

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

Bruno BIONI*

Daniel DIAS**

RESUMO: A doutrina brasileira tem focado a sua atenção em responder essencialmente uma pergunta: se o regime da responsabilidade é objetivo ou subjetivo. Por mais relevante que isso seja, não é essa questão que deve pautar o debate. Tal pergunta parece partir de uma premissa falsa de dualidade de regimes jurídicos de responsabilidade, objetiva ou subjetiva. Mais importante do que essa tentativa de classificação binária de responsabilidade, se objetiva ou subjetiva, é analisar mais de perto e, em detalhes, os elementos normativos que restringiriam ou alargariam a discussão de culpabilidade para fins de responsabilização no tratamento de dados pessoais. Ainda que a LGPD tenha esculpido um regime de responsabilidade civil subjetiva, as barreiras para a deflagração do dever de indenizar foram substancialmente diminuídas.

PALAVRAS-CHAVE: Responsabilidade civil; Lei Geral de Proteção de Dados; dano; culpa; Código de Defesa do Consumidor.

SUMÁRIO: 1. Introdução e apontamentos metodológicos; – 2. A (in)evolução do texto da LGPD: o papel da culpa na definição do regime de responsabilidade civil; – 3. Responsabilidade em caso de “violação à legislação de proteção de dados pessoais” e de “violação da segurança dos dados”; – 3.1. Tratamento irregular; – 3.1.1. Dubiedade de critérios quanto à violação à segurança dos dados: medidas aptas (art. 44. parágrafo único) *versus* a segurança que dele se pode esperar (art. 44, II); – 3.1.2. Inobservância da legislação e o não fornecimento da segurança esperada: o conceito de “legítimas expectativas de segurança”; – 3.1.3. Circunstâncias relevantes: conectando o artigo 43 ao 50 da LGPD para um juízo de culpa caso a caso; – 3.1.4. Circunstâncias relevantes: as técnicas de tratamento de dados disponíveis à época (inciso III do artigo 43); – 3.2. Pressupostos de responsabilidade e inversão do ônus da prova; – 3.3. Obrigação de meio *versus* obrigação de resultado; – 4. Conclusão.

TITLE: *Liability in Data Protection: Building Bridges between the Brazilian General Data Protection Law and the Consumer Protection Code*

ABSTRACT: *Brazilian doctrine has focused its attention on essentially one question: whether the liability regime is objective or subjective. As relevant as this may be, it is not the issue which should guide the debate. Such a question lies on the false premise of dual legal regime of liability, objective or subjective. More important than that is to analyze more closely and, in detail, the normative elements that may restrict or broaden the discussion of culpability for the purposes of accountability in the processing of personal data. Although the Brazilian data protection law has created a regime of subjective liability, the barriers to the duty to indemnify have been substantially reduced.*

* Doutorando em Direito Comercial e Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo (USP). Foi pesquisador visitante do European Data Protection Board e do Departamento de Proteção de Dados do Conselho da Europa Professor e Fundador do Data Privacy Brasil.

** Professor da FGV Direito Rio. Doutor em Direito Civil pela USP (2013-2016), com períodos de pesquisa na Universidade *Ludwig-Maximilians* de Munique e no Instituto Max-Planck de Direito Comparado e Internacional Privado, na Alemanha (2014-2015). Estágio pós-doutoral na *Harvard Law School*, nos EUA (2016-2017).

KEYWORDS: *Liability; data protection; harm; culpability; Consumer Protection Code.*

CONTENTS: *1. Introduction and methodological notes; – 2. The (non) evolution of the Brazilian data protection law: the role of culpability in the definition of the liability regime; – 3. Liability in the event of “breach of legislation” and “breach of security”; – 3.1. Irregular treatment; – 3.1.1. Dubious criteria regarding the breach of security: apt measures (art. 44.) versus the security that can be expected (art. 44, II); – 3.1.2. Non-compliance with legislation and failure to provide the expected security: the concept of “legitimate security expectations”; – 3.1.3. Relevant circumstances: connecting Article 43 to Article 50 of the Brazilian data protection law for a case-by-case judgment of culpability; – 3.1.4. Relevant circumstances: the data processing techniques available at the time (item 43 of Article 43); – 3.2. Assumptions of liability and the burden of proof; – 3.3. Obligation of means versus obligation of result; – 4. Conclusion.*

1. Introdução e apontamentos metodológicos

A Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/2018), estabeleceu¹, pela primeira vez no ordenamento jurídico brasileiro, um conjunto de normas – regras e princípios – vocacionados² a regular o tratamento de dados pessoais em todas as atividades do cotidiano do cidadão, abarcando, assim, todos os setores da economia.

O impacto desse tipo de reconfiguração do sistema jurídico tem sido comparado à repactuação do próprio contrato social.³ Afinal, atualmente, as pessoas são julgadas e avaliadas com base no que seus dados pessoais dizem em todos os âmbitos da sua vida. Do acesso a programa de transferência de renda ao de linha de crédito, essas oportunidades sociais são filtradas pelo processamento de seus dados.

Diante dos riscos que todo esse impacto representa aos indivíduos, um dos objetivos da lei foi justamente delimitar as obrigações dos agentes de tratamento de dados e, com isso, fixar regime jurídico para sua responsabilização.⁴ É inevitável que nesse “admirável novo mundo”, cheio de riscos,⁵ experimentar-se-á efeitos colaterais que

¹ A LGPD inaugurou uma nova lógica, que busca regular uma ordem informacional, algo que não havia antes de forma tão sistematizada e harmônica. Ver: SCHERTEL, Laura Mendes. *Palestra “Seminário Internacional – Lei Geral de Proteção de Dados: a caminho da efetividade”*. Superior Tribunal de Justiça, 2019. Disponível em: <<https://www.youtube.com/watch?v=oEoUSaGQ6h8>>. Acesso em: 01 maio 2020.

² BIONI, Bruno Ricardo. *País precisa ser competitivo em uma economia de dados*. *Valor Econômico*, 19 jul. 2018.

³ BIONI, Bruno Ricardo. *Nota do coordenador*. *Revista do Advogado*, n. 144, nov., 2019.

