, situação que não é apta a afastar a responsabilidade dos respectivos controladores de dados.

2.1.1.9 Prevenção

Reconhecida a possibilidade de o tratamento de dados gerar riscos aos direitos dos titulares dos dados, informa a atividade também o princípio da prevenção. Compreende a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (art. 6º, VIII, da LGPD). É comum às atividades associadas à tecnologia da informação e sua multifacetada e crescente utilização para uma série de finalidades, a identificação de novos riscos. Estes novos riscos tanto se apresentam em razão de situações novas criadas pela tecnologia – ou seja, que pressupõe sua existência – quanto a potencialização de riscos de dano já existentes, mas que o incremento tecnológico aumenta a possibilidade de ocorrência ou sua extensão. Fraude bancária, por exemplo, já existia antes de qualquer desenvolvimento significativo relativo ao processamento de dados pessoais; potencializa-se, contudo, as possibilidades (e, portanto, riscos) de fraude frente as situações de vazamento ou uso indevido de dados dos consumidores destes serviços.

O princípio da prevenção é comum às legislações de proteção de dados pessoais e de defesa do consumidor (art. 6º, VI, do CDC (LGL\1990\40)). O modo como se opera a prevenção de riscos de dano tanto abrangem providências materiais a serem exigidas, com o incremento técnico da atividade, quanto a possibilidade de delimitar, nos termos da lei, o tratamento de dados pessoais sensíveis, assim considerados também em razão da maior gravidade dos danos que podem decorrer de sua utilização indevida.

No caso da proteção de dados pessoais, a prevenção vincula a atividade de tratamento dos dados desde a concepção dos sistemas para coleta das informações, pautado pelo conceito de Privacy by Design, atribuído a informe de projeto comum da Autoridade de Proteção de Dados holandesa e do Comissariado de Informação de Ontário, liderado por Ann Cavoukian, que sustenta uma atuação proativa de todos os envolvidos na atividade, resultante da associação de três critérios: a) sistemas de tecnologia informação (IT systems); b) práticas negociais responsáveis (accountable business practices); e c) design físico e estrutura de rede (physical and networked infrastructure), visando predominantemente a preservação da privacidade dos usuários.[29] Em outros termos, os fornecedores devem promover a privacidade do consumidor em todas as etapas de desenvolvimento de seus produtos e serviços, envolvendo a segurança dos dados, limites razoáveis de coleta de boas práticas para conservação, descarte e precisão dos dados. Da mesma forma, devem conservar procedimentos abrangentes de gerenciamento de dados durante todo ciclo de vida de seus produtos e serviços.[30]

2.1.1.10 Não discriminação

O princípio da não discriminação tem importância destacada na proteção dos dados pessoais. Compreende, segundo definição legal, a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (art. 6º, IX, da LGPD). Afinal, a grande vantagem do processamento dos dados pessoais para maior precisão da segmentação e personalização dos consumidores no mercado de consumo não pode servir para prejudicar, restringir ou excluir qualquer consumidor da possibilidade de acesso ao consumo.

Coíbe-se segundo a LGPD, que o tratamento seja realizado para fins discriminatórios ou abusivos. A própria disciplina do tratamento dos dados sensíveis (art. 11 da LGPD) em

separado dos demais dados pessoais justifica-se pelo risco maior que dele resulte discriminação. Contudo, interpretação constitucionalmente adequada da norma deve compreender a proibição não apenas da finalidade discriminatória ou abusiva, mas também quando o resultado do tratamento de dados possa dar causa à discriminação. A proibição da discriminação injusta não se limita apenas ao comportamento que se dirige a discriminar, senão também em qualquer situação na qual ela é resultado de uma determinada conduta.

A proibição da discriminação injusta tem protagonismo no tratamento de dados pessoais. Afinal, a utilidade essencial do tratamento de dados é justamente segmentar, personalizar, especializar dados pessoais; portanto discriminar, assim entendida a noção como separação, diferenciação. É preciso atentar aos exatos termos da proibição presente na lei, que compreende a proibição à discriminação ilícita ou abusiva. Ilícita será a discriminação baseada em critérios que a lei proíbe a utilização para fins de diferenciação. Neste caso, é a Constituição da República quem proíbe preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (art. 3º, IV). Da mesma forma, estabelece que "ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política" (art. 5º, VIII). Além destes critérios, pode haver discriminação ilícita ou abusiva em razão de critérios que não estejam em acordo com a finalidade para a qual se realize determinada diferenciação. Assim, por exemplo, a recusa de fornecimento de produto ou serviço a quaisquer pessoas em razão de sua orientação sexual.[31] No tocante ao tratamento de dados pessoais, a própria definição legal de dado sensível compreende uma série de critérios cuja utilização, para fins de discriminação, deve ser considerada proibida (o art. 5º, II, da LGPD, relaciona os dados relativos a "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").

O exercício da liberdade individual é delimitado pela proibição à discriminação injusta. O que não significa a impossibilidade absoluta de serem feitas diferenciações ou separações, de acordo com critérios idôneos e legítimos à luz da Constituição da República e da legislação. No tocante ao tratamento de dados, a diferenciação e segmentação constitui, inclusive, uma das utilidades mais perceptíveis. Neste sentido, não basta que o critério de diferenciação seja aferido objetivamente ou que não restrinja o acesso de qualquer dos titulares de dados a quaisquer bens ou serviços em questão. Recorde-se, aqui, da doutrina norte-americana, por longo tempo admitida pela Suprema Corte daquele país, do "separate but equal", que justificava a discriminação racial pelo fato de assegurar, em tese, o acesso aos mesmos serviços a pessoas brancas e negras, porém de modo que cada grupo os utilize separadamente.[32]

No âmbito do mercado de consumo, a proibição à discriminação injusta tem efeito na rejeição de diferenciação entre consumidores em razão de critérios inidôneos ou ilegítimos que tenham por resultado a recusa do fornecimento de produto ou serviço ou a imposição de condições diferenciadas, em violação ao princípio da igualdade. Em relação ao tratamento de dados pessoais, é exemplo a diferenciação em banco de dados por raça dos consumidores (racial profiling), de modo a oferecer vantagens para contratação a um determinado grupo.[33] A rigor, o problema da discriminação se estabelece, sobretudo, nas situações em que a distinção por critérios proibidos se dá para impor diferenciação desvantajosa para um determinado grupo, que tanto pode ser uma condição mais onerosa do que a dos demais que não pertencem àquele grupo, quanto restrições de acesso ou de realização de determinados interesses legítimos, infirmando uma desigualdade de tratamento. Caracteriza tratamento discriminatório, igualmente, não apenas aquele baseado em características pessoais, mas também em relação a fatos cuja adoção como critério de diferenciação se afigure inidôneo ou ilegítimo, como é o caso em que o titular dos dados possa ser prejudicado de algum modo em razão de informação que indique o exercício regular de seu direito. Estabelece o art. 21 da LGPD: "Os dados pessoais referentes ao exercício regular de direitos pelo

titular não podem ser utilizados em seu prejuízo."

Em algumas situações não basta o exame em relação ao critério utilizado para diferenciação ou, isoladamente, a finalidade da diferenciação realizada mediante o tratamento de dados. A idoneidade e legitimidade do critério deve ser justificável a partir de uma determinada contextualização. Assim, por exemplo, a utilização do dado relativo ao endereço residencial do consumidor como critério de formação do preço pelo fornecedor. Se o caso envolver o valor do prêmio a ser pago por um determinado segurado em um contrato de seguro de automóvel, o risco que se identifique em razão das estatísticas de furto ou roubo de veículos na região em que se localiza o endereço, a princípio pode configurar critério idôneo para uma majoração do valor a ser pago por este, em relação a segurados que residam em lugares com menor ocorrência destes crimes. Se o mesmo dado, todavia, for utilizado, sem quaisquer outros elementos, para a cobrança de juros mais altos em empréstimos bancários, ou ainda para negar a contratação, a idoneidade e legitimidade do critério será questionável, e o tratamento do dado em questão, considerado discriminatório.

Dentre os instrumentos previstos na LGPD para impedir o tratamento de dados discriminatório está a previsão do direito do titular dos dados de revisão das decisões "tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade" (art. 20). Da mesma forma, tome-se em conta que o tratamento de dados ao operar com correlações entre diferentes dados, pode dificultar a identificação do critério que determine situação discriminatória do consumidor. Razão pela qual a lei prevê, ao lado do dever do controlador de fornecer, quando solicitadas, as informações sobre critérios e procedimentos utilizados para a decisão automatizada a possibilidade de, no caso de recusa, ser realizada auditoria para verificação dos aspectos discriminatórios no tratamento dos dados (art. 20, §§ 1º e 2º).

Da mesma forma, a possibilidade de anonimização dos dados, ou seja, a adoção de meio técnico pelo qual um dado perde a possibilidade de associação, direta ou indireta, a um determinado indivíduo, impedindo eventual discriminação. A anonimização, todavia, é técnica que pode não ser utilizada com maior frequência em relação aos dados de consumidores, quando a finalidade seja, justamente, a segmentação de mercado.

