UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

DEPARTAMENTO DE DIREITO PRIVADO

THAIS CARNEIRO MEDEIROS

RESPONSABILIDADE CIVIL PELA VIOLAÇÃO AO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

FORTALEZA

2021

THAIS CARNEIRO MEDEIROS

RESPONSABILIDADE CIVIL PELA VIOLAÇÃO AO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Monografia submetida à Coordenação do Curso de Graduação em Direito, da Universidade Federal do Ceará, como requisito parcial para a aquisição do título de Bacharel em Direito. Área de concentração: Direito Civil.

Orientador: Prof. Dr. Emmanuel Teófilo Furtado Filho.

FORTALEZA

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M44r Medeiros, Thais Carneiro.
Responsabilidade Civil pela Violação ao Direito à Proteção de Dados Pessoais / Thais Carneiro Medeiros. – 2021.
47 f. : il.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2021.
Orientação: Prof. Emmanuel Teófilo Furtado Filho.

1. dados pessoais. 2. proteção de dados. 3. LGPD. 4. responsabilidade civil. 5. direito fundamental. I. Título.

CDD 340

THAIS CARNEIRO MEDEIROS

RESPONSABILIDADE CIVIL PELA VIOLAÇÃO AO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Monografia apresentada à banca examinadora e à Coordenação do Curso de Direito da Universidade Federal do Ceará, adequada e aprovada para suprir a exigência parcial inerente à obtenção do grau de bacharel em direito, em conformidade com os normativos do MEC.

Aprovada em: __/__/____.

BANCA EXAMINADORA

_____
Prof. Dr. Emmanuel Teófilo Furtado Filho (Orientador)
Universidade Federal do Ceará (UFC)

_____
Mestrando Ricardo Maia
Universidade Federal do Ceará (UFC)

_____
Mestrando Rafael Sales
Universidade Estadual do Ceará (UFC)

A Deus.

Aos meus pais, família e amigos.

AGRADECIMENTOS

Aos meus pais, Cleinilton e Luzia, pelo amor, incentivo e apoio incondicional. É um grande privilégio ser filha de vocês.

Aos meus irmãos, Thiago e Thales, que compartilham comigo o amor à essa profissão, por toda troca, cuidado e amor.

Ao Alysson, meu companheiro e melhor amigo, por ter escutado todos meus medos, apreensões e apresentações de trabalho. Agradeço-lhe por todo apoio e suporte.

A Vandressa, Luisa, Paulo, Larissa, Clarissa, Giulia e Victor por terem me acompanhado nessa jornada acadêmica. Vocês tornaram a trajetória na Faculdade de Direito mais divertida e leve.

A Larissa, Ana Clara e Natália, pela amizade compartilhada ao logo dos anos e por celebrarem tantas fases da vida junto comigo.

Aos meus colegas da APSV Advogados, que ao compartilharem comigo o árduo exercício da advocacia, me ensinaram tanto e foram essenciais na minha formação profissional.

Ao Prof. Emmanuel Teófilo Furtado Filho, por toda atenção, solicitude e confiança depositada. Aos professores participantes desta banca examinadora pelo tempo e pelas contribuições feitas ao trabalho.

À Faculdade de Direito e seu corpo discente por todos os ensinamentos e pela contribuição na minha formação.

A todos aqueles que estiveram presente e me auxiliaram ao longo dos anos da minha jornada acadêmica.

“Se tornou aparentemente óbvio que nossa tecnologia excedeu nossa humanidade.” (Albert Einstein).

RESUMO

O objetivo deste trabalho é analisar a proteção dos dados pessoais sob o prisma de um direito fundamental e compreender os contornos legais de um dos mecanismos de defesa desse direito: a responsabilidade civil dos agentes de tratamento de dados. Para tanto, serão examinados o conceito de dado pessoal e a inserção da proteção desse bem jurídico no rol dos direitos fundamentais. Na sequência serão apreciados a definição dos sujeitos envolvidos no tratamento de dados, os princípios e as bases legais que irão legitimar essa atividade. Analisar-se-à, ainda, o regime da responsabilidade civil adotado pela Lei Geral de Proteção de Dados (LGPD), as hipóteses de sua incidência, os pressupostos de sua aplicação e as previsões normativas que garantem a proteção dos dados pessoais, avaliando também alguns critérios que deverão ser utilizados para reparar de forma integral eventual dano suportado pelo titular por ofensa ao seu direito fundamental. A metodologia utilizada foi a de pesquisa bibliográfica, por meio de análise de livros, artigos jurídicos, documentos internacionais, legislação e jurisprudência.

Palavras-chave: dados pessoais; proteção de dados; LGPD; responsabilidade civil; direito fundamental.

ABSTRACT

The objective of this paper is to analyze the protection of personal data from the point of view of a fundamental right and to understand the legal contours of one of the defense mechanisms of this right: the civil liability of data processing agents. For this purpose, the concept of personal data and the insertion of the protection of this legal asset in the list of fundamental rights will be examined. Next, the definition of the subjects involved in the treatment of data, the principles and the legal bases that will legitimize this activity will be examined. The civil liability regime adopted by the General Law of Data Protection (LGPD) will also be analyzed, as well as the hypotheses of its incidence, the assumptions of its application and the normative provisions that guarantee the protection of personal data, also evaluating some criteria that should be used to fully repair any damage suffered by the holder due to an offense to his fundamental right. The methodology used was bibliographical research, through the analysis of books, legal articles, international documents, legislation and jurisprudence.

Keywords: personal data; data protection; LGPD; civil liability; fundamental right.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ADI	Ação Direta de Inconstitucionalidade
CDC	Código de Defesa do Consumidor
EDPB	*European Data Protection Board*
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MP	Medida Provisória
PEC	Proposta de Emenda à Constituição
STF	Supremo Tribunal Federal

SUMÁRIO

1 INTRODUÇÃO

Na era da informação, o poder e a riqueza se concentram naqueles que detém a maior quantidade de informação, ou melhor, de dados.

Ressaltando a grande importância dos dados para a economia moderna, destaca Nick Srnicek (2018) que o capitalismo de século XXI se baseia na *data-driven economy*, na economia movida a dados. “Os dados se tornaram matéria-prima dos negócios, um recurso econômico vital, usado para criar uma nova forma de valor econômico” (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 4). São vistos como “o novo petróleo” e vem ganhando grande destaque para as articulações mercadológicas da contemporaneidade.

Diante disso, surge o problema da proteção aos dados pessoais e de como preservar o direito dos indivíduos em uma sociedade digital.

A Lei Geral de Proteção de Dados (LGPD) emerge justamente da necessidade de regulamentar esse novo mercado exploratório de dados pessoais, protegendo o titular dos dados, na medida em que cria limites à forma e ao modo em que serão realizados os tratamentos de dados pessoais.

Partindo da percepção da necessidade de se traçar mecanismos eficientes à preservação do direito dos indivíduos frente aos desatinos e anseios da economia moderna, o presente trabalho se propõe a compreender a responsabilidade civil dos agentes de tratamento como um mecanismo de tutela ao direito fundamental do titular à proteção de seus dados pessoais.

Utiliza-se, como metodologia, de pesquisa do tipo bibliográfica por meio de análise de livros, artigos jurídicos, documentos internacionais, da legislação e da jurisprudência. A pesquisa é pura, de natureza qualitativa, com finalidade descritiva e exploratória.

O texto estrutura-se em três partes.

Na primeira irá se delimitar o exato conceito de dado pessoal apto a atrair repercussão jurídica. Os contornos da definição do bem jurídico em estudo servirão para compreender com exatidão o que será resguardado sob a tutela de um direito fundamental autônomo.

Na sequência serão analisados conceitos gerais da legislação, definição dos agentes envolvidos no tratamento e a atividade que fica a cargo de cada um, explorando ainda os princípios previstos na Lei e as bases legais que irão legitimar o tratamento de dados. Essas informações irão orientar a forma como será analisada a responsabilidade civil.

Por fim, serão estudados a responsabilização civil na LGPD, o regime jurídico adotado e os elementos previstos na Lei, tais como as hipóteses que vão dar ensejo à obrigação de indenizar, a possibilidade de responsabilidade solidária, as excludentes e de inversão do ônus da prova. Compreendendo, ainda, alguns critérios que podem ser utilizados para fixação do *quantum* indenizatório devido no caso de lesão extrapatrimonial do titular dos dados pessoais.

O presente estudo não tem por objetivo esgotar o tema sobre a responsabilidade civil no regime de proteção dos dados pessoais, mas busca aclarar alguns elementos da nova legislação, a qual tem como foco principal o indivíduo, de forma a garantir a efetiva proteção deste.

2 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

O dado pessoal como um bem jurídico ganhou relevância no ordenamento jurídico brasileiro com a edição e promulgação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que estabeleceu, pela primeira vez, um conjunto de normas destinadas a regular o seu tratamento (BRASIL, 2018).

Essa Lei trouxe um regime geral sobre o tema e, juntamente com a Lei de Acesso à Informação, o Marco Civil da Internet (MCI) e o Código de Defesa do Consumidor (CDC), compõe o conjunto normativo responsável por regulamentar o tratamento da informação no Brasil (MENDES; DONEDA, 2018).

Além de emergir de uma necessidade de complementar o ordenamento jurídico interno, a Lei brasileira também surge diante da imprescindibilidade de uma regulamentação internacional e convergente sobre o tema, considerando a existência de uma economia digital global, onde as informações não ficam restritas a territórios específicos. Nesse sentido, a LGPD se inspira no modelo europeu de proteção de dados, amparado essencialmente no Regulamento 2016/679 (Regulamento Geral de Proteção de Dados), também conhecido pela sua sigla em inglês GDPR (*General Data Protection Regulation*).