⁴ SCHERTEL, Laura Mendes; DONEDA, Danilo. *Reflexões iniciais sobre a nova lei geral de proteção de dados*. São Paulo: *Revista dos Tribunais*, 2018, vol. 120, p. 469–483.. Os autores afirmam ser possível identificar outros quatro eixos: (i) unidade e generalidade da aplicação da lei, (ii) legitimação para o tratamento de dados, (iii) princípios e direitos do titular e (iv) obrigações dos agentes de tratamento de dados.

⁵ MIRAGEM, Bruno. *A internet das coisas e os riscos do admirável mundo novo*. *Consultor Jurídico*, 29 mar. 2017.

deverão ser compensados e, preferencialmente, prevenidos.⁶ A esse respeito, a seção sobre responsabilidade e ressarcimento de danos (seção III, do capítulo VI, da LGPD) desafia um exercício difícil de dogmática jurídica.

A doutrina brasileira tem, nesse primeiro momento, focado a sua atenção para responder essencialmente uma pergunta: se o regime da responsabilidade é objetivo ou subjetivo.⁷ Entendemos que, por mais relevante que isso seja, não é essa questão que deve pautar o debate. Por tratar-se de questão que parece partir de uma premissa falsa de dualidade⁸ de regimes jurídicos de responsabilidade, se objetiva ou subjetiva. Na verdade, há diversos modelos e, mesmo entre aqueles que são supostamente de responsabilidade objetiva, nem por isso são idênticos.⁹ Mais importante, portanto, do que essa tentativa de classificação binária de responsabilidade, é analisar mais de perto e, em detalhes, os elementos normativos que restringiriam ou alargariam a discussão de culpabilidade para fins de responsabilização. É o que se pretende fazer no presente artigo, o qual assume uma abordagem exploratória, de primeiras impressões, e que busca compreender qual é a racionalidade jurídica¹⁰ subjacente ao regime de responsabilidade civil contido na LGPD.

⁶ COSTA, Luiz. *Privacy and the precautionary principle*. Computer Law & Security Review, vol. 28, 2012, 14-24.

⁷ Ver, em especial: GUEDES, Gisela Sampaio da Cruz. *Regime de responsabilidade adotado pela lei de proteção de dados brasileira*. São Paulo: Revista dos Tribunais, nov. 2019, p. 167-182, um dos mais extensos sobre a matéria, visa essencialmente responder a essa pergunta. Ver também: ZANATTA, Rafael A. F. *Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor*. In: Coletânea do Instituto de Tecnologia e Sociedade sobre a Lei Geral de Proteção de Dados Pessoais. São Paulo, Revista dos Tribunais, 2019, no prelo; 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*. In: Cadernos Jurídicos – Direito digital e proteção de dados pessoais. São Paulo: Escola Paulista de Magistratura, ano 21, n. 53, jan.-mar. 2020.

⁸ Exceção feita à Caitlin Sampaio Mulholland, que se orienta por três sistemas de responsabilidade civil na LGPD. Ver: MULHOLLAND, Caitlin Sampaio. *Palestra no Webinar IBERC #2 – A Responsabilidade Civil na Lei Geral de Proteção de Dados*. Instituto Brasileiro de Estudos em Responsabilidade Civil – IBERC, 19 set. 2019.

⁹ A respeito da responsabilidade objetiva ou pelo risco, António Menezes Cordeiro afirma: “Numa leitura simplista, poder-se-ia afigurar que a responsabilidade pelo risco, nas suas várias concretizações, se reconduziria a uma responsabilidade delitual, mas sem os requisitos da culpa e da ilicitude. Não é, de todo, assim. A responsabilidade civil traduz, em cada uma das suas manifestações típicas, um modelo complexo. Os seus diversos pressupostos interagem uns com os outros, de tal modo se alterar (?), adaptando-se ao conjunto. Ainda quando conservem uma identidade linguística, já não são os mesmos, obrigando a uma reconstrução, modelo a modelo”. (CORDEIRO, António Menezes. *Tratado de direito civil português*, vol. II, t. III: gestão de negócios, enriquecimento sem causa, responsabilidade civil. Coimbra: Almedina, 2010, p. 597). Por exemplo, no caso da responsabilidade por fato de terceiro, trata-se de responsabilidade objetiva – os responsáveis respondem “ainda que não culpa de sua parte” (art. 933, CC). Nessa modalidade de responsabilidade objetiva não se exige nada dos responsáveis elencados no art. 932, CC além do vínculo com o lesante (pais e filhos, ou empregadores e empregados, entre outros). No caso da responsabilidade por fato do produto ou do serviço, apesar de tratar-se de responsabilidade também objetiva – “independentemente da existência de culpa”, como dizem os arts. 12 e 14, caput, do CDC –, para que haja responsabilização, o legislador exige o pressuposto especial do defeito relativo ao produto ou ao serviço (arts. 12 e 14, CDC).

¹⁰ CORDEIRO, A. Barreto Menezes. *Repercussões do RGPD sobre a responsabilidade civil*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coords.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019, pp. 779.

O artigo está dividido em 03 (três) partes. A primeira, na linha de outros trabalhos,¹¹ faz uma análise histórica do texto da LGPD, abrangendo, inclusive, dispositivos para além daqueles diretamente ligados à responsabilidade civil. Desta forma, o objetivo foi desvendar se a estrutura normativa da LGPD estimula ou desincentiva a discussão de culpa. A segunda propõe-se a analisar alguns elementos normativos em específico, os quais são centrais para desvendar qual será o espaço ocupado pela culpa no regime jurídico firmado na LGPD. Em especial, se as obrigações atribuídas aos agentes de tratamento de dados são de meio ou de resultado e, de forma ainda mais detida, os incisos do artigo 44 que traçam parâmetros de aferição em torno da reprovabilidade da conduta danosa. A terceira é uma espécie de colagem das duas anteriores onde se tecem conclusões e reflexões em torno da racionalidade jurídica do regramento da LGPD para a responsabilização dos agentes de tratamento de dados.