2.1.1.11 Responsabilização e prestação de contas

O princípio da responsabilização e prestação de contas compreende a exigência de "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" (art. 6º, X, da LGPD). Relaciona-se diretamente com o princípio da transparência e da prevenção, impelindo aqueles que se ocupam do tratamento de dados pessoais não apenas de observar o cumprimento das normas jurídicas aplicáveis, mas terem a capacidade de demonstrar esta conformidade legal e sua eficácia. A enunciação do princípio se inspira no Regulamento europeu, no qual consta ainda a explicitação do conteúdo do comportamento exigido na demonstração de atendimento às normas, ao referir que "essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados" (n. 74 do Regulamento 2016/679). Esta obrigação compreende inclusive a adoção de programas de conformidade (n. 78 do Regulamento 2016/679), bem como um detalhado procedimento de avaliação de impacto sobre proteção de dados (art. 35 do Regulamento 2016/679).

A LGPD brasileira previu a obrigação dos agentes de tratamento de dados (controladores e operadores), de adotarem boas práticas e de governança, inclusive com a adoção de programa de governança que atenda a requisitos mínimos definidos na legislação, sujeito a avaliação sobre sua efetividade (art. 50).[34]

2.1.2. A disciplina especial dos bancos de dados de proteção ao crédito

Os bancos de dados de proteção ao crédito resultam das primeiras iniciativas de tratamento de dados dos consumidores no mercado de consumo. Em um primeiro estágio visavam, exclusivamente, arquivar informações sobre situações de inadimplemento do consumidor, cuja consulta pelos fornecedores implicavam na restrição a contratação de crédito, daí porque conhecidos como bancos de dados restritivos de crédito. Sobre eles dispõe, prioritariamente, o art. 43 do CDC (LGL\1990\40).

Já como resultado da melhor capacidade de tratamento de dados, desenvolvem-se, em um segundo momento, bancos de dados não apenas das situações de inadimplemento, mas de forma mais ampla, de informações do histórico de crédito do consumidor, sobre frequência, volume das obrigações assumidas e pontualidade do pagamento. Com o objeto de aperfeiçoar a avaliação do risco de crédito, justifica-se pelo benefício a "bons pagadores" com melhores condições de contratação. Por isso são denominados "bancos de dados de informações positivas" ou, mais impropriamente, "cadastros positivos". Admitirão tratamento diversificados dos dados, inclusive mediante organização de sistema de atribuição de pontuação ou notas aos consumidores, sinalizando o risco maior ou menor de inadimplemento. Sua disciplina legal é conferida pela Lei 12.414/2011 (LGL\2011\1883), substancialmente alterada pela Lei Complementar 166/2019 (LGL\2019\2578).

A LGPD incide sobre o tratamento de dados com a finalidade de proteção ao crédito, devendo sua aplicação articular-se com outras fontes normativas.[35] Afinal, preserva expressamente a legislação especial, conforme prevê seu art. 7º, X, ao referir que poderá ser realizado "para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente." Nestes termos, a LGPD não derroga ou revoga o art. 43 do CDC (LGL\1990\40) ou a Lei 12.414/2011 (LGL\2011\1883), devendo suas disposições serem compatibilizadas às normas gerais de proteção de dados que estabelece. Neste particular, especial atenção deve-se dirigir ao art. 64 da LGPD, ao definir que os direitos e princípios que expressa não excluem outros previstos no ordenamento jurídico brasileiro – caso do CDC (LGL\1990\40), que dispõe de regra semelhante em seu art. 7º, e da legislação que disciplina o "cadastro positivo".

2.2 A Autoridade Nacional de Proteção de Dados e o Sistema Nacional de Defesa do Consumidor

A supervisão e fiscalização do cumprimento da legislação de proteção de dados pessoais, assim como a implementação das políticas públicas que a promovam, em diversos sistemas jurídicos serão confiados a órgão ou entidade criado especificamente para este fim. No direito brasileiro, todavia, a previsão inicial de criação da Autoridade Nacional de Proteção de Dados foi originalmente objeto de veto presidencial quando da edição da lei, seguido, contudo, de sua criação por intermédio de Medida Provisória submetida a deliberação do Congresso Nacional.

O art. 55-J da LGPD define as competências da Autoridade Nacional de Proteção de Dados,[36] várias delas com repercussão direta para a proteção do consumidor titular de dados, como ocorre com a definição de sua competência regulamentar (inciso II), de fiscalização (incisos IV a VI), por exemplo.

Merece destaque, contudo, a definição que o exercício de sua competência regulamentar deverá observar a consulta prévia a outros órgãos ou entidades da Administração que sejam responsáveis pela regulação de setores específicos da atividade econômica (art. 55-J, XIV, da LGPD), inclusive com o dever de articular e coordenar sua atuação (art. 55-J, XV e § 2º, da LGPD). Estão inseridas nesta hipótese as agências reguladoras, muitas das quais, regulando serviços oferecidos no mercado de consumo, vinculam-se a competência de defesa do consumidor.

Em relação ao Sistema Nacional de Defesa do Consumidor, o art. 55-K, parágrafo único, da LGPD, dispõe: "A ANPD articulará sua atuação com outros órgãos e entidades com

competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação."

Neste ponto, convém referir que o caput do art. 55-K reserva à Autoridade Nacional de Proteção de Dados, com exclusividade, a aplicação das sanções previstas na LGPD, assim como a prevalência de suas competências relativas à proteção de dados pessoais, em relação às competências correlatas de outras entidades ou órgãos da Administração Pública. Registre-se que a redação original da Medida Provisória que criou a ANPD continha referência expressa à articulação entre ela e os órgãos integrantes do Sistema Nacional de Defesa do Consumidor. No texto legislativo que resultou aprovado no Congresso Nacional, esta previsão foi substituída pela referência genérica a "outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais" acentuando a prevalência da competência da ANPD em relação a eles. Deste modo, a questão que se apresenta é: qual a competência dos órgãos e entidades de defesa do consumidor integrantes do Sistema Nacional de Defesa do Consumidor em matéria de proteção de dados pessoais?

A exegese do art. 55-K conduz, inicialmente, a duas conclusões: a) primeiro, sendo a Autoridade Nacional de Proteção de Dados órgão central de interpretação da LGPD e com competência para sua regulamentação, quando defina certo entendimento quanto ao sentido e alcance da lei, ou edite regulamento que discipline sua aplicação, tais atos prevalecem e vinculam os órgãos e entidades integrantes do Sistema Nacional de Defesa do Consumidor; b) segundo, em relação à competência de fiscalização prevista no CDC (LGL\1990\40) aos órgãos e entidades integrantes do Sistema Nacional de Defesa do Consumidor, bem como aquelas que tenham sido fixadas nas leis específicas de sua criação, não são derrogadas pela LGPD. Contudo, em um eventual conflito de competências prevalecem as da ANPD.

Ao contrário, a LGPD prevê que a Autoridade Nacional de Proteção de Dados articulará sua atuação com os órgãos "com competências sancionatórias e normativas". Deste modo, são preservadas estas competências de fiscalização (sancionatórias) e regulamentares, relativamente às normas previstas no CDC (LGL\1990\40). Não sugere a lei, qualquer prevalência quanto ao exercício da competência sancionatória, razão pela qual, a exemplo do que já ocorre na fiscalização de fornecedores regulados por órgãos ou entidades setoriais, a lesão a direitos do consumidor decorrentes da violação da privacidade ou utilização indevida de dados pessoais poderá também ser objeto de atuação dos órgãos e entidades de defesa do consumidor, quando tenham por fundamento a infração a normas do CDC (LGL\1990\40) ou de sua regulamentação. Apenas quando se trate da violação de deveres previstos expressamente na LGPD, e que não se reflitam na violação de alguma norma específica da legislação de proteção do consumidor, é que a Autoridade Nacional de Proteção de Dados exercerá sua competência exclusiva. Não será por outra razão, inclusive, que o art. 18, § 8º, da LGPD prevê que o direito de petição do titular dos dados contra o controlador em razão da violação de qualquer dos direitos previstos na lei pode ser dirigido também aos "organismos de defesa do consumidor".

Porém, mesmo nos casos de competência exclusiva da Autoridade Nacional de Proteção de Dados, sua atuação deverá também considerar a aplicação das normas de proteção do consumidor. É o que resulta da interpretação dos arts. 2º, inciso VI, e 64 da LGPD.