Nesse sistema regulatório, o dado pessoal ganha contornos de bem jurídico e, mais do que isso, a sua proteção se apresenta como um direito fundamental do seu titular. Mas antes de adentrar na perspectiva da proteção a esse bem jurídico, por meio do mecanismo de responsabilização civil, é necessário definir o que vem a ser dado pessoal apto a atrair repercussão jurídica.

2.1 Conceito reducionista *versus* expansionista de dados pessoais, dados anonimizados e dados pessoais sensíveis

A exata compressão do conceito de dado pessoal passa pela análise de duas teorias: a reducionista e a expansionista.

Na perspectiva reducionista, apenas os dados que digam respeito à uma pessoa identificada, específica e determinada é que serão qualificados como dado pessoal. É necessário, portanto, haver um vínculo direto e imediato entre o dado e a pessoa a que este se refira para caracterizá-lo como dado pessoal. Ao passo que sob a perspectiva expansionista, dados pessoais serão todas as informações que digam respeito à uma pessoa identificada ou

identificável. O vínculo entre o dado e pessoa a que ele diga respeito pode ser indireto ou mediato (BIONI, 2015).

Em termos práticos, os dados pessoais sob a teoria reducionista seriam, por exemplo, o número da carteira de identidade ou do cadastro de pessoa física, enquanto para a teoria expansionista abrangeria também informações como os dados de localização e o número do *Internet Protocol* (IP), que apesar de não serem capazes de identificar, por si só, o titular daquela informação, pode em conjunto com outras informações e com o tratamento adequado identificá-lo.

Nesse sentido,

> Ainda que divergentes, tais teorizações detêm o mesmo centro gravitacional. Ambas demandam uma análise contextual donde está inserido um dado, aferindo-se o seu grau de identificabilidade para, então, desencadear a compreensão se uma determinada informação está relacionada a uma pessoa identificada ou identificável. (SCHWARTZ; SOLOVE, 2011).

Disso desprende-se que a verificação de um dado como pessoal, nos termos da teoria expansionista, passa por uma análise do termo "identificável" que deve ser investigado de acordo com a informação que pode ser extraída quando analisada em conjunto os dados presentes em uma base específica.

Adotando a teoria expansionista, a LGPD define expressamente dado pessoal no seu art. 5º, inciso I, como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018, s. p.). Assim, no direito brasileiro os dados que atraem repercussão jurídica são todos aqueles que sejam aptos a identificar uma pessoa natural.

Contrapondo-se ao conceito de dado pessoal há o de dado anônimo, o qual, a *contrario sensu*, diz respeito a um dado que não tem aptidão de identificar uma pessoa individualizada. A quebra do vínculo entre o dado e seu titular pode ser fruto de um processo denominado anonimização, pelo qual o dado antes pessoal, relativo à pessoa identificada, torna-se anonimizado (DONEDA, 2006). Para tanto, pode-se utilizar-se de diversas técnicas, que, em tese, eliminariam a identificação dos dados.

Ocorre que a oposição entre dado pessoal e dado anonimizado não é tão simples. Isso porque o avanço tecnológico vem demonstrando a falibilidade do processo de anonimização, sendo possível, mediante o uso das técnicas adequadas[1], a reidentificação das bases de dados anonimizados. Sobre o tema: "o surgimento de poderosos algoritmos de reidentificação demonstra não apenas uma falha em uma técnica específica de anonimização,

[1] A respeito do tema *vide* NARAYANAN, Arvind; SHMATIKOV, Vitaly. *How to break anonymity of the Netflix.* 2007. Disponível em: https://goo.gl/RxggOU. Acesso em 11 jul. 2021.

mas sim a inadequação fundamental de todo o paradigma de proteção de privacidade com base na 'desidentificação' dos dados" (NARAYANAN; SHMATIKOV, 2010, p. 26)[2].

Há, portanto, uma zona cinzenta entre dado pessoal relativo à uma pessoa natural identificável e o dado anonimizado, uma vez que

> Por essa lógica, qualquer dado pessoal anonimizado detém o risco inerente de se transmudar em um dado pessoal. A agregação de diversos "pedaços" de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico (TENE, 2013).

Diante da possível sinonímia entre dado pessoal e dado anonimizado – considerando que este, em última análise, tem a potencialidade de se tornar identificável – faz surgir a necessidade de se delimitar a abrangência do conceito expansionista de dado pessoal no que tange especificamente a compreensão de "identificável".

O critério adotado pelo direito comunitário europeu[3] e pela LGPD[4], legislações que adotaram o conceito expansionista, foi o da razoabilidade. Isto é, a mera potencialidade de identificação de um dado pessoal não seria suficiente para enquadrar o dado pessoal como identificável. É necessário que seja possível identificar o titular daquele dado utilizando-se de um "esforço razoável"[5] (BIONI, 2020).

Na definição do que vem a ser esforço razoável, a LGPD define no art. 12, §1º que "a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios" (BRASIL, 2018, s. p.).

A aferição da razoabilidade se dá por meio de critérios objetivos (tempo e custo), que deveram ser avaliados diante das circunstâncias concretas e de acordo com o estado da

---

[2] "The emergence of powerful re-identification algorithms demonstrates not just a flaw in a specific anonymization technique(s), but the fundamental inadequacy of the entire privacy protection paradigm based on "de-identifying" the data" (tradução livre).

[3] Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679 utiliza-se do termo na consideranda 26: "Para determinar se uma pessoa singular é identificável, importa **considerar todos os meios suscetíveis de ser razoavelmente utilizados**, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. [...]" (CONSELHO EUROPEU, 2016, s. p.) (grifo nosso).

[4] "Art. 5º Para os fins desta Lei, considera-se: [...] III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a **utilização de meios técnicos razoáveis** e disponíveis na ocasião de seu tratamento" (BRASIL, 2018, s. p.) (grifo nosso).

"Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, **com esforços razoáveis**, puder ser revertido" (BRASIL, 2018, s. p.) (grifo nosso)

[5] Terminologia utilizada pela LGPD (art. 12, *caput*, Lei nº 13.709/2018): "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido" (BRASIL, 2018, s. p.).

arte, uma vez que o tempo e o custo para reverter um processo de anonimização irá variar de acordo como o avanço da tecnologia.

Será, portanto, esse filtro da razoabilidade que determinará o que vem a ser "um risco aceitável em torno da reversibilidade do processo de anonimização a fim de que os dados anonimizados estejam fora do conceito de dados pessoais" (BIONI, 2015, p. 32).

Assim, a conceituação de dado pessoal, apto a atrair proteção jurídica, passa pela compreensão de que este diz respeito à uma informação relativa a uma pessoa natural identificada ou identificável, considerando que a potencialidade de identificação tem que ser aferida de acordo com o conjunto constante em uma base de dados específica e observando, ainda, o uso de técnicas que importem em um esforço razoável à sua identificação.

Em oposição a essa definição, os dados que não digam respeito à uma pessoa identificada ou identificável ou, ainda, que para sua identificação demande um esforço que ultrapasse o razoável, são considerados dados anônimos (ou anonimizados) e estão fora da tutela jurídica da LGPD.

Acertadamente a legislação brasileira atribuiu conceitos dinâmicos ao que vem a ser dados pessoais e dados anônimos, visto que o que definirá se um dado pode vir a ser identificável é o *status* da tecnologia. Essa flexibilidade dada pela legislação é de extrema importância para não engessar sua aplicação e possibilitar uma ampla proteção.

Além da categorização dos dados em pessoais e anônimos, há ainda os dados pessoais sensíveis, os quais correspondem a dados pessoais destacados pela sua natureza e, em razão desta, merecem proteção jurídica diferenciada.

De forma a estruturar a compreensão, pode se conceber uma categoria mais abrangente de dados pessoais *latu sensu*, a qual se subdivide em dados pessoais *stricto sensu* e dados pessoais sensíveis.

Assim, nos termos do art. 5º, II da LGPD, dados sensíveis são dados pessoais que versem sobre 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" (BRASIL, 2018, s.p.). Ou seja, dados sensíveis são aqueles relacionados a questões mais subjetivas e comportamentais da pessoa natural e, por isso, apresentam um maior potencial lesivo, exigindo, consequentemente, um regime jurídico próprio mais protetivo, o qual encontra previsão na Seção II do Capítulo II da LGPD, que trata especificamente das regras que regulamentam o tratamento dos dados pessoais sensíveis.

> A categoria de dados sensíveis foi desenvolvida a partir da percepção de que o armazenamento, processamento e circulação de alguns tipos de dados podem se constituir em uma ameaça maior à personalidade individual, especialmente, se utilizados para condutas discriminatórias (MENDES, 2008, p. 64).

É o potencial do tratamento discriminatório desses dados que o fazem com que estes recebam a proteção jurídica diferenciada.

Contudo, não apenas dados que digam respeito diretamente às categorias elencadas pela legislação podem ser utilizados com o cunho discriminatório. A verdade é que até mesmo os dados pessoais *stricto sensu*, que a priori não conteriam informações sensíveis, podem ser utilizados como potencialmente discriminatórios.

> Quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade. Ainda que, assim como um dado anônimo pode se tornar um dado pessoal, um dado 'trivial' pode também se transmudar em um dado sensível, particularmente, quando se têm disponíveis tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos, tal como ocorreu com a loja de departamentos que identificou quais consumidoras estariam grávidas, precisando, inclusive, o período gestacional (BIONI, 2019, p. 106).

Quando se pensa na utilização de altas tecnologias como o *Big Data*[6], as fronteiras do que é possível se fazer ou as formas em que os dados pessoais podem ser tratados se expandem, possibilitando a reidentificação de dados anonimizados, a utilização de bases para a criação de perfis comportamentais, entre outros, sendo esta uma tendência que se projeta ao futuro.

Justamente considerando essas circunstâncias que a lei brasileira dá um passo à frente e expande a proteção conferida pelo regime específico conferido a essa categoria de dados pessoais prevendo que esse regime será aplicado a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular[7].

Daí surge a importância em superar conceitos teóricos restritivos, devendo se pensar em uma normatização da proteção de dados que supere a teoria e se volte para a prática, protegendo o indivíduo sempre que a atividade de tratamento de dados possa lhe causar algum dano (BIONI, 2015).

---

[6] O Instituto de Tecnologia & Sociedade do Rio (2016, p. 9) define *big data* como "O conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores."

[7] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] § 1º **Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular**, ressalvado o disposto em legislação específica" (BRASIL, 2018, s. p.) (grifo nosso).

2.2 Proteção aos dados pessoais enquanto direito fundamental do titular

A percepção da proteção de dados pessoais baseado em um direito fundamental do titular ganhou contornos mais evidentes com a paradigmática decisão do Tribunal Constitucional Federal Alemão, no julgamento da inconstitucionalidade da "Lei do recenseamento de População, Profissão, Moradia e Trabalho".

Reconhecendo um direito à "autodeterminação informativa", o Tribunal Alemão julgou parcialmente inconstitucional a referida lei, que previa sobre a coleta de dados diversos dos cidadãos com o objetivo de obter informações acerca do crescimento populacional e sua distribuição pelo território, além das atividades econômicas exercidas, autorizando, ainda, a criação de um banco de dados e a comunicação dos dados obtidos com outros órgãos e o seu cruzamento com as informações presentes em registros públicos.

A declaração de nulidade pelo Tribunal se deu em relação aos dispositivos que autorizavam o cruzamento dos dados coletados e que tratavam da possibilidade de transferência desses dados, entendendo que: "sob as modernas condições de processamento de dados, o livre desenvolvimento da personalidade pressupõe a proteção do indivíduo contra coleta, armazenamento, uso e transmissão irrestritos de seus dados pessoais" (MARTINS, 2005, p. 238)[8]

O ineditismo da decisão proferida em meados de 1983 evocou a proteção dos dados pessoais enquanto um direito inerente ao livre desenvolvimento da personalidade do seu titular, garantindo a este o poder de determinar sobre o uso de suas informações pessoais, a "autodeterminação informativa".

> A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subsequentes leis sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo como protagonista no processo de tratamento de seus dados (MENDES, 2008, p. 48).

A concepção da autodeterminação informativa remota ao próprio direito à privacidade, constitucionalmente tutelado enquanto direto fundamental e direito inerente à personalidade do indivíduo.

Aqui é preciso se ter em mente que o direito à privacidade não se satisfaz na sua dimensão negativa, como ficou conhecido o *right to be alone*[9] (direito de ser deixado só),

---

[8] O original do Julgamento BVERFGE, 65, 1 – 71: "*Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus".*

[9] Definição dada pelo Juiz Thomas McIntyre Cooley (1988) em sua obra *Treatise of the law of torts*.

mas sim na sua dimensão mais ampla, de caráter positivo, “como o direito de se construir uma esfera privada própria, a partir da ideia de livre desenvolvimento da personalidade” (MENDES, 2008, p. 10). Nessa dimensão positiva, o direito à privacidade visa satisfazer a própria dignidade da pessoa humana, na medida em que se confere aos indivíduos autonomia, capacidade de autodeterminação e liberdade.

Nessa perspectiva, Canotilho (2003), em estudo sobre a liberdade e a privacidade em programas de *reality shows*, defende exatamente a ideia de autonomia e liberdade do indivíduo na medida em que “o direito à privacidade consiste na possibilidade de a pessoa controlar, tanto quanto possível a massa de informações sobre si mesma a que outros podem ter acesso” (CANOTILHO, 2003, p. 55-56).

Há, portanto, uma notória proximidade entre o direito à proteção dos dados pessoais e o direito à privacidade, tendo ambos um núcleo comum associado à liberdade e autonomia individual, relativo ao controle do próprio indivíduo sobre suas próprias informações. No entanto, a proteção de dados pessoais, apesar de ter como fundamento o direito à privacidade, ultrapassa o seu âmbito.

> O direito à proteção de dados não se limita à proteção da personalidade humana, sua intimidade e vida privada. A proteção de dados visa permitir gama muito maior de relações, ou, de outra parte, evitar que se criem barreiras para a fruição de todos os direitos e garantias. É fonte de fomento para igualdade social (ROTUNDO, 2017, p. 10).

Enquanto o direito à privacidade foca sua tutela no âmbito de informações relacionadas à intimidade da pessoa, o direito à proteção de dados não se limita a esfera privada. A informação de caráter público do titular também atrai a proteção jurídica conferida aos dados pessoais. Assim, qualquer tipo de cadastro de banco de dados pessoais, mesmo que não envolvam a vida privada da pessoa, será amparado pelo direito a proteção de dados (BIONI, 2019, p. 67):

> Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade. O eixo da privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito. A proteção dos dados pessoais não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob a esfera pública, discutindo-se, apenas, a sua exatidão, por exemplo.

Assim,

> Significa dizer que mesmo os cadastros e bancos de dados formados com dados pessoais que não envolvam aspectos da intimidade e vida privada do indivíduo submetem-se às regras do direito à proteção de dados pessoais. Essa concepção depende, sobretudo, da percepção de que até as informações aparentemente mais inócuas podem ser integradas a outras e provocar danos ao seu titular (ZANON, 2012, p. 147).

E não só, além da diferença entre o caráter privado e/ou público das informações protegidas. O direito a proteção de dados visa também conferir, sob determinado ponto de vista, uma proteção à igualdade, principalmente quando se está diante de dados pessoais sensíveis, que possuem, por sua natureza, um potencial de causar discriminações.

> A igualdade se apresenta como um princípio ameaçado, na medida em que a vigilância realizada por organismos privados e estatais, a partir de informações obtidas em bancos de dados, pode acarretar a classificação e a discriminação dos indivíduos, afetando expressivamente as suas oportunidades sociais (MENDES, 2008, p. 58).

Pense-se, por exemplo, no caso de uma empresa voltada ao recrutamento de pessoas para um emprego e imagine que esta empresa faça uso de bases de bancos de dados de proteção ao crédito para seleção de pessoas que estão concorrendo a um emprego, classificando-as de acordo com um "grau de risco" e as enquadrando em um "grupo social" matematicamente construído.

Esse é um dos casos relatados pela matemática e programadora chefe com passagens em *hedge funds* e *start-ups* nos Estados Unidos, Cathy O'Neil, em *Weapons of math destruction: How big data increases inequality and threatens democracy*, onde demonstra o potencial de construção de perfis ("*profiling*") por meio de bases de dados diversos e como isso influencia e impacta diretamente não só a esfera privada, mas também a esfera social e relacional dos indivíduos, sendo uma ferramenta potencialmente discriminatória (O'NEIL, 2016).

> Sob essa ótica, nota-se a necessidade de que a tutela jurídica dos dados pessoais abranja também a proteção dos cidadãos e não apenas a sua liberdade, como ocorreu majoritariamente nas primeiras normas de proteção de dados. Para tanto, a proteção de dados pessoais deve ser apta a combater a discriminação passível de ocorrer em razão das informações extraídas dos bancos de dados, buscando fornecer uma tutela mais rígida em caso de tratamento de dados sensíveis e de situações potencialmente discriminatórias (MENDES, 2008, p. 59).

Desse modo, é fundamental compreender a disciplina de proteção de dados pessoais para além da proteção à privacidade, devendo-se refletir também na importância da sua tutela como forma de concretizar outros princípios tão caros a qualquer sociedade democrática que tenha como norte a promoção da igualdade.

Por essas razões, não se pode pensar na proteção dos dados pessoais tão somente como decorrência da tutela à privacidade, sustentando a autonomia da sua proteção jurídica, sob pena de limitar o seu conteúdo e a sua necessária abrangência.

A previsão autônoma do direito à proteção dos dados pessoais consta em diversos diplomas, a exemplo da Constituição de Portugal:

> Artigo 35.º (Utilização da informática)
> 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
> 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
> 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
> 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.
> 5. É proibida a atribuição de um número nacional único aos cidadãos.
> 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
> 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei (PORTUGAL, 1976, s.p.).

Além de Portugal, outros ordenamentos jurídicos tutelam expressamente os dados pessoais de seus cidadãos, entendendo-o como projeção da personalidade do indivíduo, a merecer uma tutela constitucional autônoma. Dentre esses países estão Espanha, a Hungria e a Rússia (VIEIRA, 2007).

Legislações infraconstitucionais também visam a proteção desse direito, privilegiando a sua autonomia, a exemplo da GDPR que dispõe: “Artigo 1º [...] 2. Esta regulamentação protege os direitos fundamentais e liberdades da pessoa natural em particular o direito à proteção de dados pessoais” (CONSELHO EUROPEU, 2016, s. p.).