A hipótese deste trabalho considera que há uma espécie de *gradiente* que pode ser um filtro ou um catalisador da culpa enquanto um dos pressupostos da responsabilidade civil. Ao qualificar de forma intensa quais são as obrigações dos agentes de tratamento de dados, e, ainda, ao traçar parâmetros com alta vagueza normativa para mensurar a reprovabilidade de uma conduta danosa, há uma considerável margem interpretativa para que a culpa exerça, ao final, um papel na determinação da responsabilidade civil dos agentes de tratamento. Dessa forma, a principal contribuição do artigo é mapear quais são tais elementos normativos e, com isso, extrapolar uma falsa dualidade entre regimes de responsabilidade civil subjetiva ou objetiva como sendo o cerne da dogmática do regime jurídico de responsabilidade civil formatado na LGPD.

2. O processo de elaboração da LGPD e o papel da culpa no regime de responsabilidade civil

Foram quase dez anos de debate para que se chegasse à redação atual da LGPD.¹² Permeados por ricos debates públicos e algumas disputas de poder, eles deixaram pistas hermenêuticas valiosas e possibilidades analíticas a partir dos trabalhos preparatórios da lei. Nesse sentido, merece destaque a forte disputa em torno da definição do modelo de regime de reponsabilidade civil, tanto em torno da seção diretamente dedicada ao tema, como também, de outros elementos normativos que

¹¹ ZANATTA, op. cit., no prelo; TASSO, op. cit.

¹² Sobre isso: DATA PRIVACY BRASIL. Memória da LGPD. Observatório da Privacidade e Proteção de Dados Pessoais. Disponível em <<https://observatorioprivacidade.com.br/memorias/>>.

indiretamente calibram o regime jurídico da reponsabilidade no tratamento de dados pessoais.¹³

Quanto a esse primeiro caso, é importante destacar: a) o abandono deliberado do regime de responsabilidade civil objetiva; e b) a adoção de técnica legislativa mais prescritiva quanto às excludentes de reponsabilidade civil.

Tanto a primeira versão do anteprojeto da lei de proteção de dados pessoais como a proposta legislativa do Senado Federal, expressamente adotavam um regime de responsabilidade civil objetiva. Enquanto a primeira preceituava que “o tratamento de dados [seria] uma atividade de risco”,¹⁴ a segunda estabelecia que os agentes da cadeia responderiam, “independentemente da existência de culpa”,¹⁵ pela reparação dos danos.

A partir da segunda versão do anteprojeto de lei, ganhou força a opção por um regime de reponsabilidade civil subjetiva. Apesar de ter sido amplamente criticada ao longo do segundo processo de consulta pública¹⁶ e em audiência pública realizada na Câmara dos Deputados,¹⁷⁻¹⁸ essa escolha foi a que prevaleceu no Congresso. A redação final da LGPD eliminou os termos antes aventados – “independentemente de culpa” ou “atividade de risco” – que eliminariam a culpa como um dos pressupostos da responsabilidade civil.

¹³ Sobre a regulamentação do tema no âmbito da União Europeia, ver: ALSENOY, Brendan Van. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7 J. Intell. Prop. Info. Tech. & Elec. Com. L. 271 (2016).

¹⁴ Disponível em: <<http://culturadigital.br/dadospessoais/files/2010/11/PL-Protacao-de-Dados.pdf>>, ver tabela comparativa adiante nesse artigo.

¹⁵ Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&ts=1571776630206&disposition=inline>>, ver tabela comparativa adiante nesse artigo.

¹⁶ INTERNETLAB. *O que está em jogo no debate sobre dados pessoais no Brasil?*. 2016. Disponível em <https://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Um dos autores desse relatório, Bruno Bioni, à época pesquisador do Grupo de Políticas Públicas para o Acesso à Informação/GPoPAI da USP, apresentou contribuição em defesa de um regime de responsabilidade civil objetiva.

¹⁷ Na ocasião da audiência pública, realizada em 03.05.2017, Rafael Zanatta, representando o Idec, defendeu um regime de responsabilidade objetiva e solidária, fundando-se no diálogo com as demais fontes legislativas, na vulnerabilidade dos consumidores e no estímulo à segurança jurídica e à confiança dos usuários. Leonardo Bessa, representando o Brasilcon, defendeu um regime de responsabilidade objetiva e solidária, tendo em vista o diálogo das fontes e a vulnerabilidade dos consumidores. E Leandro Alvarenga, representando a Confederação Nacional de Dirigentes e Lojistas, criticou a adoção de um regime de responsabilidade solidária, por excluir pequenos lojistas do acesso à informação (e dificultar o acesso ao crédito) e não levar em conta a atuação individual. Disponível em: <<https://www.youtube.com/watch?v=-tU53jLMSyk>>. Acesso em: 30 abr. 2020.

¹⁸ ZANATTA, op. cit., p. 11: “A tensão também ficou clara em dois textos de posição produzidos por entidades distintas: de um lado, o *Manifesto sobre a Futura Lei de Proteção de Dados Pessoais*, coordenada por Brasscom, Abranet e outras associações; de outro, a *Carta Aberta à Comissão Especial de Tratamento e Proteção de Dados Pessoais* produzida pelo Idec. Observando-se as contribuições do setor privado à Comissão Especial de Tratamento e Proteção de Dados Pessoais – em especial, BSA, Facebook, Brasscom, Febraban, ABMED e ANBC –, nota-se, também, um posicionamento massivo contra as regras de responsabilidade solidária”.

1ª versão do anteprojeto	PLC 53/2018	LGPD
<p>Art. 6º O tratamento de dados pessoais é atividade de risco e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarcí-lo, nos termos da lei.</p>	<p>Art. 42. O responsável 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.</p> <p>§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:</p> <p>I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do responsável, hipótese em que o operador equipara-se a responsável, salvo nos casos de exclusão previstos no art. 43 desta Lei;</p>	<p>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.</p> <p>§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:</p> <p>I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;</p>
<p>2ª versão do anteprojeto</p> <p>Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.</p>	<p>II – os responsáveis 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.</p> <p>§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.</p> <p>§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto no Título III da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).</p> <p>§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.</p>	<p>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.</p> <p>§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.</p> <p>§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.</p> <p>§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.</p>

Tabela comparativa entre os dois textos citados e o final da LGPD

Ademais, o texto foi gradualmente esculpido para delimitar quais seriam as excludentes de responsabilidade civil. as versões anteriores ao substitutivo aprovado de autoria do Deputado Orlando Silva eram, senão silentes, extremamente tímidas com relação aos contornos da definição de ilicitude de uma conduta, bem como com relação ao seu nexos de causalidade para deflagrar a responsabilização dos agentes de tratamento. É apenas nesse último estágio da discussão legislativa que são prescritos tais pilares fundantes do regime jurídico da responsabilidade civil da LGPD.