3 Os direitos do consumidor e o tratamento de dados pessoais

3.1 Exigência de prévio e expresso consentimento

A formação de bancos de dados de consumidores, pela incidência em comum da LGPD e do CDC (LGL\1990\40) – excluídos os bancos de dados de crédito cuja disciplina especial do art. 43 do CDC (LGL\1990\40) e da Lei 12.414/2011 (LGL\2011\1883) tem precedência – submete-se, necessariamente, à exigência de consentimento expresso do

consumidor titular dos dados pessoais. Ordinariamente, relacionam-se como condições para o consentimento que ele tenha sido emitido por vontade livre do titular dos dados, voltado a uma finalidade específica e que tenha sido informado sobre esta finalidade, o processamento e utilização dos dados, bem como da possibilidade de não consentir.[37] O art. 5º, XII, da LGPD, em clara influência do Regulamento Geral europeu sobre proteção de dados, define o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

A rigor, seu significado se identifica com os requisitos que se exigem para a manifestação de vontade do consumidor capaz de vincular-lhe juridicamente. Sabe-se que nos negócios jurídicos de consumo, o silêncio não caracteriza anuência, tampouco convalida o abuso ou a ilicitude. A aceitação do consumidor sempre deve ser expressa, ainda que se possa interpretar, naquilo que não se lhe seja oneroso ou determine prejuízo, o consentimento tácito, segundo os usos. No caso do consentimento, para o tratamento de dados (art. 7º, I, da LGPD) observam-se requisitos substanciais e formais.

3.1.1 Requisitos substanciais e formais do consentimento

São requisitos substanciais os que digam respeito à qualidade do consentimento. Conhecimento e compreensão por aquele de quem se requer o consentimento são elementos essenciais para sua configuração.[38] Daí o sentido de que se trate de uma manifestação de vontade livre – significa dizer, isenta de pressões ou ameaças diretas ou indiretas que contaminem a decisão do consumidor. Neste particular, o art. 8º, § 3º da LGPD, inclusive faz referência expressa aos vícios do consentimento, o que remete, no direito atual, aos defeitos do negócio jurídico previstos no Código Civil (LGL\2002\400) (em especial, o erro, o dolo, a coação, a lesão e o estado de perigo, art. 138 e ss). Da mesma forma, deve-se recordar da violação da qualidade de consentimento que informa a abusividade das cláusulas contratuais, quando a aceitação do consumidor é colhida sem conhecimento efetivo do conteúdo da sua deliberação e/ou de suas repercussões concretas – como ocorre na hipótese do art. 46 do CDC (LGL\1990\40).

Exige-se também que seja uma manifestação de vontade informada. O consentimento informado é tema cujo significado, no direito brasileiro, já possui boa densidade, em especial no tocante aos deveres pré-negociais de profissionais liberais que assuma obrigações de meio (tais como médicos ou advogados), assim como, em geral no âmbito dos serviços de saúde, como expressão da autodeterminação do paciente. Nas relações de consumo, e informado pela boa-fé, a noção de consentimento informado firma-se em termos amplos não apenas com o reconhecimento de um dever de repassar informações àquele que deve manifestar seu consentimento, mas um autêntico dever de esclarecimento (esclarecer = tornar claro), de modo a reconhecer o dever daquele a quem compete informar, de tornar estas informações compreensíveis para o destinatário. Neste caso, só é reconhecido como eficaz o consentimento quando aquele que manifesta vontade teve as condições plenas de compreender o conteúdo da sua decisão e de que modo ela repercute em relação aos seus interesses pressupostos. Consentimento daquele que decide a partir de informações incorretas ou incompletas não é reconhecido como tal, de modo a tornar ilícita, no âmbito do tratamento dos dados pessoais, quaisquer operações que venham a se basear nele.

Da mesma forma há exigência legal expressa de que a manifestação de consentimento deve se dar em vista de finalidades determinadas para a utilização dos dados, sendo nulas as manifestações que se caracterizem como autorizações genéricas para o tratamento de dados (art. 8º, § 4º, da LGPD). Deste modo é correto entender que a declaração de vontade do titular dos dados vincula-se expressamente a certas e determinadas finalidades. Há evidente controle sobre o conteúdo da manifestação da vontade, inclusive quanto a seus termos específicos, de modo que não poderão ser redigidos de modo exemplificativo, senão que a manifestação de vontade exaure as

hipóteses de uso admitidas.

Por fim, a lei define que a manifestação deve ser inequívoca. Assume o sentido de que o consentimento, quando expresso pelo consumidor, deve ser compreendido por ele como tal. Visa-se impedir a manipulação da vontade daquele do titular dos dados.[39] Ou seja, a realização do consentimento deve ser perceptível pelo consumidor, após ser informado sobre sua repercussão, circunstância que terá especial relevância quando venha a ser manifestado por meio eletrônico, exigindo-se nesta circunstância que a forma ou o momento de realização do consentimento (p.ex., mediante um clique, a digitação de uma senha, ou a indicação do desenho, imagem ou letras que constem na tela) seja devidamente identificada como tal. Neste sentido percebe-se a regra do art. 9º, § 1º da LGPD, que comina de nulidade o consentimento obtido mediante fornecimento de informações de conteúdo enganoso ou abusivo, que devem ser compreendidas como aquelas que faltam ao dever de veracidade ou clareza, assim como possam induzir em erro o titular dos dados.

A exigência de que o consentimento seja inequívoco associa-se a requisitos formais definidos pela lei. O art. 8º, caput, da LGPD, estabelece que o consentimento "deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular." A exigência de consentimento escrito ou por outro meio que demonstre a manifestação da vontade do titular revela o propósito de assegurar a certeza sobre a existência do consentimento e seu objeto. E no caso de o consentimento ser fornecido por escrito, o §1º do art. 8º, da LGPD define, ainda, que deverá constar em cláusula destacada "das demais cláusulas contratuais". Lendo de outro modo: integrando um determinado instrumento contratual, a cláusula que preveja o consentimento do titular deve constar em destaque em relação às demais, justamente para permitir ser identificado como tal por aquele que venha a consentir.

No caso em que o consentimento refira-se ao tratamento de dados sensíveis, assim entendidos aqueles "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5.º , II, da LGPD), incide regra que delimita de forma mais estrita a manifestação de vontade do titular dos dados (art. 11, I, da LGPD). Dispõe que será admitido o tratamento de dados sensíveis "quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas". Ao contrário do consentimento em relação aos demais dados pessoais, quanto aos dados sensíveis – por sua óbvia repercussão em vista dos riscos de agravamento e extensão dos dados ao titular dos dados – exige, a lei, que a manifestação de vontade seja dada "de forma específica e destacada, para finalidades específicas". A exigência de forma específica e destacada implica no exame do contexto da manifestação de vontade. Se em texto escrito, o destaque se faz de modo que a manifestação de vontade se possa distinguir facilmente do restante das cláusulas e condições presentes. Pode ser apartada ou não do texto ou do instrumento principal, recordando-se que o ônus da prova de atendimento deste requisito será daquele que colher o consentimento, e em última análise, do controlador dos dados. É consentimento específico, para finalidades específicas, o que indica que a manifestação de vontade em consentir com o tratamento dos dados pelo titular deve se dar direta e objetivamente vinculado a certas finalidades expressas, sendo a interpretação neste caso, restritiva.

3.1.2 Ônus da prova da regularidade do consentimento

O ônus de demonstrar a correta obtenção e manifestação do consentimento nos termos da lei é atribuído expressamente ao controlador dos dados (art. 8º, §2º, da LGPD). Controlador é aquele a quem compete a decisão relativa ao tratamento de dados pessoais. No caso da relação de consumo, pode ser que o próprio fornecedor tenha este poder, porque coletou os dados para ele próprio incrementar suas decisões negociais, ou pode ser gestor do banco de dados ao decidir formatar determinadas informações que diretamente coletou ou recebeu por intermédio de compartilhamento. O elemento

nuclear da definição de controlador, nestes termos será aquele que tenha poder de decisão sobre os dados, e cuja atuação, desta forma, repercuta sobre o interesse dos respectivos titulares, em especial nos casos em que se verifique a violação de seus direitos.

A atribuição do ônus da prova da regularidade aos controladores de dados, neste sentido, termina por lhes impor a necessidade de organizar meios de obtenção e arquivamento dos respectivos consentimentos dos titulares, sejam eles dados por escrito ou por outros meios previstos na lei. Atribuído o ônus da prova nos termos da lei, se o controlador não demonstrar que obteve o consentimento do titular dos dados, presume-se a utilização indevida dos dados, submetendo-se às sanções previstas na LGPD.

3.2 Direitos subjetivos do titular dos dados

A eficácia da proteção dos interesses do titular dos dados, segundo a técnica legislativa adotada pela LGPD implica reconhecer e assegurar os direitos fundamentais de liberdade, de intimidade e de privacidade, de acordo com a estrutura normativa definida pela lei (art. 17). Nos mesmos termos, define uma série de direitos subjetivos específicos do titular de dados, em relação aos quais corresponde ao controlador uma situação jurídica passiva, do dever de realizar seu conteúdo.

3.2.1 Confirmação da existência de tratamento

O titular dos dados tem o direito à confirmação da existência de tratamento de seus dados pessoais. Observe-se que o tratamento de dados pode se dar mediante consentimento do titular dos dados, hipótese na qual, como regra, não há razão para que o confirme aquilo em relação ao que anuiu. Porém, se admite o tratamento de dados em outras diferentes situações previstas na lei (art. 7º, II a X, da LGPD), na qual poderá não existir o consentimento prévio do titular. Da mesma forma, em relação aos dados "tornados manifestamente públicos" pelo titular, é dispensado o consentimento, o que não afasta seu direito de ter ciência sobre a existência do tratamento. Ou ainda, é o que ocorre em relação aos dados pessoais sensíveis nos quais se dispensa o consentimento nos casos em que o tratamento se dirige ao cumprimento de obrigação legal ou regulatória pelo controlador, ou de modo compartilhado, quando necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (art. 11, § 2º, da LGPD).