Já no Brasil, a proteção aos dados pessoais ganhou mais destaque com a edição e promulgação da LGPD que no seu primeiro artigo já fixa como objetivos da regulamentação a proteção de direitos fundamentais e o livre desenvolvimento da personalidade:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018, s.p.).

A referida lei prevê também uma série de fundamentos à disciplina da proteção dos dados pessoais, tais como o respeito à privacidade e a autodeterminação informativa, além de expressamente dispor sobre o princípio da não discriminação em seu artigo 6º.

Além da proteção infraconstitucional sobre o tema, há a Proposta de Emenda à Constituição (PEC) nº 17/2019 [10] que pretende incluir entre os direitos e garantias fundamentais a proteção de dados pessoais, alterando o inciso XII do artigo 5º da Constituição da República. Se aprovada, o texto constitucional passará a ser:

> Art. 5º [...] XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (BRASIL, 2019, s. p.).

Nota-se, portanto, o crescente reconhecimento da importância da proteção jurídica autônoma dos dados pessoais enquanto um direito fundamental, o qual foi inclusive ratificado pelo Supremo Tribunal Federal em recente decisão histórica proferida quando referendada uma decisão liminar da Ministra Rosa Weber nas Ações Diretas de Inconstitucionalidade de nº 6387, 6388, 6389, 6393, 6390 propostas em face da Medida Provisória (MP) nº 954/2020, a qual previa o compartilhamento de dados por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para fins de produção de estatística oficial durante a pandemia do coronavírus.

A referida decisão é um marco na tutela dos dados pessoais no ordenamento jurídico brasileiro, ao passo que se traduz no reconhecimento pela Corte Constitucional brasileira da existência deste como direito autônomo, que se diferencia da proteção à intimidade e privacidade, o que pode ser observado em diferentes momentos do julgado, como no voto do Ministro Luiz Fux:

> A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do *habeas data* (art. 5º, LXXII), todos previstos na Constituição Federal de 1988 (BRASIL, 2020, p. 65).

E no voto do Ministro Gilmar Mendes:

> A autonomia do direito fundamental em jogo na presente ADI exorbita, em essência, de sua mera equiparação com o conteúdo normativo da cláusula de proteção ao sigilo. A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da

[10] A PEC nº 17/2019 encontra-se aguardando apreciação pelo Plenário da Câmara dos Deputados, em 18 de julho de 2021.

> proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do *Habeas Data* enquanto instrumento de tutela material do direito à autodeterminação informativa (BRASIL, 2020, p. 109).

Avança-se, então, para uma compreensão constitucional da proteção aos dados pessoais, exigindo não apenas uma postura negativa (de não sofrer intervenção indevida do poder estatal ou privado), mas sobretudo uma postura positiva, na qual cabe ao Estado atuar de forma ativa na proteção desse direito.

3 ASPECTOS GERAIS DA LEGISLAÇÃO – AGENTES DE TRATAMENTO, PRINCÍPIOS E BASES LEGAIS

Superada a compreensão inicial de dados pessoais e feitos breves comentários acerca da sua tutela sob a ótica de um direito fundamental, passa-se a análise dos aspectos gerais da legislação.

3.1 Agentes de tratamento de dados pessoais e o encarregado pelo tratamento de dados pessoais

A legislação brasileira elenca três figuras que estão relacionados a atividade de tratamento de dados pessoais, são: o controlador, o operador e o encarregado. Antes de analisar a responsabilidade civil, é imprescindível delimitar a atividade a cargo de cada um desses sujeitos.

De início, a atividade de tratamento de dados pessoais consiste, nos termos da lei, em "toda operação realizada com dados pessoais", entre as quais se enquadram 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" (BRASIL, 2018, s. p.).

O conceito de tratamento de dados pessoais é, portanto, bem amplo, compreendendo desde a atividade de coleta dos dados até a sua eliminação e arquivamento e aplica-se, por força do artigo 3º da LGPD, a toda operação realizada em território nacional, quando os dados pessoais forem coletados neste, ou, ainda, quando "a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional" (BRASIL, 2018, s. p.).

Essa atividade de tratamento é praticada, essencialmente, por dois sujeitos, o controlador e o operador, que se distinguem de acordo com a função que desempenham.

O controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Ou seja, controlador é aquele que exerce o poder de decisão sobre o tratamento de dados, ao passo que o operador é aquele que irá executar o tratamento em observância às solicitações do controlador, sendo este último, conforme a definição legal, quem "realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018, s. p.).

> Sob uma visão civilista, o controlador seria o mandante, e o operador, o mandatário. Talvez possa se aventar a hipótese de que a relação controlador-operador constitua modalidade especial de mandato, própria das relações que envolvam tratamento de dados pessoais (CAPANEMA, 2020, p. 163).

A definição atribuída pela LGPD tem clara inspiração no Regulamento Geral de Proteção de Dados da União Europeia, o GDPR, que já previa as figuras do *data controller* e do *data processor*, os quais equivalem, respetivamente, ao controlador e ao operador na legislação brasileira.

O guia orientativo elaborado pelo Conselho Europeu de Proteção de Dados (EDPB) ajuda a compreender melhor a atividade de cada um desses sujeitos, definindo o *controller* como aquele que determina os propósitos e meios do processamento dos dados pessoais, determinando o "porquê" e o "como" este se realizará. Isso não significa que caberá ao controlador tomar todas as decisões no curso do tratamento de dados. Alguns aspectos mais práticos da implementação, ditos não essenciais, podem ser deixados a cargo do operador (EUROPEAN DATA PROTECTION BOARD, 2021).

Seguindo a mesma linha, o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, elaborado pela Autoridade Nacional de Proteção de Dados (ANPD), tratando dos pontos essenciais à definição do poder decisório do controlador, dispõe que

> O segundo ponto relevante é a desnecessidade de que todas as decisões sejam tomadas pelo controlador, bastando apenas que este mantenha sob sua influência e controle as principais decisões, isto é, aquelas relativas aos elementos essenciais para o cumprimento da finalidade do tratamento. De fato, especialmente quando há a contratação de um operador, é usual e legítimo que parte das decisões a respeito do tratamento, limitadas aos seus elementos não essenciais, fique sob a alçada do operador. A título de exemplo, podem ser mencionados a escolha dos softwares e equipamentos que serão utilizados e o detalhamento de medidas de prevenção e segurança (BRASIL, 2021, p. 10-11).

Assim, pela própria definição conferida observa-se que o controlador assume uma posição central na atividade de tratamento de dados pessoais, considerando que é o tomador das principais decisões. Como consequência, a responsabilidade pela conformidade do tratamento com a legislação recai sobre ele, cabendo-lhe controlar a finalidade e os meios gerais de como os dados devem ser usados.

> A definição será bastante útil para a responsabilização dos agentes, o que fará com que as empresas em geral delimitem muito bem o papel que desejam assumir no tratamento de dados. Por exemplo: se uma empresa deseja decidir sobre os dados recebidos, assumirá o papel de *Controlador* e responderá diretamente pelos danos causados ao titular, de forma solidária com outros *Controladores* presentes na

> mesma relação. Contudo, se a empresa deseja simplesmente prestar serviços delimitados em contratos comerciais, sem se envolver em processos decisórios quanto ao tratamento, essa empresa se enquadrará na figura do *Operador*, respondendo apenas pelos danos que der causa por descumprimento da lei ou do contrato (OLIVEIRA, 2018, p. 255).

Além da possibilidade do exercício singular da função de controlador, há a possibilidade de controladoria conjunta dos dados pessoais, isto é, quando há dois ou mais controladores na tomada de decisões quanto ao tratamento de dados pessoais.

Embora a LGPD não preveja de forma explicita a possibilidade de controladoria conjunta, pode-se inferir que ela está contemplada no sistema jurídico brasileiro de proteção de dados, considerando que há na lei um dispositivo que trata da responsabilidade solidária quando mais de um controlador estiver diretamente envolvido no tratamento[11].

Assim, valendo-se da influência da GDPR na lei brasileira, regata-se o conceito utilizado por aquele regulamento, para se definir controladoria conjunta:

> Artigo 1º [...] 1. Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13º e 14º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados (EUROPA, 2016, s. p.).

Portanto, haverá controladoria conjunta quando houver participação de duas ou mais entidades na determinação dos objetivos e meios de tratamento dos dados pessoais. Essa participação pode assumir a forma de decisões comuns ou decisões convergentes (EUROPEAN DATA PROTECTION BOARD, 2021).

Todavia, é importante destacar que não se estará diante de uma controladoria conjunta se os objetivos de tratamento forem diferentes, ainda que a base de dados utilizada seja a mesma. É o que ocorre, por exemplo, quando se está diante uma base de dados disponibilizada ao acesso público por uma Agência Reguladora, sendo utilizada por esta para subsidiar decisões administrativas. Enquanto, de outro lado, uma Organização da Sociedade Civil utiliza essa mesma base para realização de ações voltadas às suas finalidades. Nesse caso, apesar de se valerem da mesma base de dados, não há uma finalidade comum ou

[11]"Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: (...) II - **os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente**, salvo nos casos de exclusão previstos no art. 43 desta Lei." (BRASIL, 2018, s. p.) (grifo nosso).

convergente no tratamento realizado por cada uma das entidades. Serão, portanto, controladoras singulares, respondendo cada uma pelos respectivos tratamentos realizados (BRASIL, 2021).