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,¹⁹ 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”.²⁰ Trata-se de elementos que afastam a aplicação do sistema de responsabilidade civil objetiva.

Ao completar um regime jurídico que se orienta pela discussão da culpa, não se pode negligenciar a inserção do princípio da *accountability*, acompanhada dos chamados

¹⁹ O art. 44, parágrafo único, fala em obrigação de indenizar por danos causados em decorrência de “violação da segurança dos dados”. Com base em referência nele expressa, esse dispositivo deve ser lido em conjunto com o art. 46, *caput*. Disso depreende-se que a “violação da segurança dos dados” configura-se nos casos em que, com os dados pessoais, ocorrem: (i) acessos não autorizados; (ii) situações acidentais ou ilícitas de destruição, perda, alteração, comunicação; ou (iii) quaisquer outras formas de tratamento inadequado ou ilícito.

²⁰ Artigo 46 da LGPD: “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. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei. § 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução”.

*relatórios de impacto à proteção de dados pessoais*²¹ e, de forma mais ampla e geral, o estímulo e reforço à capacidade dos agentes de tratamento de dados pessoais de auto-organização. Ao longo dos trabalhos preparatórios da LGPD, foi dedicada uma seção específica sobre “Boas Práticas e da Governança”. Trata-se de elementos que, ainda que indiretamente, reforçam um regime de responsabilidade civil de natureza subjetiva.

Além do próprio *nomen iuris* do referido princípio, a sua definição aponta para que haja juízo de valor em torno da conduta do agente de tratamento de dados para a sua responsabilização. Nesse sentido, aliás, há conexão expressa entre este princípio e o mencionado elemento de responsabilidade civil mais voltado a um sistema de natureza subjetiva.

Com relação aos *relatórios de impacto à proteção de dados pessoais*,²² trata-se de instrumento que foi ganhando cada vez mais protagonismo ao longo dos trabalhos preparatórios da lei. Enquanto na segunda versão do anteprojeto da lei havia sido referido uma única vez, passa a ser mencionado oito vezes no desenho final da LGPD. Além disso, o texto aprovado ressalta que tal ferramenta deveria ser ativada para os casos em que as atividades de tratamento de dados fossem de “alto risco”. É uma gramática que, mais uma vez, não nivela toda e qualquer atividade de tratamento de dados como sendo de risco exacerbado, afastando-se um regime de natureza objetiva.

Por fim, deve ser também destacado que a parte relativa à “segurança e boas práticas”, que antes era um título do capítulo da tutela administrativa, passa a ser um

²¹ “Art. 4º [...] § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais”. “Art. 10 [...] § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial”. “Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público”. “Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados”. “Art. 55-J. Compete à ANPD: [...] XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; [...] § 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório”.

²² Sobre isso: ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>. GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados pessoais. Revista do Advogado, n. 144, nov., pp. 174-183, 2019.

capítulo próprio. Em termos topográficos e de técnica legislativa, ganha autonomia e, principalmente, passa a ser referenciado como um gatilho para deflagrar a responsabilidade civil dos agentes de tratamento de dados. Mais uma vez, há uma estrutura normativa que prioriza um juízo de valor em torno da conduta do lesante.

Os trabalhos preparatórios da LGPD deixam claro que sua política legislativa refutou deliberadamente um regime de reponsabilidade civil objetiva. Há outros elementos normativos que, direta ou indiretamente, convergem para que haja um juízo de valor em torno da culpa do lesante. Algo que não está apenas cristalizado no rol de excludentes de responsabilidade, mas, também, na principiologia e em outras partes importantes e integrantes do texto da LGPD. É uma racionalidade inescapável e que está por trás da lógica do regime de responsabilidade civil em questão.

3. Hipóteses de responsabilização na LGPD: a violação à legislação e a violação à segurança

A LGPD estabelece duas hipóteses para a configuração da responsabilidade civil dos agentes de tratamento de dados: a “violação à legislação de proteção de dados pessoais” e a “violação da segurança dos dados”. Ambos são calibrados pela noção de tratamento irregular, previsto no artigo 44, o qual procura sistematizar critérios para aferição da culpa dos agentes de tratamento de dados a esse respeito. Ressalta-se desde logo, contudo, que não parece haver razão para tal bifurcação, uma vez que as consequências são as mesmas (obrigação de indenizar) e, em especial, que essas duas hipóteses de reponsabilidade civil são reunidas no artigo 44 sob a noção ampla de “tratamento irregular”.

Ainda que se conclua pela adoção de um regime de responsabilidade civil subjetivo pela LGPD, esse artigo é central para a construção de uma dogmática que pode reduzir ou ampliar o espaço a ser ocupado pela culpa para fins de deflagração da responsabilidade dos agentes de tratamento de dados.

3.1. Tratamento irregular

O art. 44 prevê que “o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual

é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado”.

Antes das “circunstâncias relevantes”, mencionada no *caput* do referido artigo, é necessário analisar uma questão: a relação do tratamento irregular com a hipótese de violação à legislação de proteção de dados pessoais.

3.1.1. Avaliando a segurança dos dados: critério das medidas aptas (art. 44. parágrafo único) versus critério da segurança esperada (art. 44, II)

A noção de “tratamento irregular” apresenta-se de forma dúbia no texto da LGPD.. Da sua leitura, percebe-se que ele visa conectar-se tanto com a hipótese de responsabilidade por violação da legislação, quanto por violação da segurança. Apesar disso, a previsão de tratamento irregular encontra-se prevista no *caput* do dispositivo (art. 44) que abarca, em seu parágrafo único, a responsabilidade por violação da segurança.