O direito de confirmação do tratamento é exercido perante o controlador mediante requerimento do titular dos dados (art. 19 da LGPD), que poderá requerê-lo em formato simplificado ou mediante declaração clara e completa na qual indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial. No caso de ser requerido em formato simplificado, o que é próprio daquele que pretenda apenas confirmar a existência ou não do tratamento, a resposta do controlador deve ser imediata, o que permite inclusive, a utilização de meios de comunicação instantânea. Requerendo, o titular dos dados, declaração mais completa, a lei define que deverá indicar a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, hipótese em que deverá ser fornecida pelo controlador no prazo de até 15 dias. A lei prevê a possibilidade deste prazo ser alterado, por regulamento, para setores específicos (art. 19, § 4º). O atendimento do requerimento do titular dos dados poderá se dar por meio eletrônico ou sob a forma impressa (art. 19, § 2º, da LGPD).

3.2.2 Acesso aos dados

O direito subjetivo do titular de acesso a dados relaciona-se ao princípio do livre acesso, e compreende a possibilidade reconhecida de consulta facilitada e gratuita sobre os dados a seu respeito de que dispõe o controlador, assim como a forma do tratamento

dos dados. No âmbito das relações de consumo, o acesso aos dados relaciona-se ao direito à informação do consumidor, que deve ser assegurado não apenas com atenção aos produtos e serviços específicos objeto de contrato de consumo, senão no tocante a todos aspectos de seu relacionamento com o fornecedor direto e demais integrantes da cadeia de fornecimento. Este sentido já transparecia desde a edição do CDC (LGL\1990\40) em relação aos bancos de dados de que trata seu art. 43 e o dever de notificação e acesso aos dados arquivados.

Segundo a disciplina estabelecida pela LGPD, o dever do controlador de assegurar o direito do titular de acesso aos dados é amplo. Compreende as diferentes fases, desde a coleta dos dados e do consentimento, durante o período em que se der o tratamento, e inclusive após seu encerramento. O art. 9º da LGPD define em caráter exemplificativo – que poderão ser estendidas por intermédio de regulamento à lei – das informações sobre o tratamento que devem ser prestadas ao titular dos dados, tais como: a finalidade específica do tratamento; sua forma e duração; a identidade do controlador e suas informações de contato; as informações sobre o uso compartilhado dos dados e sua finalidade; a responsabilidade dos agentes que vão realizá-lo; e os direitos assegurados aos titulares dos dados. Embora a norma não seja explícita a respeito, deve-se entender que tais informações, quando se trate de tratamento que se submeta a consentimento prévio, deverão ser prestadas antes da manifestação de vontade do titular dos dados. É conclusão a que se chega tanto em termos lógicos – uma vez que são informações necessária à própria viabilidade do exercício do direito de acesso em muitos casos, quanto pela interpretação do § 1º do mesmo art. 9º da LGPD, o qual refere que "na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca." As informações em questão, a toda evidência, são aquelas do caput do mesmo artigo.

Porém, nada impede que nas demais hipóteses em que se admite o tratamento de dados independentemente do consentimento do seu titular, ou porque a lei autoriza com fundamento em outras situações, ou porque expressamente dispensa, a garantia do direito de acesso se mantém. Neste caso, tanto em relação às informações a que se refere o art. 9º, quanto, propriamente, do conteúdo dos dados pessoais que estão sendo objeto de tratamento.

Há hipóteses em que o acesso a dados será objeto de regulamentação, caso daqueles que sirvam a estudos de saúde pública (art. 13, § 3º, da LGPD).

As mesmas regras sobre o requerimento do titular dos dados no exercício do direito de confirmação do tratamento se aplicam para o caso de pretender o acesso aos dados (nos termos do art. 19 da LGPD). Assim, pode o titular dos dados requerer o acesso de modo simplificado, a ser prestada imediatamente, ou declaração completa por parte do controlador (contendo a origem dos dados, os critérios utilizados e a finalidade do tratamento, dentre outras informações), hipótese em que fica submetida ao prazo de até 15 dias para atendimento do requerimento, que a lei prevê poder ser alterado, em regulamento, para setores específicos.

Também coincide a forma de atendimento do requerimento do titular dos dados, que poderá ser por meio eletrônico, seguro e idôneo para esse fim, ou de modo impresso. Tendo o tratamento sido objeto de consentimento específico ou tendo sido previsto em contrato, poderá o titular dos dados solicitar que a resposta do controlador compreenda cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, "em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento." (art. 19, §3º, da LGPD). O modo de atendimento a esta solicitação do titular dos dados poderá ser detalhado em regulamento da lei.

3.2.3 Correção dos dados

A proteção de dados pessoais como direito da personalidade e direito fundamental

pressupõe a autodeterminação do titular dos dados sobre sua utilização, ou o tratamento destes dados de acordo com finalidades legítimas previstas em lei. Esta dimensão pressupõe a legitimidade do acesso aos dados do titular mediante seu consentimento ou, como já foi mencionado, para finalidades previstas em lei. Outra dimensão, contudo, diz respeito ao risco que o próprio tratamento de dados implica, de que informações incorretas sejam associadas a uma determinada pessoa, causando-lhe prejuízo.

Daí o direito do titular dos dados à correção dos dados objeto de tratamento. Trata-se de direito que já era consagrado no art. 43 do CDC (LGL\1990\40) e também na Lei 12.414/2011 (LGL\2011\1883), sobre o "cadastro positivo". Revela-se pela posição ativa do titular de exigir a retificação dos dados incorretamente arquivados perante o controlador. O art. 18, III, da LGPD, estabelece o direito do titular à correção de dados incompletos, inexatos ou desatualizados. O direito subjetivo à correção dos dados abrange, portanto, a pretensão do titular de exigir que sejam completos, exatos e atualizados. Isso é especialmente relevante quando em razão destes dados possam ser definidas certas condições para contratação, acesso ao crédito ou a determinadas ofertas e vantagens ao consumidor. A incorreção dos dados pode dar causa a inconvenientes (recorde-se a possibilidade de ser importunado por ligações telefônicas ou mensagens dirigidas a outras pessoas por um equívoco de registro do número de telefone), ou consequências mais graves (e.g. dados incorretos sobre a saúde do titular arquivados por um hospital ou outro prestador de serviços de saúde).

O direito à correção dos dados é exercido mediante requerimento ao controlador ou ao operador dos dados. No caso de compartilhamento dos dados, aquele que recebe o requerimento do titular deve comunicar imediatamente a todos com quem tenha compartilhado os dados, para que adotem o mesmo procedimento de correção (art. 18, § 6º, da LGPD).No âmbito das relações de consumo, todos se equiparam a fornecedor para efeito de exigência do dever ou a responsabilidade por sua violação.

3.2.4 Anonimização

O direito à anonimização dos dados é um dos principais recursos destinados a preservar a privacidade do titular dos dados (art. 18, IV). Anonimização implica tornar anônimo, impedindo a associação entre o titular dos dados e as informações objeto de tratamento. Segundo a definição legal, compreende a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". A anonimização compreende uma alteração da disposição inicial dos dados, de modo a não permitir a identificação do titular, de modo que compreende mais o resultado do que o caminho para alcançá-lo, ainda que a rigor, o anonimato absoluto no mundo digital, hoje, seja uma ilusão.[40] Afinal, há sempre elementos passíveis de identificação, como o endereço de IP do computador, dados em um telefone celular, de cartões de crédito, chips RFID,[41] ou outros que permitam uma associação a determinada pessoa e fornece um perfil detalhado do seu comportamento a partir do uso de determinado meio de comunicação ou em relação a determinados dados.

A preservação da privacidade, por intermédio da anonimização é providência exigida, sobretudo, no tratamento de dados para fins de pesquisa (arts. 7º, IV, e 13, da LGPD). Da mesma forma, pode o controlador manter os dados após o término do tratamento dos dados, desde que anonimizados, e apenas para consulta própria (art. 16, IV, da LGPD). Com a anonimização dos dados estes deixam de ser considerados dados pessoais, salvo quando o processo puder ser revertido (art. 12 da LGPD). No âmbito das relações de consumo, pesquisas de mercado ou indicadores de sinistralidade nos seguros são exemplos de dados que, anonimizados, podem ser conservados pelos controladores para sua utilização, independentemente do término do tratamento.