Por fim, há um terceiro sujeito nessa relação jurídica, o encarregado, que, diferentemente dos demais, não desempenha um papel direto na atividade de tratamento de dados.

O encarregado atua na função de intermediação entre os demais atores, é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (BRASIL, 2018, s. p.).

Apesar de trazer o conceito de encarregado, a LGPD não estabeleceu critérios quanto a obrigatoriedade da indicação do encarregado, nem tampouco se o encarregado deve ser pessoa física ou jurídica, ou se deve ser pertencente ou não ao quadro de colabores do controlador. Tal tarefa ficou a cargo da ANPD, que "poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação" (BRASIL, 2018, s. p.).

No que se refere a responsabilidade do encarregado, como regra geral, ela inexiste. Apenas o controlador e o operador, no âmbito de suas atividades, devem garantir e demonstrar que o tratamento de dados pessoais está de acordo com a legislação (MALDONADO; BLUM, 2018, p. 315-316).

3.2 Princípios informadores do tratamento de dados pessoais

Além da definição de tratamento de dados pessoais e dos seus sujeitos, a LGPD elenca também os princípios informadores dessa atividade, os quais tem a importante função de legitimar o tratamento de dados desenvolvido.

O artigo 6º indica, assim, onze princípios que vão orientar a atividade de tratamento de dados pessoais, são eles a: (i) boa-fé; (ii) finalidade; (iii) adequação; (iv) necessidade; (v) livre acesso; (vi) qualidade dos dados; (vii) transparência; (viii) segurança; (ix) prevenção; (x) não discriminação; e (xi) responsabilização e prestação de contas (BRASIL, 2018).

O princípio da boa-fé, previsto no *caput* do artigo 6º, é um antigo conhecido do ordenamento jurídico brasileiro e se trata de princípio que disciplina amplamente as relações jurídicas, sejam elas de direito público sejam de direito privado. A boa-fé é um postulado que

orienta a conduta das partes, exigindo-se destes uma conduta de cooperação e lealdade, relacionando-se à existência de deveres anexos (TARTURCE, 2017).

No âmbito específico do tratamento e da proteção dos dados pessoais, a boa-fé, além de ditar deveres de conduta, vai respaldar a tutela da legítima expectativa do titular em face do controlador e do tratamento empregado por este, a qual é concebida diante das circunstâncias concretas em que se deu o consentimento e a finalidade que o respaldou (MIRAGEM, 2019).

Assim, intrinsecamente interligado ao princípio da boa-fé está o princípio da finalidade, o qual diz respeito aos propósitos legítimos, específicos, explícitos e informados ao titular que fundamentam a realização do tratamento dos dados. Ou seja, pelo princípio da finalidade o tratamento de dados pessoais fica vinculado à finalidade que motivou e justificou a coleta dos dados inicialmente. Isso significa que o tratamento estará sempre associado a uma determinada função, que a legitimará e sempre poderá ser avaliada, conferindo ao titular meio de controle efetivo da utilização do seu dado pessoal (MENDES; DONEDA, 2018).

> 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 (MIRAGEM, 2019, p. 6).

Na sequência a LGPD trás os princípios da adequação e da necessidade, os quais dialogam também com o princípio da finalidade, sendo a adequação a "compatibilidade do tratamento com as finalidades informadas ao titular" e a necessidade a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades" (BRASIL, 2018, s. p.).

Assim, enquanto o princípio da adequação "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" (MIRAGEM, 2019, p. 9), o princípio da necessidade relaciona-se a restrição ao uso dos dados pessoais de forma a rechaçar o uso excessivo e desnecessário à finalidade que se encontra vinculado o tratamento.

Os princípios do livre acesso, da qualidade dos dados e da transparência, previstos nos incisos IV, V e VI do artigo 6º da lei, são definidos enquanto garantias dos titulares dos dados relativas, respectivamente, ao acesso fácil e gratuito ao tratamento e integralidade dos dados, à exatidão, clareza e atualização dos dados; e às informações claras, precisas e acessíveis sobre a realização do tratamento e sobre os agentes envolvidos.

Por fim, os princípios da segurança, prevenção, não discriminação e responsabilização e prestação de contas, em que se pese também constituírem também garantias aos titulares dos dados pessoais, possuem conteúdo que se volta a, principalmente, orientar e ditar deveres e condutas para atuação dos sujeitos do tratamento de dados pessoais.

No tocante ao princípio da segurança, exige-se do controlador e do operador "a 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" (BRASIL, 2018, s. p.). Isto é, exige-se um dever geral de segurança a ser cumprido mediante a adoção das técnicas adequadas.

> 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. (MIRAGEM, 2019, p. 12-13).

O princípio da prevenção, por sua vez, fundamenta-se no reconhecimento de que o tratamento de dados pode gerar riscos aos titulares e, por essa razão, os responsáveis devem adotar medidas que sejam aptas a prevenir a ocorrência de danos.

Nesse aspecto, a prevenção vincula a atividade de tratamento desde a concepção dos sistemas de coleta de dados pessoais, o qual será pautado no *privacy by design* (MIRAGEM, 2019). Desenvolvido pela canadense Ann Cavoukian, a ideia de *privacy by design* baseia-se na incorporação de salvaguardas de privacidades em todos os projetos desenvolvidos por uma organização. Integra, portanto, uma ideia de governança adequada dos dados pessoais.

Por último, os princípios da não discriminação e da responsabilização e prestação de contas informam sobre a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018, s. p.) e sobre o dever dos agentes em demonstrar a observância às normas de proteção e a adoção de medidas eficazes ao seu cumprimento.

3.3 Bases legais para o tratamento dos dados pessoais

Além dos princípios explícitos que orientam a atividade de tratamento de dados, a LGPD elenca também as hipóteses que autorizam o tratamento de dados pessoais, são as

chamadas bases legais. Isso significa que o tratamento de dados para ser legítimo e lícito, deverá se amoldar a pelo menos uma dessas hipóteses previstas nos artigos 7º, 11 e 23.

Destrinchando os dispositivos legais, observa-se que enquanto o artigo 7º prevê as hipóteses gerais para o tratamento de dados, enquanto os artigos 11 e 23 tratam das hipóteses para tratamentos específicos, seja para o tratamento de dado pessoal sensível (artigo 11), seja para o exercício das competências e cumprimento de atribuições legais da Administração Pública (artigo 23). Para esse estudo, importará apenas as previsões legais dos artigos 7º e 11 que dizem respeito ao regime jurídico próprio das relações privadas.

Desse modo, inaugurando as hipóteses autorizativas do tratamento de dados está o consentimento fornecido pelo titular. Essa base legal recebeu tutela destacada na LGPD, que tem como norte a proteção a direitos fundamentais e o livre desenvolvimento da personalidade da pessoa natural[12]. Mas vale lembrar que não há hierarquia entre as hipóteses legais, devendo a opção por aquela que irá se utilizar no caso em concreto se basear no que se mostrar mais adequada e eficiente para a finalidade a que se propõe o tratamento (TEFFÉ; VIOLA, 2020).

> O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele promove a personalidade, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações (TEFFÉ; VIOLA, 2020, p. 7).

O consentimento é definido pela LGPD enquanto "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018, s. p.). Portanto, o consentimento para ser válido e eficaz deve corresponder a uma manifestação expressa, clara e não viciada de vontade, na qual o titular tem acesso adequado e transparente sobre as informações e implicações do tratamento de dados.

Além do consentimento, é autorizado o tratamento de dados para o cumprimento de obrigação legal ou regulatória pelo controlador. Essa base inclui obrigações impostas pelo próprio ordenamento brasileiro, como obrigações trabalhistas, por exemplo, como por outros ordenamentos, permitindo que a LGPD não entre em conflito com outras leis (BURKART, 2021, p. 47).

---

[12] "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o **objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**." (BRASIL, 2018, s. p.) (grifo nosso).

Pode-se também tratar dados, nos termos do artigo 7º, IV, “para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais” (BRASIL, 2018, s. p.). Esta base legal possibilita que estudos sejam realizados por órgãos de pesquisa com dados pessoais, ressalvando, porém, a necessidade de anonimização dos dados de forma a garantir a privacidade dos titulares de dados.

Outra hipótese autorizativa é o tratamento de dados para a execução de obrigações contratuais, nas quais se incluem as relativas à fase pré-contratual, a qual o titular seja parte (artigo 7º, V). Assim, enquanto durar o contrato, o controlador poderá manter os dados fornecidos pelo titular que sejam necessários para a sua regular execução.

Na sequência, o inciso VI trata do exercício regular de direitos em processo judicial, administrativo ou arbitral no tratamento de dados, de forma a permitir o uso de dados pessoais para instrução de processos, assegurando, em última instância, a ampla defesa e o contraditório nos processos em geral (TEFFÉ; VIOLA, 2020, p. 26).

No rol das hipóteses autorizativas, encontram-se ainda bases legais que visam a proteção da vida, da incolumidade física do titular ou de terceiro e a tutela da saúde, previstas nos incisos VII e VIII do artigo 7º.

A penúltima base é a do legítimo interesse do controlador e do terceiro (artigo 7º, IX), o qual tem por objetivo possibilitar o tratamento de dados de acordo com o escopo de atividades praticadas pelo controlador. A flexibilidade dessa base legal encontra freio nas expectativas, na finalidade e necessidade do tratamento e na proporcionalidade da utilização dos dados do titular (TEFFÉ; VIOLA, 2020).