Se a figura do tratamento irregular conecta-se igualmente com ambas as hipóteses de responsabilidade, melhor seria prevê-la em dispositivo autônomo, permitindo a essa regra ficar equidistante das duas hipóteses de violação de normas da LGPD. Da forma como está, parece sugerir uma conexão mais próxima (ou quiçá exclusiva) da noção de regularidade do tratamento para com a violação da segurança, do que para com a violação à legislação da proteção de dados. E mais: melhor ainda seria um dispositivo que previsse, no *caput*, que os agentes de tratamento responderiam pelos danos decorrentes de tratamento irregular de dados. E, em parágrafo, houvesse a explicação do conteúdo do tratamento irregular.²³

Essa má técnica legislativa pode, contudo, ser parcialmente explicada. Essa previsão de tratamento irregular corresponde à transposição para a LGPD de previsão do CDC que regula defeito do serviço. O art. 14, § 1º do CDC prevê: “O serviço é defeituoso quando

²³ Essa questão dos dispositivos dos artigos não deixa de ter reflexos materiais. Segundo Patricia Peck Pinheiro, o art. 44 “traz as condições de demonstração da ilicitude do tratamento de dados pessoais, assim como ocorre com o artigo 6º do GDPR, que pontua as condições de licitude do tratamento de dados pessoais”. (PINHEIRO, Patricia Peck. *Proteção de dados pessoais: Comentários à lei n. 13.709/2018 (LGPD)*. São Paulo: Saraivajur, 2018, p. 101). Note-se que o art. 6º do GDPR, ou melhor RGPD conforme sua sigla em português, encontra correspondência material no art. 7º da LGPD, que trata dos requisitos para o tratamento de dados pessoais. Esse dispositivo, por sua vez, está diretamente ligado à hipótese de “violação à legislação de proteção de dados pessoais”, prevista no art. 42, *caput*. Essa leitura da autora sobre o conteúdo do dispositivo deixa de fora, portanto, a relação entre tratamento irregular e violação da segurança dos dados. Nesse caso, a associação teria de ter incluído o art. 32 do RGPD, o qual prevê os parâmetros para a determinação das medidas de segurança exigíveis para tratamento de dados.

não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido”. É exatamente o conteúdo que foi espelhado nos incisos do artigo 44 da LGPD.

CDC	LGPD
<p>Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.</p> <p>§ 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:</p> <p>I - o modo de seu fornecimento;</p> <p>II - <u>o resultado e os riscos que razoavelmente dele se esperam;</u></p> <p>III - <u>a época em que foi fornecido.</u></p> <p>§ 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.</p> <p>§ 3º O fornecedor de serviços só não será responsabilizado quando provar:</p> <p>I - que, tendo prestado o serviço, o defeito inexiste;</p> <p>II - a culpa exclusiva do consumidor ou de terceiro.</p> <p>§ 4º A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.</p>	<p>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:</p> <p>I - o modo pelo qual é realizado;</p> <p>II - o resultado e os riscos que razoavelmente dele se esperam;</p> <p>III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.</p> <p>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.</p>

Tabela comparativa CDC vs LGPD

É possível depreender, assim, que tal previsão tem maior vocação para fornecer elementos a respeito da concretização de falha de segurança do tratamento de dados. Isso explica, inclusive, sua localização no mesmo dispositivo que a violação da segurança dos dados e ter com ela maior proximidade e interação material.

A segunda desconformidade é de conteúdo. O art. 44, parágrafo único, prevê que os agentes de tratamento de dados respondem ao deixarem de adotar medidas de segurança aptas a proteger os dados pessoais (art. 46) e, assim, derem causa ao dano. A irregularidade aqui, para utilizar uma nomenclatura da própria LGPD, é a não adoção, por parte do controlador e operador, das medidas de segurança aptas a proteger os dados pessoais. Por outro lado, o art. 44, *caput*, diz que o tratamento será irregular quando não fornecer a segurança que o titular dele pode esperar. Vê-se, portanto, que,

de um lado, tem-se como pressuposto as medidas de segurança aptas a proteger os dados pessoais. E, de outro, tem-se a segurança que o titular dele pode esperar. Em face disso, questiona-se: em caso de violação da segurança dos dados, o agente responde se ele não adotar as medidas de segurança aptas a protegê-los, ou se o tratamento não fornecer a segurança que o titular dele pode esperar?

Note-se que são critérios distintos. Para ficar apenas em um exemplo: o titular pode esperar que o tratamento forneça segurança maior ou menor que aquela garantida pela adoção das medidas de segurança aptas a proteger os dados pessoais. Os critérios geram questionamentos diferentes. De um lado, o que são medidas de segurança *aptas*? São aquelas que potencialmente garantem a segurança, ou apenas aquelas que seguramente o fazem? De outro lado, quando a lei fala em “segurança que o titular dele pode esperar”, o critério é subjetivo ou objetivo? Trata-se do que a pessoa do titular de dados do caso concreto pode esperar, devendo-se então levar em conta o seu nível especial de conhecimento ou ignorância? Ou critério objetivo, falando de um titular padrão?

3.1.2. Violação à legislação e violação à segurança: o recurso do conceito de “legítimas expectativas de segurança” como elemento interpretativo

Como vimos, “tratamento irregular” não é noção autônoma, e o não fornecimento da segurança que o titular pode esperar (art. 44, *caput*) deve coincidir com “deixar de adotar as medidas de segurança” *aptas* a proteger os dados pessoais (art. 44, parágrafo único, *c/c* art. 46, *caput*).