3.2.5 Portabilidade

É assegurado ao titular dos dados sua portabilidade a outro fornecedor de serviço ou

produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador (art. 18, V, do LGPD). Este direito não abrange os dados que já foram anonimizados pelo controlador (art. 18, § 7º, da LGPD). A portabilidade dos dados se dá, sobretudo, no âmbito das relações de consumo, visando assegurar concretamente a liberdade de escolha do consumidor no mercado, especialmente em relação à contratos de duração, nos quais, para promover a concorrência, admite-se ou regulamenta-se a possibilidade de "portabilidade" do contrato. Conforme já considerava a boa doutrina nacional, mesmo antes da edição da LGPD, a imbricação da proteção de dados com o direito do consumidor e, sobretudo, da concorrência na regulação do mercado, a recusa da portabilidade dos dados, além de violar o direito do titular, pode se caracterizar como infração à ordem econômica.[42]

Neste caso "portabilidade" do contrato que a rigor é direito a celebrar com um segundo fornecedor contrato de prestação de serviços que suceda contrato original. É o que ocorre atualmente, por exemplo, na denominada "portabilidade" de dívidas, ou no âmbito dos serviços de telecomunicações ("portabilidade" do número de telefone pelo consumidor). Também pode abranger dados relativos à saúde do titular dos dados, desde haja seu consentimento (art. 11, § 4º, I, da LGPD), hipótese que pode abranger tanto seguros quanto contratos de assistência à saúde, por exemplo. O direito à portabilidade permite que o consumidor tenha a liberdade de celebrar novo contrato levando consigo as informações relevantes do contrato anterior, de modo a evitar solução de continuidade, ou viabilizar a prestação de serviços de acordo com a sua necessidade.

Por outro lado, com o objetivo de assegurar a efetividade deste direito, o art. 40 da LGPD confere à Autoridade Nacional de Proteção de Dados competência para dispor sobre padrões de interoperabilidade para, dentre outros fins, promover a portabilidade. Neste particular, a portabilidade dos dados pessoais não abrange, a priori, a dos dados que resultem do tratamento em decorrência da técnica ou dos critérios adotados pelo controlador, que poderá ser requerido para os elimine nos casos previstos na lei.

De modo a viabilizar a portabilidade dos dados é conferida à Autoridade Nacional de Proteção de Dados competência regulamentar para definir padrões de interoperabilidade entre sistemas (art. 40 da LGPD).

3.2.6 Eliminação dos dados

A autodeterminação que informa a disciplina da proteção dos dados pessoais também abrange a possibilidade de eliminação dos dados objeto de tratamento. A eliminação dos dados é consequência lógica da possibilidade de revogação do consentimento para tratamento.

Neste particular, refira-se que o término do tratamento dos dados implica a exigência de sua eliminação, nos termos do art. 16 da LGPD. Esta mesma norma, todavia, refere ser autorizada a conservação dos dados para as finalidades de "I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

Este direito à eliminação dos dados contrapõe-se à possibilidade de manutenção dos dados em arquivo, porém interditando sua utilização. Admitir-se a manutenção dos dados sem a possibilidade de utilização é solução que aumenta os riscos de uso indevido ou vazamento. Daí porque se justifica a manutenção apenas segundo as finalidades previstas na lei (art. 16, I a IV, da LGPD), ou com os cuidados que preceitua (em especial, a anonimização). Registre-se, ainda, o dever do controlador de comunicar imediatamente àqueles com quem tenha compartilhado os dados, para que adotem o mesmo procedimento de eliminação (art. 18, § 6º, da LGPD).

3.2.7 Informação sobre compartilhamento

O titular dos dados tem direito de requerer do controlador informação de quais entidades públicas ou privadas realizou o uso compartilhado dos dados (art. 18, VII, da LGPD). As informações sobre o compartilhamento dos dados justificam-se para que o titular tenha conhecimento sobre qual o uso e que pessoas tiveram acesso aos dados.

Recorde-se, contudo, que o compartilhamento de dados pessoais pelo controlador (independentemente de ser pessoa jurídica de direito público ou de direito privado) supõe o consentimento do titular, exceto nas hipóteses em que a lei o dispensa. São os casos do uso para execução de políticas públicas (art. 7º, III e 11, II, "b", da LGPD), por exemplo. Da mesma forma, observam-se as restrições de compartilhamento de dados pelo Poder Público (art. 26 da LGPD).

3.2.8 Revogação do consentimento

O direito à revogação do consentimento é inerente à autodeterminação do titular dos dados. Pode consentir com o tratamento e alterar sua decisão, revogando o consentimento. A possibilidade do exercício do direito à revogação deve ser dado por procedimento gratuito e facilitado (art. 8º, § 5º, da LGPD). A rigor, no mínimo se deve exigir que seja oferecido o mesmo meio para revogação daquele que se serviu o controlador para obter o consentimento, sendo sua eficácia a partir de quando é manifestado (ex nunc).[43] O direito de revogar relaciona-se também com o direito de informação do titular dos dados sobre a possibilidade e as consequências da revogação, inclusive sobre a eventualidade dela não impedir a continuidade do tratamento nas hipóteses que a lei estabelece.

3.3 Disciplina especial da proteção de dados pessoais sensíveis

A proteção de dados pessoais como expressão de uma dimensão de proteção da pessoa humana encontra maior fundamento e extensão no tocante aos denominados dados pessoais sensíveis. A LGPD define os dados pessoais sensíveis como aqueles "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II). Evidencia-se da definição que a natureza sensível do dado em questão refere-se á potencialidade de sua utilização de modo a dar causa à discriminação proibida do titular dos dados, em ofensa aos direitos fundamentais de liberdade e igualdade assegurados pela Constituição. Sobretudo se for considerada a utilização, no tratamento de dados, a partir de modelos automatizados, e para fins diversos, inclusive – nas relações de consumo – sobre a decisão do fornecedor de contratar ou não com determinado consumidor, ou as condições em que deva fazê-lo. Situações que, baseando-se na distinção a partir dos dados considerados sensíveis, caracterizarão conduta abusiva, proibida por lei, a ensejar sua rejeição pelo Direito nos diferentes planos, da responsabilização civil, penal e administrativa, assim como fundamentando providências processuais de modo a inibir ou fazer cessar a lesão.

A disciplina especial da proteção de dados sensíveis fixada pela LGPD tem a finalidade de prevenir e reduzir os riscos de discriminação em razão dos critérios proibidos pela Constituição, a partir da delimitação mais estrita das condições do seu tratamento. Conforme já foi mencionado, quanto aos dados pessoais sensíveis, o próprio consentimento do titular dos dados para tratamento é exigido que seja feito "de forma específica e destacada" vinculado a "finalidades específicas" (art. 11, I, da LGPD). Não se admite, portanto, um consentimento genérico, tampouco que se insira sem destaque em condições gerais contratuais, sem o devido destaque. Igualmente, não se autoriza qualquer espécie de presunção sobre o conhecimento prévio do consumidor da finalidade específica ao prestar o consentimento, para o que se atribui o ônus de demonstrar o regular atendimento das condições previstas na lei.

As hipóteses em que é autorizado o tratamento dos dados independentemente do consentimento do titular dos dados, da mesma forma, devem ser interpretadas restritivamente. São definidas no art. 11, inciso II, da LGPD. Tratam-se de situações em que o controlador esteja cumprindo obrigação legal ou regulatória; ou que os dados sirvam à execução, pela administração pública, de políticas públicas previstas em lei ou regulamento; da mesma forma, para realização de estudos por órgão de pesquisa em relação a dados anonimizados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para proteção da vida ou incolumidade do titular ou de terceiro; para tutela da saúde; ou em garantia da prevenção à fraude e à segurança do titular.

A LGPD prevê, igualmente, a possibilidade de ser estabelecida restrição ao tratamento de dados sensíveis, ao definir que sua comunicação ou uso compartilhado com objetivo de obter vantagem econômica poderá ser objeto de vedação ou regulamentação por parte da Autoridade Nacional de Proteção de Dados, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (art. 11, § 3º). Da mesma forma, se proíbe a comunicação ou uso compartilhado de dados relativo à saúde com objetivo de obter vantagem econômica, exceto no caso de portabilidade de dados consentido pelo titular, ou para atender necessidade de comunicação para a adequada prestação de serviços de saúde suplementar (art. 11, § 4º, II, da LGPD).

3.4 Disciplina especial da proteção de dados de crianças e adolescentes

Quando o titular dos dados seja crianças e adolescentes, informa a disciplina sua proteção a doutrina do melhor interesse, fundada no art. 227 da CF/1988 (LGL\1988\3). Não podem elas próprias manifestar consentimento válido. Daí porque a lei exige que o consentimento específico seja realizado por pelo menos um dos pais ou pelo representante legal (art. 14, § 1º, da LGPD).

Será definido um procedimento que assegure a publicidade sobre os termos do tratamento de dados, definindo que os controladores deverão manter pública a informação sobre os tipos de dados coletados, sua utilização e os procedimentos para exercício dos direitos pelo titular dos dados (art. 14, § 2º, da LGPD). Admite, contudo a possibilidade de coleta de dados pessoais de crianças sem consentimento, se forem utilizados para contatar pais ou responsáveis uma única vez, sem armazenamento, ou para sua proteção, sem que possam ser repassados a terceiros.