> Mostrar que há um interesse legítimo significa que o controlador (ou um terceiro) deve ter algum benefício ou resultado claro e específico em mente. Não basta afirmar a existência de interesses comerciais vagos ou genéricos. Deve-se pensar detalhadamente no que se está tentando alcançar com a operação de tratamento específica. Embora determinado objetivo possa ser potencialmente relevante, ele deverá ser "legítimo". Qualquer interesse ilegítimo, antiético ou ilegal não será um interesse legítimo para a LGPD (TEFFÉ; VIOLA, 2020, p. 15).

Por fim, a última base legal prevista para o tratamento de dados não sensíveis refere-se à proteção do crédito. Por meio da qual autoriza-se expressamente a utilização e tratamento de dados relativos ao seu comportamento de crédito, nível de comprometimento de renda, eventuais situações de inadimplemento, histórico de pagamento, entre outras informações hábeis a permitir a análise do risco do crédito.

No caso das hipóteses de tratamento de dados sensíveis, muitas vezes as bases se confundem e se repetem, mas diferentemente do tratamento dos dados pessoais *strictu sensu*,

para o tratamento dos dados pessoais sensíveis, as hipóteses se apresentam mais restritas exigindo quase sempre requisitos específicos.

Nesse sentido, o consentimento, previsto no inciso I do artigo 11, se apresenta enquanto um consentimento qualificado, sendo necessário que o titular consinta de forma específica e destacada para finalidades específicas.

As demais bases legais de tratamento dizem respeito ao cumprimento de obrigação legal, à realização de estudos por órgão de pesquisa, ao exercício regular de direito (execução de contratos e para instrução de processos), à proteção da vida, da incolumidade física, à tutela da saúde e à garantia da prevenção à fraude e à segurança do titular, conforme as alíneas do inciso II do artigo 11 da LGPD.

4 RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

A responsabilidade civil encontra-se regulamentada na Seção III do Capítulo VI da LGPD, intitulada de “Da Responsabilidade e do Ressarcimento de Danos”. Nessa seção serão dispostas as regras de incidência de responsabilidade, solidariedade, inversão do ônus da prova e excludentes, sobre as quais se tratará a seguir.

De antemão, entretanto, é imprescindível a compressão acerca do regime jurídico específico da responsabilidade na tutela da proteção dos dados pessoais.

4.1 Regime jurídico

No direito brasileiro a responsabilidade civil pode ser analisada sob a ótica de dois regimes, o da responsabilidade civil subjetiva e o da responsabilidade civil objetiva, os quais se diferenciam pela necessidade ou não de demonstração de culpa do agente.

De um modo geral, para a configuração do dever de indenizar, deve existir, cumulativamente: (i) ação ou omissão jurídica relevante; (ii) nexo causal; e (iii) dano. Esses elementos são comuns aos dois regimes jurídicos de responsabilização. Porém, enquanto a responsabilidade civil subjetiva exige a demonstração de culpa do agente – aqui compreendida enquanto culpa *latu sensu*, em que está inserido o dolo e a culpa *strictu sensu* –, a responsabilidade civil objetiva fundamenta-se no risco inerente à atividade praticada.

No que tange ao regime jurídico adotado pela LGPD, a legislação não estabeleceu de forma expressa a opção por um ou outro, o que tem gerado um intenso debate doutrinário. Enquanto parte da doutrina afirma haver um sistema baseado na responsabilidade objetiva, outros defendem a adoção do regime de responsabilidade subjetiva.

Para os que defendem que o regime adotado é o da responsabilidade civil objetiva, o cerne da questão estaria no risco da atividade desenvolvida e na maior proteção do direito fundamental dos titulares dos dados pessoais.

> Essas limitações ao tratamento de dados, conjuntamente com a verificação de que a LGPD assume como regra a eliminação dos dados quando seu tratamento esteja encerrado (art. 16) e igualmente o aceno que faz em diversas oportunidades à necessidade de se levar em conta o risco presente no tratamento de dados, indicam que a Lei procura minimizar as hipóteses de tratamento àquelas que seja, em um sentido geral, úteis e necessárias, e que mesmo estas possam ser limitadas quando da verificação de risco aos direitos e liberdades do titular de dados. Trata-se, dessa forma, de uma regulação que tem como um de seus fundamentos principais a diminuição do risco, levando-se em conta que o tratamento de dados apresenta risco intrínseco aos seus titulares.

> Assim justifica-se o legislador optar por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação de reparação ao dano no exercício de atividade de tratamento de dados pessoais (MENDES; DONEDA, 2018, p. 477).

Desse modo, sendo a atividade de tratamento de dados potencialmente lesiva aos titulares dos dados pessoais ante os riscos a ela inerentes, a LGPD reclamaria uma interpretação que fosse coerente e sistemática com o ordenamento jurídico e em especial com o Código Civil, o qual, em seu artigo 927, parágrafo único[13], adotou a teoria da responsabilidade objetiva baseada no risco da atividade exercida (NOVAKOSKI; NASPOLINI, 2020).

Em complemento, sustenta-se que o fato de a legislação ter prescrito no artigo 43 as hipóteses excludentes de responsabilidade para os atos cometidos pelos agentes de tratamento, levaria também a conclusão da adoção do regime objetivo de responsabilidade, ou seja, para a aferição do dever reparatório não se analisaria culpa e os agentes somente seriam isentos de responsabilidade quando ocorresse qualquer das hipóteses previstas pela Lei (DIVINO; LIMA, 2020).

Contrapondo-se a esse raciocínio, os doutrinadores que afirmam que a legislação teria elegido o regime subjetivo de responsabilidade fundamentam a sua linha de pensamento com base em interpretações sistemática, teleológica e histórica da LGPD (TASSO, 2020).

Da interpretação sistemática, Tasso (2020) elucida que o legislador sempre que excepciona a regra da responsabilidade subjetiva, o faz de forma expressa, o que não ocorreu na LGPD. Não há na Lei nenhuma expressão que indique de modo inequívoco a adoção pelo regime da responsabilidade independente de culpa.

Além disso, a Lei institui diversos deveres aos agentes de tratamento de dados, tendo o legislador estabelecido um *standard* de conduta a esses agentes. Portanto, seria um contrassenso se fosse imputado aos agentes a responsabilidade pela reparação decorrente de incidente que tenha ocorrido ainda que em observância a todos os deveres impostos (TASSO, 2020). Nesse sentido, a parte relativa à "segurança e boas práticas", prevista em capítulo próprio, reforça a existência de um juízo de valor em torno da conduta do lesante (BIONI; DIAS, 2020).

Uma interpretação dos dispositivos previstos na seção dedicada à responsabilidade civil nas relações de direito privado também levaria a conclusão da necessidade de comprovação de culpa para a responsabilização dos agentes. Para tanto, a

[13] "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. **Haverá obrigação de reparar o dano, independentemente de culpa**, nos casos especificados em lei, ou **quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.**" (BRASIL, 2002, s. p.) (grifo nosso)

análise da excludente de responsabilidade prevista no inciso II do artigo 43[14] e da hipótese de responsabilização constante no parágrafo único artigo 44[15], permitem, de igual modo, concluir que para a responsabilização dos agentes é necessário a infringência de um dever originário, afastando a conclusão da responsabilização pela simples ocorrência do dano (TASSO, 2020, p. 109).

> Em vez de simplesmente espelhar as excludentes do CDC, o legislador optou por eximir a responsabilização dos agentes de tratamento de dados caso comprovem "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II). Da mesma forma, quando a LGPD dispõe sobre a responsabilidade civil pela violação à segurança dos dados, há ressalva de que tal responsabilização somente é deflagrada se não foram adotadas as "medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação". Trata-se de elementos que afastam a aplicação do sistema de responsabilidade civil objetiva (BIONI; DIAS, 2020, p. 7).

Pela interpretação teleológica se extrairia que a finalidade da norma seria não apenas a proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade enunciado no artigo 1º da LGPD, mas também o desenvolvimento econômico e tecnológico, com o prestígio à inovação, à livre iniciativa e à livre concorrência.

Essas finalidades seriam desprestigiadas com a adoção como regra do sistema de responsabilidade civil objetiva, uma vez que esvaziaria a força normativa das normas que preveem os deveres de proteção, prevenção e segurança impostos aos agentes de tratamento, e, de igual forma, desestimularia o desenvolvimento econômico baseado na circulação e tratamento de dados (TASSO, 2020).

A interpretação histórica, por sua vez, remonta aos processos de alteração e elaboração das propostas legislativas que deram origem à LGPD. Analisando a evolução do texto normativo, é possível se observar um abandono deliberado do regime objetivo de responsabilidade, retirando-se da redação final da Lei as expressões que aludiam a responsabilização independente de culpa (BIONI; DIAS, 2020).

---

[14] "Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: (...) **II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;**" (BRASIL, 2018, s. p.) (grifo nosso).

[15] "Art. 44. 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: (...) Parágrafo único. **Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano**." (BRASIL, 2018, s. p.) (grifo nosso).

Portanto, em que se pese a posição divergente, a compreensão sistemática dos dispositivos legais e da intenção do legislador, a qual não pode ser desconsiderada, leva a conclusão da adoção do regime subjetivo de responsabilidade pela LGPD.

Frise-se que a opção por um regime subjetivo da responsabilidade não importa em um desprestígio à proteção de um direito fundamental à proteção de dados. Ao contrário, a Lei ao prever princípios, deveres e obrigações a serem seguidas no tratamento de dados privilegia e protege esse direito, de modo que o desrespeito a essas normas importaram na responsabilização do agente.