Mas o que isso significa na prática? Analisando detidamente, percebe-se que apenas o critério de não fornecimento da segurança que o titular pode esperar do tratamento (art. 44, *caput*) parece oferecer diretrizes na elaboração do seu conteúdo. Isso se deve, em primeiro lugar, pelo fato de o critério da adoção de tratamentos aptos a proteger os dados pessoais ser demasiadamente amplo. Ele confere apenas um critério mínimo, ou quiçá nem isso. De fato, seria ilógico pensar que o agente teria de adotar medidas inaptas para proteger os dados pessoais. Contudo, o universo de medidas aptas é demasiadamente amplo. Por exemplo, a rigor poderiam ser consideradas medidas aptas a proteger os dados pessoais, tanto uma desproporcionalmente mais custosa do que as demais, quanto uma outra cuja eficácia tivesse sido confirmada e disseminada apenas após o evento danoso, mas antes da decisão judicial de responsabilidade. Mas,

apesar de aptas, seriam essas medidas exigíveis, ou seja, que o agente deveria ter adotado sob pena de responsabilização? Entendemos que não.

Por outro lado, é bem mais frutífera a análise do critério de irregularidade do tratamento “quando não fornecer a segurança que o titular dele pode esperar”. Mas o que isso significa exatamente? Em primeiro lugar, não é a segurança cujo fornecimento de fato se espera, mas sim aquela que se “pode esperar”. No primeiro caso, seria uma mera constatação fática. No segundo, há aí um *filtro jurídico*: aquilo que, do ponto de vista jurídico, o titular está autorizado a esperar. Não se trata de qualquer expectativa de segurança, mas sim de expectativas juridicamente legítimas.²⁴ Vai-se trabalhar aqui, assim como se trabalha no CDC, com “legítimas expectativas de segurança”. Trata-se de conceito jurídico indeterminado, “cujo sentido deve ser concretizado pelos tribunais em vista das circunstâncias do caso concreto”.²⁵

Um exemplo que ilustra bem os desdobramentos práticos de tal dogmática proposta é o que se testemunhou recentemente no campo da criptografia. Foi apenas mais recentemente que se desenvolveu e se disseminou a chamada criptografia assimétrica de “ponta a ponta”,²⁶ de sorte que hoje é uma expectativa de segurança que se pode esperar dos chamados aplicativos de mensagens instantâneas. Em um passado não muito distante, em particular antes dos escândalos de espionagem “Snowden”, tal tecnologia de segurança da informação não estava disseminada e, muito provavelmente, não corresponderia a uma expectativa juridicamente tutelável.²⁷

²⁴ No CDC, essa questão é mais clara quando se regula responsabilidade por defeito do produto do que por defeito do serviço. No primeiro caso, o CDC prevê que “o produto é defeituoso quando não oferece a segurança que dele legitimamente se espera” (art. 12, § 1.º). No caso da responsabilidade por defeito do serviço, fala apenas que “o serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar” (art. 14, § 1.º). Apesar da distinção, a doutrina não faz diferenciação. Em ambos os casos, entende-se que a expectativa tem de ser legítima. A LGPD inspirou-se no regramento da responsabilidade por defeito do serviço, por isso que não menciona legitimamente. Mas, da mesma forma que acontece no CDC, isso não é sinal de que as expectativas não precisam ser legítimas.

²⁵ REINIG, Guilherme Henrique Lima. *A responsabilidade do produtor pelos riscos do desenvolvimento*. São Paulo: Atlas, 2013, p. 30.

²⁶ Essa discussão é o que está no cerne da ADPF 403-SE: se as ordens de bloqueio do aplicativo WhatsApp, por franquear acesso às mensagens criptografadas dos seus usuários, gera lesão a uma série de direitos fundamentais. A esse respeito, veja-se todo o mapa das argumentações feito pelo InternetLab, disponível em: <<http://bloqueios.info/pt/audiencia-publica-sobre-criptografia-e-bloqueios-do-whatsapp-argumentos-diante-do-stf/>>.

²⁷ Na criptografia assimétrica de ponta a ponta, dois tipos de chave são usados para cada ponta da comunicação, uma chave pública e uma chave privada. As chaves públicas estão disponíveis para qualquer outra pessoa, todos compartilham suas chaves públicas antes da comunicação. ABREU, Jacqueline de Souza, *From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp*, Columbia Journal of Transnational Law Online Edition, 17 de outubro de 2016.

Um outro exemplo a esse respeito, desta vez projetando um cenário futuro, será quando for escalada a chamada computação quântica.²⁸ Dado o aumento da capacidade de processamento de informação em termos quantitativos e qualitativos que se experimentalá, conseqüentemente as técnicas de segurança progredirão e, em última análise, haverá a atualização do filtro jurídico hoje existente em torno do que se considera “legítima expectativa de segurança”.²⁹

Um segundo ponto refere-se à necessidade de delimitar esse “titular”, se é a pessoa em si do caso concreto, ou um titular médio. Retornando ao referencial do direito do consumidor, como bem coloca Guilherme Reinig, referindo-se às expectativas de segurança no CDC, “para tal concretização importa, antes de tudo, especificar a perspectiva a partir da qual o juiz deve identificar as expectativas de segurança [...]. Trata-se, em outros termos, da determinação da ‘titularidade’ da legítima expectativa de segurança. Em linhas gerais, o problema consiste em saber se o legislador adotou um critério subjetivo ou objetivo”.³⁰ Isto é, se vai fazer uma análise em concreto, ou em abstrato. Tendo como base a pessoa em causa, ou um grupo abstrato de pessoas.

De maneira análoga ao que ocorreu no CDC, o legislador da LGPD não é expresso em relação à solução seguida. No direito do consumidor, uma vez que o CDC trabalha com noção parecida: o produto ou serviço é defeituoso quando não oferece a segurança que o consumidor dele pode esperar (art. 14, § 1.º). A doutrina, contudo, conclui pelo critério objetivo.³¹

²⁸ Em 08.01.2019 foi lançado o primeiro computador quântico de uso comercial do mundo. Contudo, estima-se um período entre cinco e dez anos para que a computação quântica passe a ser adotada nos negócios. Assim, apesar de existente, essa tecnologia não compreenderia o estado da arte da tecnologia (ou meio técnico razoável disponível, nos termos da LGPD), tornando um encargo demasiado excessivo a expectativa de sua adoção. Disponível em <<https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/como-computacao-quantica-vai-abalar-os-negocios-para-sempre.html>>. Acesso em: 29 abr. 2020.