A coleta dos dados deve se dar de forma leal, considerando a vulnerabilidade agravada das crianças e adolescentes. Para tanto, compete ao controlador realizar "todos os esforços razoáveis" para determinar que o consentimento tenha sido realmente dado pelos pais ou responsáveis pelo titular dos dados. Da mesma forma, não pode o controlador condicionar a participação das crianças e adolescentes em jogos, aplicações de internet ou outras atividades, ao fornecimento de informações pessoais "além das estritamente necessárias à atividade". (art. 14, § 4º, da LGPD). No âmbito das relações de consumo, o art. 39, IV, do CDC (LGL\1990\40), define como prática abusiva "prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços". A utilização de jogos, aplicações de internet ou outros meios para coletar dados de consumidores crianças e adolescentes revela um prevalecimento de sua vulnerabilidade agravada, contaminando o posterior tratamento destes dados e a finalidade para as quais forem utilizados (especialmente para direcionamento ou segmentação de ofertas de produtos ou serviços).

Há, da mesma forma, um dever de informar qualificado em relação ao tratamento de dados de crianças e adolescentes, considerando tanto a capacidade de compreensão do titular dos dados, quanto de seus pais ou responsáveis. Para tanto, o art. 14, § 6º, da LGPD, define que tais informações deverão ser fornecidas "de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado",

no que se conforma ao dever de esclarecimento previsto também no CDC (LGL\1990\40).

3.5 Responsabilidade pelos danos aos consumidores: tratamento indevido de dados pessoais

Em relação aos danos causados em relação ao tratamento indevido de dados pessoais, é necessário que se compreenda a existência de um dever de segurança imputável aos agentes de tratamento (controladores e operadores de dados), que é segurança legitimamente esperada daqueles que exercem a atividade em caráter profissional, e por esta razão presume-se que tenham a expertise suficiente para assegurar a integridade dos dados e a preservação da privacidade de seus titulares. Daí porque a responsabilidade dos agentes de tratamento decorre do tratamento indevido ou irregular dos dados pessoais do qual resulte o dano. Exige-se a falha do controlador ou do operador, que caracteriza o nexo causal do dano. Contudo, não se deve perquirir se a falha se dá por dolo ou culpa, senão que apenas sua constatação é suficiente para atribuição da responsabilidade, inclusive com a possibilidade de inversão do ônus da prova em favor do titular dos dados, nas mesmas hipóteses de hipossuficiência e verossimilhança que a autorizam no âmbito das relações de consumo (art. 42, § 2º, da LGPD).

O art. 44 da LGPD define que "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I – o modo pelo qual é realizado; II – o resultado e os riscos que razoavelmente dele se esperam; III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado." A técnica legislativa empregada na LGPD aproxima-se notoriamente daquela adotada pelo CDC (LGL\1990\40) ao disciplinar o regime do fato do produto e do serviço, em especial na definição dos critérios a serem considerados para determinação do atendimento ao dever de segurança.

Note-se que a regra coloca em destaque, assim como ocorre em relação à responsabilidade do fornecedor no CDC (LGL\1990\40), a questão relativa aos riscos do desenvolvimento, uma vez que delimita a extensão do dever de segurança àquela esperada em razão das "técnicas de tratamento de dados disponíveis à época em que foi realizado". Isso é especialmente relevante considerando a grande velocidade do desenvolvimento da tecnologia no tratamento de dados, e os riscos inerentes, em especial as situações de vazamento e acesso não autorizado de terceiros aos dados armazenados pelo controlador ou pelo operador. Nestas hipóteses trata-se de definir em relação ao controlador e operador dos dados, se seria possível identificar um dever de atualização técnica imputável, e nestes termos, eventual adoção de novas técnicas que permitam o uso indevido do dado, especialmente por terceiros, venha a caracterizar espécie de risco inerente (fortuito interno), que não exclui sua responsabilidade pelos danos que venham a suportar os titulares dos dados; ou se delimitação quanto às técnicas disponíveis à época em que foi realizado o tratamento exclui eventual responsabilização do controlador e do operador pelo desenvolvimento tecnológico que permita obtenção de dados ou tratamento indevido por terceiros, desviado da finalidade originalmente prevista. Em outros termos, trata-se de situar, em relação à responsabilidade pelos danos causados em relação ao tratamento indevido de dados, qual o lugar dos riscos do desenvolvimento, considerando, neste caso, a própria previsibilidade de uma atualização e avanço técnico em atividades vinculadas à tecnologia da informação, mais veloz do que em outras atividades econômicas.

Os danos causados pelo tratamento indevido de dados pessoais dão causa à pretensão de reparação dos respectivos titulares dos dados pelos danos patrimonial e moral, individual ou coletivo. Responde pela reparação o controlador e o operador dos dados. No caso do operador, segundo o regime estabelecido pela LGPD, responderá solidariamente pelos danos causados quando descumprir as obrigações definidas na lei ou quando não tiver seguido as instruções lícitas do controlador, "hipótese em que o

operador equipara-se ao controlador" (art. 42, §1º, I). Já os controladores que estiverem "diretamente envolvidos" no tratamento do qual decorram danos ao titular dos dados, também responderão solidariamente pela reparação (art. 42, §1º, II). Deve-se bem compreender do que se tratam as situações em que o controlador dos dados esteja "diretamente envolvido", afinal, a ele cabe o tratamento de dados, diretamente, ou por intermédio dos operadores. Afinal, ao controlador competem "as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI, da LGPD). O operador, de sua vez, "realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII, da LGPD). Nestes termos, as condições de imputação de responsabilidade do controlador e do operador pelos danos decorrentes do tratamento indevido dos dados serão: a) a identificação de uma violação às normas que disciplinam o tratamento de dados pessoais; e b) a existência de um dano patrimonial ou extrapatrimonial (moral) ao titular dos dados. Para a imputação de responsabilidade de ambos não se exigirá a demonstração de dolo ou culpa (é responsabilidade objetiva). Da mesma forma, é correto compreender da exegese da lei, e em razão da própria essência das atividades desenvolvidas, que responderão solidariamente, de modo que o titular dos dados que sofrer o dano poderá demandar a qualquer um deles, operador ou controlador, individualmente ou em conjunto.

Tratando-se de danos a consumidores decorrentes do tratamento indevido de dados, contudo, o art. 45 da LGPD, ao dispor que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente", conduzem tais situações ao regime do fato do serviço (art. 14 do CDC (LGL\1990\40)). Neste caso, controlador e operador de dados respondem solidariamente assim como outros fornecedores que venham intervir ou ter proveito do tratamento de dados do qual resulte o dano. Neste caso, incidem tanto as condições de imputação da responsabilidade pelo fato do serviço (em especial o defeito que se caracteriza pelo tratamento indevido de dados, ou seja, desconforme à disciplina legal incidente para a atividade), quanto as causas que porventura possam excluir eventual responsabilidade do fornecedor (art. 14, § 3º), que estão, porém, em simetria com o disposto no próprio art. 43 da LGPD. Outro efeito prático da remissão do art. 45 da LGPD ao regime de reparação próprio da legislação de proteção do consumidor será a submissão de eventuais pretensões de reparação dos consumidores ao prazo prescricional previsto no seu art. 27 do CDC (LGL\1990\40), de cinco anos contados do conhecimento do dano ou de sua autoria.

4 Considerações finais

O tratamento de dados pessoais é um dos principais ativos da nova economia digital, expressão do que temos chamado novo paradigma tecnológico, cuja repercussão no mercado de consumo apenas se iniciou. Extensão da personalidade humana, os dados pessoais, resguardados sob a privacidade pessoal, converte-se em ativo ofertado pelo consumidor em troca de serviços até aqui qualificados como aparentemente gratuitos, mas que em verdade possuem uma onerosidade indireta decorrente da exigência de consentir em prestar dados como condição de acesso a serviços. Da mesma forma, a capacidade exponencial de processamento de dados permite usos novos ao tratamento destes dados, alterando a estratégia das empresas na oferta de produtos e serviços, direcionando e segmentando sua mensagem publicitária, na análise de risco de crédito do consumidor ou acompanhando a utilização do produto ou serviço ao longo do tempo. Estas circunstâncias, ao tempo em que podem aumentar a qualidade da prestação do fornecedor, lhe conferem um maior poder contratual, uma vez que o tratamento de dados pessoais permite antecipar preferências e identificar o perfil do consumidor com quem pretenda contratar, inclusive com a possibilidade de predizer seu comportamento negocial.

Daí porque, nos vários sistemas jurídicos, a legislação de proteção de dados pessoais orienta-se pela proteção não apenas da privacidade do titular dos dados, mas da sua liberdade pessoal, tanto no âmbito das relações negociais como também, em sentido

mais amplo, do exercício de seus direitos fundamentais em geral. Nas relações de consumo, a nova legislação brasileira confiou na sua interação com as normas de proteção do consumidor, ao prever em seu art. 64 a possibilidade de diálogo de fontes, bem como a articulação da Autoridade Nacional de Proteção de Dados e outros órgãos com competência sancionatória, inclusive os de proteção do consumidor (art. 55-K, parágrafo único). A prevalência da competência da Autoridade Nacional de Proteção de Dados não afasta a observância das normas de proteção do consumidor, por força do princípio da legalidade. No curso do exercício da sua atividade de regulação e supervisão da atividade de tratamento de dados, eventuais situações de conflito de competências entre os órgãos deverão orientar-se segundo o critério de predominância da matéria em exame.