Importante ressaltar, ainda, que esse entendimento não irá afastar a aplicação do regime de responsabilidade objetiva nos casos que se estiver diante de uma relação consumerista, considerando a ressalva presente no artigo 45 da Lei[16], que expressamente privilegia o regime jurídico específico do Código de Defesa do Consumidor (CDC).

4.2 Responsabilização civil dos agentes de tratamento de dados na LGPD

A LGPD estabelece duas hipóteses que vão dar ensejo à obrigação de indenizar dos agentes de tratamento de dados: a violação de normas jurídicas e a violação de normas técnicas (CAPANEMA, 2020). Essas duas hipóteses são, ao final, reunidas no *caput* do artigo 44[17] da Lei sob a noção ampla de tratamento irregular (BIONI; DIAS, 2020).

A primeira hipótese encontra-se disposta no *caput* do artigo 42, o qual prevê a responsabilização do controlador ou do operador por violação à legislação de proteção de dados: "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (BRASIL, 2018, s. p.).

Ressalte-se que o artigo faz menção a responsabilidade decorrente de uma conduta que viole a legislação de proteção de dados e não simplesmente a Lei, o que permite inferir que há um reconhecimento do microssistema voltado à proteção dos dados, o que abarca não só as leis que versem sobre o tema – CDC, Marco Civil da Internet, Lei do Cadastro Positivo,

[16] "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente." (BRASIL, 2018, s. p.).

[17] "Art. 44. 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: (...)" (BRASIL, 2018, s. p.).

entre outros – mas também as normas administrativas regulamentares expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades (CAPANEMA, 2020).

A segunda hipótese está prevista no parágrafo único do artigo 44, o qual prevê a responsabilidade quando houver danos decorrentes da não adoção pelos agentes de tratamento de medidas de segurança: "Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano" (BRASIL, 2018, s. p.).

Nesse caso, é essencial delimitar qual o critério que será utilizado para analisar a responsabilidade dos agentes por violação as normas técnicas, o qual é retirado do próprio sentido dos dispositivos normativos da Lei.

Se de um lado, o artigo 44, parágrafo único, em conjunto com o artigo 46[18], preveem a responsabilização pela não adoção de medidas de segurança aptas a proteger os dados pessoais, de outro, o caput do artigo 44 define tratamento irregular (por violação à segurança) quando não for fornecida a segurança que o titular dele pode esperar.

A aparente imprecisão pela verificação de dois critérios, encontra convergência na compreensão de que a responsabilização pela violação às normas técnicas reclama, antes de tudo, a aferição do estado da arte da tecnologia. Assim, as medidas aptas a proteção dos dados e a segurança esperada pelo titular, em última análise, irão ser as que razoavelmente seriam possíveis de serem adotadas, segundo as técnicas conhecidas e disponíveis no momento do tratamento.

Inclusive, nesse sentido, o artigo 44 dispõe, no inciso III, como uma das circunstâncias relevantes para a verificação do tratamento irregular "as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado" (BRASIL, 2018, s. p.).

Além dessa, há mais duas circunstâncias relevantes indicadas pela Lei para a determinação da segurança que o titular médio pode esperar do tratamento de dados e de potencial violação à legislação, quais sejam: o modo de realização do tratamento e o resultado e risco que razoavelmente se pode esperar dele.

> A estrutura normativa da LGPD parte do pressuposto de que haverá uma alta variação do potencial lesivo entre as mais diferentes atividades de tratamento de dados, o que tornará determinante avaliar-se a maneira pela qual estas devem ser executadas e os riscos que delas derivam. (BIONI; DIAS, 2020, p. 15).

[18] "Art. 46. Os agentes de tratamento **devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (BRASIL, 2018, s. p.) (grifo nosso).

Portanto, na definição de tratamento irregular e, consequentemente, da obrigação de reparar eventual dano, deveram ser considerados os aspectos relativos ao modo, ao resultado, ao risco envolvido no tratamento e às técnicas disponíveis para este.

Assim, verificada a ocorrência de uma das hipóteses de responsabilização, enunciadas acima, o(s) agente(s) envolvido(s) deverá(ão) indenizar os danos suportados pelo titular dos dados.

A responsabilidade do controlador e do operador será solidária como forma de assegurar a indenização ao titular dos dados, nos termos do §1º do artigo 42, o qual informa que o operador responderá solidariamente pelos danos causados pelo tratamento de dados quando (i) descumprir as obrigações da legislação de proteção de danos; ou (ii) se desviar das instruções lícitas do controlador, ocasião na qual irá se equiparar ao controlador.

Isso significa que a reparação pode ser exigida diretamente do controlado ou do operador, ou dos dois, uma vez que o cumprimento da Lei e a segurança da atividade é encargo de todos os agentes de tratamento, não importando se um dos agentes está submisso aos comandos do outro.

Além da responsabilidade solidária entre controlador e operador, também serão responsáveis solidariamente os controladores que estiverem atuando sob controladoria conjunta, cuja definição foi tratada no capítulo anterior.

Há, ainda, situações em que os agentes estarão isentos de responsabilização, são as excludentes previstas pelo artigo 43:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018, s. p).

O inciso I vai dispor sobre a situação em que o agente não realizou o tratamento de dados. Essa figura se assemelha a ilegitimidade passiva. Já o inciso II trata da hipótese em que há a ocorrência de um dano, mas não há ilícito por parte do agente; é o caso, por exemplo, de uma decisão automatizada. E, por último, o inciso III é o caso de culpa exclusiva seja do titular seja de terceiro, ou seja, não haveria uma conduta do agente capaz de imputar algum dano (CAPANEMA, 2020).

Analisando as excludentes de responsabilidade verifica-se que há uma presunção legal quanto à autoria do tratamento por parte do agente a quem o tratamento é atribuído e quanto a violação à legislação de proteção de dados ou irregularidade do tratamento, cabendo

prova do contrário pelo agente (BIONI; DIAS, 2020). Caberia, portanto, ao titular dos dados lesado provar a realização do tratamento de dados, o dano sofrido e o nexo causal.

Contudo, esses elementos que ficariam à encargo do titular dos dados podem ser alvo de uma inversão do ônus da prova caso a alegação do titular de dados seja verossímil ou haja hipossuficiência para produção da prova ou quando essa produção importar em um ônus excessivo ao titular, conforme disciplina o §2º do artigo 42 da LGPD. "Como resultado, a vítima não precisará provar nenhum elemento da responsabilidade, ficando a cargo dos agentes de tratamento o ônus de provar a sua não ocorrência." (BIONI; DIAS, 2020).

> É possível concluir, assim, que o regime jurídico da responsabilidade civil estabelecido pela LGPD traz uma erosão bastante significativa dos filtros da responsabilidade civil em favor do titular dos dados. Ainda que o regime seja o de responsabilidade civil subjetiva, a culpa e autoria do agente de tratamento de dados são presumidas e, adicionalmente, pode haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil (BIONI; DIAS, 2020, p. 19).

Portanto, é possível observar que, ainda que se adote a compreensão da assunção da responsabilidade subjetiva no regime da responsabilização dos agentes de tratamento por danos provocados ao titular, este não está desassistido em seu direito fundamental à proteção dos dados pessoais, o qual encontra-se satisfatoriamente preservado por uma legislação que prestigia e o coloca como figura central.

4.3 Fixação do *quantum* indenizatório

Como derradeiro ponto a ser abordado no presente trabalho está a problemática da fixação do valor indenizatório devido ao titular em razão da ofensa ao seu direito fundamental tutelado pela LGPD.

Os dados pessoais normalmente têm conotação patrimonial para os agentes de tratamento, que os utilizam e comercializam, porém, sua apreciação não é mensurável, em regra, para o titular. Em determinados caso, é possível se vislumbrar uma lesão de ordem material, quando se está diante de casos de fraude, por exemplo. Quando o dano ocorre diretamente com lesão ao patrimônio do titular, a indenização será correspondente com a lesão. Porém, na maioria dos casos o dano sofrido será o extrapatrimonial. "Consequentemente, há a dificuldade de reparação que lhe é própria, uma vez que reparar patrimonialmente algo que não tem cunho patrimonial acarreta um problema de origem e de valoração" (GONDIM, 2021).

Sob esse aspecto, o artigo 944 do Código Civil informa que “a indenização mede-se pela extensão do dano” (BRASIL, 2002, s. p.). Ante essa previsão normativa, Capanema (2020) enumera alguns parâmetros para aferir a extensão do dano, são eles: quantidade e natureza de dados pessoais afetados; reincidência da conduta; omissão na adoção de medidas de segurança e técnicas para minorar o dano ou em colaborar com a ANPD; ausência de notificação dos usuários sobre a ocorrência do incidente causador de dano; e, ainda, a eventual utilização dos dados pessoais vazados por terceiros.

Além da extensão do dano, há outros critérios para a quantificação dos danos, tais como a capacidade econômica do ofensor e o caráter pedagógico da reparação.

Inclusive um dos parâmetros que podem e devem ser utilizados para a quantificação dos danos morais suportados, é o valor econômico dos próprios dados utilizados em desconformidade com as normas jurídicas e/ou técnicas. Isso porque será esse o valor parâmetro que será capaz de gerar um desestímulo à conduta do ofensor, já que seria o lucro do ofensor se baseará no valor econômico do dado (GONDIM, 2021).