²⁹ Sobre uma discussão mais detida a esse respeito sobre as chamadas técnicas de anonimização, veja-se: BIONI, Bruno Ricardo. *Compreendendo o conceito de anonimização e dado anonimizado*. In: Cadernos Jurídicos – Direito digital e proteção de dados pessoais. São Paulo: Escola Paulista de Magistratura, ano 21, n. 53, janeiro-março 2020. Disponível em <https://brunobioni.com.br/wp-content/uploads/2020/04/Bioni_Anonimiza%C3%A7%C3%A3o.pdf>. Acesso em: 01 maio 2020.

³⁰ REINIG, op. cit., p. 30.

³¹ Segundo fundamenta Guilherme Reinig, “o uso da voz passiva sintética na oração subordinada adjetiva restritiva [...], não deixa dúvida de que o legislador optou pelo critério objetivo”. E complementa: “Em última instância, as legítimas expectativas de segurança são determinadas pelo chamado ‘horizonte da coletividade afetada pela falta de segurança do produto’ (*Horizont der durch die fehlende Produktsicherheit betroffenen Allgemeinheit*), o qual nem sempre se confunde com a perspectiva da sociedade em geral. O mencionado horizonte abrange tanto os destinatários ou consumidores do produto como os *bystanders*. Como, porém, a consideração dos interesses destes não altera significativamente os critérios de verificação da existência de defeito, não há problema algum em se apontar como titular das expectativas de segurança o consumidor médio ou ideal-típico. Nesse sentido, esta noção é um instrumento conceitual de identificação das legítimas expectativas de segurança do setor social afetado pelos riscos relacionados ao produto” (REINIG, op. cit., p. 30).

Em relação à LGPD, deve-se chegar a conclusão análoga. Nesse sentido, na doutrina nacional sobre proteção de dados, Cots e Oliveira afirmam: “a análise da expectativa deverá sempre ser realizada sobre um caso concreto, utilizando a noção que se espera do homem-médio em relação a determinado tratamento de seus dados”.³²

É possível concluir, assim, que o critério determinante para a imputação de responsabilidade é o da “irregularidade do tratamento”. Esse critério é analisado com base nas legítimas expectativas de segurança que um titular médio pode esperar do tratamento de dados em questão.

3.1.3. “Circunstâncias relevantes” como critério ao juízo de culpa

No artigo 44 da LGPD o legislador elencou três exemplos (não exaustivos) de “circunstâncias relevantes” para a determinação da segurança que o titular médio pode esperar do tratamento de dados e de potencial violação à legislação.: I – o modo pelo qual o tratamento é realizado; II – o resultado e os riscos que razoavelmente dele se esperam; e III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Um possível caminho para dar densidade normativa a tais incisos é colá-los ao que preceitua o artigo 50, em especial os §§ 1º e 2º. Ao considerar que os agentes de tratamento de dados devem estabelecer mecanismos de mitigação de “riscos” das suas atividades de tratamento de dados, referidos dispositivos apontam que se deverá levar em consideração respectivamente: (i) a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular; (ii) a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados.

Dessa forma, o modo pelo qual é realizado um tratamento de dados (inciso I) e os riscos que razoavelmente dele se esperam (inciso II) são calibrados diretamente por tais variações. 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.

³² COTS, Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2019, p. 186.

Volta-se ao que foi mencionado anteriormente (tópico 1), a (in)evolução do texto da LGPD não nivela toda e qualquer atividade de tratamento de dados como sendo de risco exacerbado. Pelo contrário, demanda-se uma análise casuística para se desdobrar um juízo de valor sobre o modo pelo qual deve ser realizado um tratamento de dados e os riscos que dele razoavelmente se esperam.

Alguns exemplos e considerações podem ser elucidativos. De um lado, é notório que dados de cartão de crédito detêm um risco maior diante do interesse de terceiros fraudadores, do que em relação a endereços de e-mail.³³ A mesma coisa com relação ao CPF do que outros dados cadastrais para fins de fraudes bancárias. De outro, é uma análise que não olha para o porte ou o tamanho do agente de tratamento de dados, mas que é voltada para a atividade de tratamento de dados em si. Por exemplo, pense-se no caso de uma empresa nascente de tecnologia, com apenas cinco colaboradores, que fornece uma solução de inteligência artificial para automatizar diagnósticos e prognósticos na área de oncologia. Para tanto, é necessário manipular um grande volume de dados sensíveis de pacientes de uma série de hospitais e laboratórios. Tal atividade de tratamento de dados é mais arriscada do que aquela praticada por uma grande rede de supermercados, com mais de quinhentos colaboradores, que não tem sequer um programa de fidelidade dos seus consumidores.

Os agentes devem, assim, ajustar suas medidas de segurança para corresponder à probabilidade e à gravidade que violações podem assumir em face do impacto a direitos e liberdades dos titulares dos dados. É, então, vital separar e estimar esses riscos variados e, em seguida, aplicar medidas de segurança correspondentes. A política legislativa da LGPD reconhece que seu objeto constitui uma plêiade de relações jurídicas que apresentam uma multiplicidade de efeitos colaterais distintos, devendo-se investigar a culpa do agente de tratamento de dados de forma casuística.

3.1.4. Análise objetiva das “circunstâncias relevantes”

Outro critério de análise da noção de “tratamento irregular” são “as técnicas de tratamento de dados pessoais *disponíveis à época* em que foi realizado”. Tendo em vista que a legislação consumerista inspirou a LGPD, o produto ou serviço será

³³ De maneira análoga, lecionando sobre segurança no tratamento de dados com base no art. 32 do RGPD, ver: MORGENROTH, Sven. *GDPR Article 32: Security of Data Processing*. Disponível em: <<https://www.netsparker.com/blog/web-security/gdpr-article-32-security-data-processing/>>. Acesso em: 30 mar. 2020.

defeituoso quando não fornecer a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, como risco que razoavelmente se espera *e a época* em que foi colocado em circulação ou fornecido (art. 12, § 1º, III e art. 14, § 1º, III, CDC).