Certo é que a edição e plena eficácia da Lei Geral de Proteção de Dados eleva o direito brasileiro a um novo estágio de proteção da personalidade, considerando as transformações operadas pelas novas tecnologias da informação e da internet, que abrangem praticamente todas as dimensões da vida em sociedade. No âmbito das relações de consumo, sua repercussão deve ser tomada sempre de modo a assegurar a efetividade dos direitos do consumidor.

5 Bibliografia

BERGSTEIN, Lais. O tempo do consumidor e o menosprezo planejado. São Paulo: Ed. RT, 2019.

BEYLEVELD, Deryck; BROWSWORD, Roger. Consent in the law. Oxford: Hart Publishing, 2007.

BIONI, Bruno Ricardo. Proteção de dados pessoais. A função e os limites do consentimento. São Paulo: Forense, 2019.

CACHAPUZ, Maria Cláudia. Os bancos cadastrais positivos e o tratamento à informação sobre (in)adimplemento. Revista AJURIS, v. 40, n. 131. Porto Alegre: Ajuris, set. 2013.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. Revistade Direitodo Consumidor. v. 46. São Paulo: Ed. RT, abr.-jun. 2003.

CRAVO, Daniela Copetti. Direito à portabilidade de dados: interface entre a defesa da concorrência, do consumidor e proteção de dados. Rio de Janeiro: Lumen Juris, 2018.

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

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.) Direito digital. Direito privado e internet. 2. ed. Indaiatuba: Foco, 2019.

FLETCHER, David. Internet of things. In: BLOWERS, Misty (Ed.) Evolution of cyber technologies and operations to 2035. Cham: Springer, 2015.

FTC. Protecting consumer privacy in an Era of Rapid Change. Recomendations for businesses and policymakers. FTC Report, march/2010, p. vii.

GARFINKEL, Simson. Database nation. The death of privacy in 21th century. Sebastopol: O'Reilly Media, 2000.

HACKENBERG, Wolfgang. Big data. In: HOEREN, Thomas; SIEBER, Ulrich; HOLZNAGEL, Bernd (Hrsg.) Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs. 37 Auf, Teil, 16.7, Rn 13, EL juli-2017.

HAHN, Horst; SCHREIBER, Andreas. E-Health. Potenziale der Digitalen Transformation in

der Medizin. In: NEUGEBAUER, Reimund (Hrsg.) Digitalisierung Schlüsseltechnologien für Wirtschaft und Gesellschaft. Heidelberg: Springer Vieweg, 2018.

HÄRTING, Niko. Anonymität und Pseudonymität im Datenschutzrecht, Neue Juristische Wochenschrift, 29. Munich: C.H. Beck, 2013.

HUSTINX, Peter. Privacy by design: delivering the promises. Identity in the information society, n. 3, 2010

JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (Coords.) Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Ed. RT, 2019.

MARQUES, Claudia Lima; GSELL, Beat (Orgs.) Novas tendências do direito do consumidor: rede Alemanha-Brasil de pesquisa em direito do consumidor. São Paulo: Ed. RT, 2015.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.) Direito digital. Direito privado e internet. 2. ed. Indaiatuba: Foco, 2019.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. In: MARQUES, Claudia Lima; GSELL, Beat (Orgs.) Novas tendências do direito do consumidor: rede Alemanha-Brasil de pesquisa em direito do consumidor. São Paulo: Ed. RT, 2015.

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

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, v. 120. São Paulo: Ed. RT, nov.-dez., 2018.

MICKLITZ, Hans-Wolfgang; JOOST, Lucia A. Reisch Gesche; ZANDER-HAYAT, Helga (Hrsg.). Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt. Baden-Baden: Nomos, 2017.

MINOW, Martha. Making all the difference. Inclusion, exclusion and American Law. Ithaca: Cornell University Press, 1990.

MIRAGEM, Bruno. Curso de direito do consumidor. 7. ed. São Paulo: Ed. RT, 2018.

MIRAGEM, Bruno. Eppur si muove: diálogo das fontes como método de interpretação sistemática no direito brasileiro. In: MARQUES, Claudia Lima (org.). Diálogo das fontes. Do conflito à coordenação de normas do direito brasileiro. São Paulo: Ed. RT, 2012.

OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados pessoais e sua repercussão no direito brasileiro. São Paulo: Ed. RT, 2019.

PIORE, Michael J.; SABEL, Charles F. The second industrial divide. Possibilities for prosperity. New York: Basic Books, 1986 (reimpressão do original de 1984).

RESTA, Giorgio. Revoca del consenso ed interesse al tratamento nella legge sulla protezione dei dati personali. Rivista Critica del Diritto Privato, ano XVIII, n. 2. Bologna, giugno/2000.

SCHMECHEL, Philipp. Verbraucherdatenschutzrecht in der EU-DatenschutzGrundverordnung. In: MICKLITZ, Hans-Wolfgang; JOOST, Lucia A. Reisch Gesche; ZANDER-HAYAT, Helga (Hrsg.). Verbraucherrecht 2.0 – Verbraucher in

der digitalen Welt. Baden-Baden: Nomos, 2017.

SCHWENKE, Matthias Cristoph. Individualisierung und datenschutz. Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung. Wiesbaden: Deutscher Universitäts-Verlag, 2006.

SIMITIS, Spiros (Hrsg). Bundesdatenschutzgesetz, 8. Auf. Baden-Baden: Nomos, 2014.

SIMITIS, Spiros. Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. Neue Juristische Wochenschrift, 8. München: C.H. Beck, 1984.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados pessoais e sua repercussão no direito brasileiro. São Paulo: Ed. RT, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados pessoais e sua repercussão no direito brasileiro. São Paulo: Ed. RT, 2019.

VAINZOF, Rony. Comentários ao art. 6º. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (Coords.). LGPD: Lei geral de proteção de dados comentada. São Paulo: Ed. RT, 2019.

---

1 GARFINKEL, Simson. Database nation. The death of privacy in 21th century. Sebastopol: O'Reilly Media, 2000, p. 4-5.

2 MIRAGEM, Bruno. Curso de direito do consumidor. 7. ed. São Paulo: Ed. RT, 2018, p. 352 e ss.

3 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, v. 120. São Paulo: Ed. RT, nov.-dez. 2018, p. 469-483.

4 MENDES/DONEDA. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados, cit.

5 Sobre o tema já examinei em: MIRAGEM, Bruno. Eppur si muove: diálogo das fontes como método de interpretação sistemática no direito brasileiro. In: MARQUES, Claudia Lima (org.). Diálogo das fontes. Do conflito à coordenação de normas do direito brasileiro. São Paulo: Ed. RT, 2012, cit.

6 BIONI, Bruno Ricardo. Proteção de dados pessoais. A função e os limites do consentimento. São Paulo: Forense, 2019, p. 51 e ss.

7 MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 161 e ss. DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.) Direito digital. Direito privado e internet. 2. ed. Indaiatuba: Foco, 2019, p. 35 e ss. Em sua tese doutoral Danilo Doneda registra interessante assertiva, apontando a trajetória pela qual o direito à privacidade sofre metamorfose da qual resulta a proteção de dados pessoais. DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. Rio de Janeiro: Renovar, 2006, p. 3.

8 Em especial do direito alemão, a partir de decisão paradigmática do Tribunal Constitucional (Volkszählungsurteil), de 15 de dezembro de 1983, que julgou parcialmente inconstitucional a "Lei do Censo" na qual se consagrou o Grundrecht auf

informationelle Selbsbestimmung, traduzido então como "direito de autodeterminação informativa", como projeção do direito geral de personalidade. (A decisão em questão era relativa a lei aprovada pelo Parlamento em 1982, que determinava as informações que deveriam ser coletadas para efeito da realização de censo populacional, e cuja recusa em fornecê-las submetia aquele que o fizesse a sanções. O Tribunal terminou por reconhecer o direito do indivíduo de poder decidir, ele próprio sobre o fornecimento e utilização de seus dados por terceiros, o que só poderia ser limitado por razões de interesse público, observada a proporcionalidade. Veja-se: SIMITIS, Spiros. Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. Neue Juristische Wochenschrift, 8. München: C.H. Beck, 1984, p. 398-405.