> São os denominados “ilícitos lucrativos”, quando o valor da condenação é tão ínfimo que, ao calcular o lucro obtido pela conduta (ainda que indevida) e a reparação a ser paga (em caso de condenação), o resultado é de que, economicamente, vale a pena lesar, tal como ocorreu no paradigmático caso Ford Pinto. (GONDIM, 2021, p. 29).

Dessa maneira, de forma a não esvaziar a proteção jurídica dos titulares dos dados pessoais em face de transgressões que lhes causem danos – os quais afetaram, principalmente, a esfera extrapatrimonial destes – deve se observar elementos concretos do caso em questão quando da fixação do valor indenizatório.

5 CONSIDERAÇÕES FINAIS

Ao longo desse trabalho, vislumbrou-se que o dado pessoal ganhou relevância no ordenamento jurídico brasileiro com a edição e promulgação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que veio complementar as normas brasileiras, estabelecendo um regime geral sobre o tema. A Lei surge diante da imprescindibilidade de uma regulamentação internacional e convergente, considerando o crescimento de uma economia digital global, onde as informações não ficam restritas a territórios específicos.

Inspirada no modelo europeu de proteção de dados, amparado essencialmente na GDPR (*General Data Protection Regulation*), o sistema regulatório brasileiro se baseia na proteção do dado pessoal e no reconhecimento desta enquanto um direito fundamental do titular.

Nesse sentido, nos termos da teoria expansionista, a qual foi adotada pela LGPD, a conceituação de dado pessoal, apto a atrair proteção jurídica, passa pela compreensão de que este diz respeito à uma informação relativa a uma pessoa natural identificada ou identificável, onde a potencialidade de identificação tem que ser aferida de acordo com o conjunto constante em uma base de dados específica e observando, ainda, o uso de técnicas que importem em um esforço razoável à sua identificação. A *contrario sensu*, os dados que não digam respeito à uma pessoa identificada ou identificável ou, ainda, que para sua identificação demande um esforço que ultrapasse o razoável, são considerados dados anônimos (ou anonimizados) e estão fora da tutela jurídica da LGPD.

Acertadamente a legislação brasileira atribuiu conceitos dinâmicos à definição de dados pessoais e de dados anônimos, os quais serão calibrados de acordo com o *status* da tecnologia. A flexibilidade conferida pela legislação impede o engessamento da sua aplicação e possibilita uma ampla proteção.

Assim, no âmbito da proteção de dados pessoais, ainda em 1983 da decisão proferida pelo Tribunal Constitucional Federal Alemão já traçava os contornos da tutela de um direito fundamental. Reconhecendo um direito fundamental à autodeterminação informativa, a decisão alemã alçou o indivíduo como protagonista no processo de tratamento de seus dados.

Frise-se que não se pode pensar na proteção dos dados pessoais tão somente como decorrência da tutela à privacidade – ainda que compreendida em sua esfera mais ampla, enquanto um direito de construir uma esfera privada própria, com a capacidade de controle pelo indivíduo sobre as informações sobre si a que outros podem ter acesso. O direito a

proteção de dados visa também conferir uma proteção à igualdade, principalmente quando se está diante de dados pessoais sensíveis, que possuem, por sua natureza, um potencial de causar discriminações. Por essas razões, sustenta-se a autonomia da proteção jurídica dos dados pessoais.

Justamente reconhecendo essa autonomia há a PEC nº 17/2019, a qual pretende incluir de forma expressa entre os direitos e garantias fundamentais a proteção de dados pessoais, e as decisões proferidas pelo STF no âmbito das ADIs nº 6387, 6388, 6389, 6393, 6390.

Compreendido os contornos do bem jurídico objeto de estudo, observou-se que um dos mecanismos de defesa do direito à proteção dos dados pessoais é justamente a possibilidade de responsabilizar civilmente os agentes de tratamento de dados.

O regime de responsabilização civil no âmbito da LGPD não foi estabelecido de forma clara e expressa, o que tem o que tem gerado um intenso debate doutrinário, onde parte da doutrina afirma haver um sistema baseado na responsabilidade objetiva, enquanto outra parte defende a adoção de um regime de responsabilidade subjetiva.

Porém, considerando interpretações sistemática, teleológica e histórica da LGPD, chegou-se a conclusão que o regime adotado foi o da responsabilidade subjetiva, o qual, contudo, não importa em um desprivilegio à proteção do direito do titular, o qual é salvaguardado pelas disposições legais que preveem a possibilidade de responsabilidade solidária, inversão do ônus da prova e enumera de forma taxativa as hipóteses excludentes de responsabilidade.

REFERÊNCIAS

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos jurídicos,** São Paulo, v. 21, n. 53, p. 191-201, Janeiro-Março/2020.

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

BIONI, Bruno Ricardo. **Xeque-mate:** o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI, 2015.

BIONI, Bruno Ricardo; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, v. 9, n. 3, p.1-23, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, DF: [s. n.], 2021. 23 p. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 1 ago. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8727.htm. Acesso em: 28 jun.2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Brasília, DF: Presidência da República, [2002]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8727.htm. Acesso em: 28 jun.2021.

BRASIL, Senado Federal. **Projeto de Emenda Constitucional nº 17 de 2019.** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1564052658848&disposition=inline. Acesso em: 07 ago. 2019.

BRASIL. Supremo Tribunal Federal. **Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387.** Medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. *Fumus boni juris. Periculum in mora* . Deferimento. Relator: Ministra Rosa Weber, 07 de maio de 2020. Disponível: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567. Acesso em: 25 jun. 2021.

BURKART, Daniele Vincenzi Villares. **Proteção de dados e o estudo da LGPD**. 2021. Dissertação (Mestrado em Mídia e Tecnologia) – Faculdade de Artes, Arquitetura e Comunicação, Universidade Estadual Paulista Júlio de Mesquita Filho, São Paulo, 2009. 141 f. Disponível em: http://hdl.handle.net/11449/204091. Acesso em: 15 ago. 2021.

CANOTILHO, José Joaquim Gomes. **"Reality Shows" e Liberdade de Programação.** Portugal: Coimbra, 2003.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos:** Direito Digital e proteção de dados pessoais, São Paulo, v. 21, n. 53, p. 163-170, jan./mar. 2020.

CONSELHO EUROPEU. **Regulamento Geral sobre Proteção de Dados nº 679 de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: https://www.uc.pt/protecao-de-dados/rgpd. Acesso em: 10 jul. 2021.

COOLEY, McIntyre.**Treatise of the law of torts.** Reino Unido: Callaghan, 1988.

DIVINO, Sthéfano Bruno Santos; LIMA, Taisa Maria Macena de. Responsabilidade civil na lei geral de proteção de dados brasileira. **Revista em Tempo**, São Paulo, v. 20, n. 1, p. 201-226, 2020.

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

EUROPEAN DATA PROTECTION BOARD. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR.** Bruxelas, Bélgica, 2021. 51 p. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: 1 ago. 2021.

GONDIM, G. G. A responsabilidade civil no uso indevido dos dados pessoais. **Revista IBERC,** Minas Gerais, v. 4, n. 1, p. 19-34, 9 mar. 2021.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Big Data no projeto Sul Global:** relatório sobre estudos de caso. 2016. Disponível em: https://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf. Acesso em: 10 jul. 2021.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados comentada.** São Paulo: Thomson Reuters Brasil, 2018.

MARTINS, Leonardo. **Cinqüenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevidéu: Fundação Konrad Adenauer, 2005.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data:** como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013.

MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito)- Universidade de Brasília, Brasília, 2008.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120. N. 27. p. 469-483, 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais,** São Paulo, v. 1009, n.2, p. 173-222, nov. 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 11 ago. 2021.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **How to break anonymity of the Netflix.** 2007. Disponível em: https://goo.gl/RxggOU. Acesso em 11 jul. 2021.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade civil na LGPD: problemas e soluções. **Conpedi Law Review**, Florianópolis, v. 6, n. 1, p. 158-174, 2020.

OLIVEIRA, Ricardo Alexandre de. Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico. **Revista dos Tribunais,** São Paulo, v. 998, n. 107, p. 241-261, 2018.

O'NEIL, Cathy. **Weapons of math destruction**: How big data increases inequality and threatens democracy. Nova Iorque: Broadway Books, 2016.

PORTUGAL. **Constituição da República Portuguesa.** Defende a independência nacional, garante os direitos fundamentais dos cidadãos, estabelece os princípios basilares da democracia e assegura o primado do Estado de Direito democrático. Lisboa: Assembleia da República, 1976. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:1989;000185347. Acesso em: 11 jul. 2021.

ROTUNDO, Rafael Pinheiro. **Proteção de dados.** São Paulo: Revista dos Tribunais, 2017.

SCHWARTZ, Paul M.; SOLOVE, George Washington. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. **New York University Law Review,** New York, v. 86, n. 2, p. 1814-1823, 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366. Acesso em: 22 ago. 2021.

SRNICEK, Nick. **Plataform capitalism.** Cambridge: Polity Press, 2018.

TARTUCE, Flávio. **Manual de direito civil**: volume único. 7 ed. Rio de Janeiro: Forense, 2017.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, v. 9, n. 1, p. 1-38, 2020.

TENE, Omer. Privacy law's midlife crisis: a critical assessment of the second wave of global privacy laws. **Ohio State Journal**, Columbus, v. 74, n. 6, p. 127-1262, 2013.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito)-Universidade de Brasília, Brasília, 2007.

ZANON, João Carlos. **Direito à Proteção dos Dados Pessoais.** Dissertação (Mestrado em Direito). PUCSP, 2012.