9 Dentre outros, veja-se: CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. RevistadeDireitodoConsumidor. v. 46. p. 77. São Paulo: Ed. RT, abr.-jun. 2003, p. 77 e ss; MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. In: MARQUES, Claudia Lima; GSELL, Beat (Orgs.) Novas tendências do direito do consumidor: rede Alemanha-Brasil de pesquisa em direito do consumidor. São Paulo: Ed. RT, 2015, p. 203; CACHAPUZ, Maria Cláudia. Os bancos cadastrais positivos e o tratamento à informação sobre (in)adimplemento. Revista AJURIS, v. 40, n. 131. Porto Alegre: Ajuris, set. 2013, p. 259. Na jurisprudência, veja-se a síntese deste pensamento na decisão da Min. Nancy Andrighi: "Os direitos à intimidade e à proteção da vida privada, diretamente relacionados à utilização de dados pessoais por bancos de dados de proteção ao crédito, consagram o direito à autodeterminação informativa e encontram guarida constitucional no art. 5º, X, da Carta Magna, que deve ser aplicado nas relações entre particulares por força de sua eficácia horizontal e privilegiado por imposição do princípio da máxima efetividade dos direitos fundamentais." (STJ, EDcl no REsp 1630659/DF, Rel. Min. Nancy Andrighi, 3ª T., j. 27.11.2018, DJe 06.12.2018).

10 SCHWENKE, Matthias Cristoph. Individualisierung und datenschutz..., p. 168 e ss.

11 SIMITIS, Spiros (Hrsg). Bundesdatenschutzgesetz, 8. Auf. Baden-Baden: Nomos, 2014, p. 470 e ss. No direito brasileiro, Bruno Bioni refere-se ao consentimento como "protagonista" da proteção de dados: BIONI, Bruno. Proteção de dados pessoais..., p. 139. No mesmo sentido, sustentam: TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e sua repercussão no direito brasileiro. São Paulo: Ed. RT, 2019, p. 298.

12 A referência, aqui, à noção de especialização flexível, atribui-se a: PIORE, Michael J.; SABEL, Charles F. The second industrial divide. Possibilities for prosperity. New York: Basic Books, 1986 (reimpressão do original de 1984).

13 A noção de especialização flexível possui características mais amplas em relação à toda a organização e divisão do trabalho, amplamente estudadas pela teoria da administração e na economia, que repercutirá em transformações no mercado de consumo. De regra, se traduzem a partir de uma estratégia de inovação permanente e de uso flexível da tecnologia, dentre outras características.

14 No direito brasileiro, relaciona esta transformação do mercado a valorização do tratamento de dados pessoais: MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 84 e ss.

15 SCHMECHEL, Philipp. Verbraucherdatenschutzrecht in der EU-DatenschutzGrundverordnung. In: MICKLITZ, Hans-Wolfgang; JOOST, Lucia A. Reisch Gesche; ZANDER-HAYAT, Helga (Hrsg.). Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt. Baden-Baden: Nomos, 2017, p. 266.

16 SCHWENKE, Matthias Cristoph. Individualisierung und datenschutz. Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung. Wiesbaden: Deutscher Universitäts-Verlag, 2006, p. 49.

17 BIONI, Bruno Ricardo. Proteção de dados pessoais. A função e os limites do consentimento. São Paulo: Forense, 2019, p. 41-42.

18 A vulnerabilidade dos dispositivos com aplicações da denominada internet das coisas, sobretudo em relação à segurança dos dados que armazenem ou utilizem, é um dos principais desafios reconhecidos à esta nova tecnologia, conforme refere: FLETCHER, David. Internet of things. In: BLOWERS, Misty (Ed.) Evolution of cyber technologies and operations to 2035. Cham: Springer, 2015, p. 19 e ss.

19 TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados pessoais e sua repercussão no direito brasileiro. São Paulo: Ed. RT, 2019, p. 300.

20 DONEDA, Danilo. Direito fundamental à proteção de dados pessoais, p. 45.

21 "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador; III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

22 "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

23 "§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências."

24 Não se perca de vista a profunda transformação que o tratamento de dados, ao lado de outras tecnologias da informação vem trazendo à área médica, na redução de custos e maior precisão, agilidade e eficiência na prevenção, diagnóstico precoce e tratamento de enfermidades, resultando no estágio atual em que o desafio dos diversos prestadores de serviço orientam-se a busca de maior poder de integração e acesso a dados pessoais de saúde, a partir de uma "superconvergência tecnológica". A respeito, veja-se: HAHN, Horst; SCHREIBER, Andreas. E-Health. Potenziale der Digitalen Transformation in der Medizin. In: NEUGEBAUER, Reimund (Hrsg.) Digitalisierung Schlüsseltechnologien für Wirtschaft und Gesellschaft. Heidelberg: Springer Vieweg, 2018, p. 321-345.

25 BIONI, Bruno Ricardo. Proteção de dados pessoais..., p. 250 e ss.

26 Neste particular, com maior gravidade quando se trate do que a doutrina vem denominando de menosprezo planejado do tempo do consumidor, conforme: BERGSTEIN, Lais. O tempo do consumidor e o menosprezo planejado. São Paulo: Ed. RT, 2019, p. 104 e ss.

27 GARFINKEL, Simson. Database nation. The death of privacy in 21th century. Sebastopol: O'Reilly Media, 2000, p. 156-157.

28 Embora em outro contexto, foi o caráter excessivo e a perda da relevância das informações com o decurso do tempo que levou o STJ, em 2018, a reconhecer o direito à desindexação em sites de busca do nome do autor e de notícias desabonadoras a seu respeito: STJ, REsp 1660168/RJ, Rel. Min. Nancy Andrighi, Rel. p/ Acórdão Min. Marco Aurélio Bellizze, 3ª Turma, j. 08.05.2018, DJe 05.06.2018.

29 Veja-se: HUSTINX, Peter. Privacy by design: delivering the promises. Identity in the information society, n. 3, 2010, p. 253 e ss. No direito brasileiro, veja-se: VAINZOF, Rony. Comentários ao art. 6º. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (Coords.). LGPD: Lei geral de proteção de dados comentada. São Paulo: Ed. RT, 2019, p. 158-159; JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (Coords.) Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Ed. RT, 2019, p. 169 e ss.

30 Neste sentido, as recomendações da Federal Trade Comission para elaboração de políticas públicas de proteção da privacidade do consumidor: FTC, Protecting consumer privacy in an Era of Rapid Change. Recomendations for businesses and policymakers. FTC Report, march/2010, p. vii.

31 TJRS, ApCiv 70049609944, 9ª Câmara Cível, Rel. Leonel Pires Ohlweiler, j. 24.10.2012.

32 A doutrina do "separate but equal" foi afirmada pela Suprema Corte norte-americana a partir do caso Plessy vs. Ferguson (1896), sendo sustentada até a reversão do entendimento pelo festejado precedente Brown vs Board of Education (1954). Por outro lado, identifica-se o denominado "dilema da diferença", pelo qual se questiona como a proibição de diferenciação de um lado pode inibir a proteção dos grupos diferentes, inclusive para efeito de inclusão e acesso aos bens e serviços que em razão da discriminação lhe foram historicamente restringidos. Sobre o debate, no direito norte-americano, veja-se: MINOW, Martha. Making all the difference. Inclusion, exclusion and American Law. Ithaca: Cornell University Press, 1990, p. 19 e ss.

33 MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor, p. 213.

34 Constituem requisitos mínimos do programa de governança conforme definido na lei, que: "a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas." (art. 50, § 2º, I, da LGPD)

35 OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e sua repercussão no direito brasileiro. São Paulo: Ed. RT, 2019, p. 566.

36 São competências da Autoridade Nacional de Proteção de Dados relacionadas no art. 55-J da LGPD: "I – zelar pela proteção dos dados pessoais; II – editar normas e procedimentos sobre a proteção de dados pessoais; III – deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos; IV – requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; V – implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; VI – fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; VII – comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; VIII – comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; IX – difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; X – estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores; XI – elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; XII – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; XIII – realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; XIV – realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; XV – articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XVI - elaborar relatórios de gestão anuais acerca de suas atividades."

37 SIMITIS, Spiros (Hrsg). Bundesdatenschutzgesetz, 8. Auf. Baden-Baden: Nomos, 2014, cit.

38 BEYLEVELD, Deryck; BROWSWORD, Roger. Consent in the law. Oxford: Hart Publishing, 2007, p. 145 ss.

39 BIONI, Bruno Ricardo. Proteção de dados pessoais..., p. 198.

40 HÄRTING, Niko. Anonymität und Pseudonymität im Datenschutzrecht, Neue Juristische Wochenschrift, 29. Munich: C.H. Beck, 2013, p. 2065-2071.

41 HACKENBERG, Wolfgang. Big data. In: HOEREN, Thomas; SIEBER, Ulrich; HOLZNAGEL, Bernd (Hrsg.) Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs. 37 Auf, Teil, 16.7, Rn 13, EL juli/2017.

42 CRAVO, Daniela Copetti. Direito à portabilidade de dados: interface entre a defesa da concorrência, do consumidor e proteção de dados. Rio de Janeiro: Lumen Juris, 2018, p. 105.

43 Assim como é da tradição da legislação de proteção de dados, conforme assinala RESTA, Giorgio. Revoca del consenso ed interesse al tratamento nella legge sulla protezione dei dati personali. Rivista Critica del Diritto Privato, ano XVIII, n. 2. Bologna, giugno/2000, p. 299 e ss.