Essa previsão reflete a necessidade de se determinar um momento a partir do qual se afere a irregularidade do tratamento.³⁴ A questão a se responder, contudo, diz respeito à cognoscibilidade e exigibilidade de adoção das medidas de segurança para que elas sejam consideradas como disponíveis à época em que foi realizado o tratamento de dados. Ou seja, considera-se como disponível à época do tratamento as medidas de segurança perceptíveis e acessíveis aos agentes de tratamento de diligência comum ou média?

Em relação a essa questão, Márcio Cots e Ricardo Oliveira pontuam que “a LGPD dispõe que as técnicas de tratamento disponíveis à época devem ser consideradas. A regra é importante, especialmente porque utiliza a palavra ‘disponíveis’, não existentes, o que são coisas completamente diferentes”. Os autores propõem, então, dois exemplos: “Imagine, por exemplo, que na Noruega esteja sendo testado um sistema de segurança extremamente eficiente, mas que ainda não está sendo comercializado fora do âmbito daquele país. Ora, o sistema existe, mas não está disponível aos controladores brasileiros. Por outro lado, suponha que após determinado tempo o sistema passe a ser comercializado no Brasil, mas pelo valor de 50 milhões de dólares a licença”. Em face disso, questionam: “Isso faz com que o sistema esteja ‘disponível’ para os controladores brasileiros? Entendemos que não. A palavra ‘disponíveis’ precisa levar em consideração a possibilidade ou não de o controlador ter acesso a determinado sistema, não o simples fato de ele existir ou ser comercializado fora dos padrões econômicos do controlador sob análise”.³⁵

De acordo com essa leitura, o critério determinante seria o da diligência média dos agentes de tratamento. Contudo, essa posição não leva em conta que essa previsão foi inspirada em previsão análoga no CDC. Nesse diploma, é necessário verificar se o

³⁴ Essa indispensabilidade já foi reconhecida no direito do consumidor em relação ao juízo de defeito do produto ou serviço, sendo os argumentos aqui aproveitáveis. Segundo analisa Guilherme Reinig: “Diversos fatores, como o aumento das necessidades de segurança da sociedade e especialmente o desenvolvimento de novas tecnologias, concorrem para que a segurança que legitimamente se espera do produto não seja constante, modificando-se com o passar do tempo. Por isso, é necessário o estabelecimento de um instante decisivo para a avaliação da defectibilidade do produto. Esse instante ou momento é, de acordo com o texto legal, aquele em que o produto é colocado em circulação. Se o produto corresponder à segurança que dele legitimamente se espera no mencionado instante ou momento, ele não poderá ser considerado defeituoso, ainda que haja uma posterior elevação das legítimas expectativas de segurança” (REINIG, op. cit., p. 36).

³⁵ COTS; OLIVEIRA, op. cit., p. 186.

fornecedor adotou ou não as medidas necessárias para que o produtor ou serviço fornecesse a segurança que o consumidor dele pode esperar, levando-se em conta a época em que o serviço foi fornecido. Contudo, o legislador previu que a responsabilidade do fornecedor seria independentemente de culpa. O critério não é, portanto, o da diligência média do próprio fornecedor nem a diligência de um fornecedor médio. Isso porque a diligência média do fornecedor, ou a diligência de fornecedor médio são os dois critérios tradicionais para determinar a culpa subjetiva (ou *in concreto*) e objetiva (ou *in abstracto*).

Na LGPD não há previsão de exclusão da culpa análoga a essa do CDC (“independentemente da existência de culpa”). Contudo, como a previsão da circunstância da época em que o serviço foi prestado foi o que deu origem à disposição da LGPD, é possível conceber que o critério almejado é, assim como no CDC, mais rigoroso do que o da culpa.

3.2. Pressupostos da responsabilização e inversão do ônus da prova

A partir das excludentes de responsabilidade estabelecidas no artigo 43 da LGPD, e em face de dano decorrente de tratamento de dados, presume-se: (i) a autoria do tratamento por parte do agente a quem o tratamento é atribuído; e (ii) a violação à legislação de proteção de dados ou irregularidade do tratamento.

Acontece que, além dessa presunção geral de dois elementos da responsabilidade civil dos agentes de tratamento, a LGPD prevê também a possibilidade de o juiz inverter o ônus da prova a favor do titular dos dados quando a alegação for verossímil, quando houver hipossuficiência ou quando a produção de provas for excessivamente onerosa (art. 42, § 2.º). Como compatibilizar?

O art. 43 implica a presunção automática de alguns elementos da responsabilidade civil, mas não de todos. Contando com essa presunção, resta ainda ao lesado, em geral, alegar e provar: (i) a realização de (algum) tratamento de dados pessoais – não sendo necessário provar que foi realizado pelo réu; (ii) o dano sofrido; e (iii) o nexo causal entre o tratamento de dados realizado e o dano.

A compatibilização entre as previsões do art. 43 e art. 42, § 2.º é, então, a seguinte: caso a alegação da vítima seja verossímil, ou haja hipossuficiência para produção de provas, ou a produção seja excessivamente onerosa, o juiz poderá inverter o ônus da prova em

relação a esses três últimos elementos. 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.

Uma inversão tão extremada do ônus da prova é justificada pela, igualmente dramática, hipossuficiência do titular de dados. Como observam Tarcisio Teixeira e Ruth Armelin, essa hipossuficiência torna-se “facilmente constatável quando se tem uma sociedade permeada pela cultura do *Big Data*, em que há uma coleta massiva de dados, muitas vezes até desnecessária”. Em face dessa realidade, complementam os autores, “o titular de dados se encontra em uma posição claramente desfavorável, em que beira [a]o impossível saber quais de seus dados estão sendo tratados, de que forma isso tem sido feito e quem seriam os agentes de tratamento”.³⁶

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.

Presunção automática-legal	Presunção mediante inversão do ônus da prova em juízo
(i) a autoria do tratamento por parte do agente a quem o tratamento é atribuído; (ii) a violação à legislação de proteção de dados ou irregularidade do tratamento	Resta ao lesado provar: (i) o dano sofrido; e (ii) o nexo causal entre o tratamento de dados realizado e o dano.
(artigo 43, I e II, da LGPD)	(artigo 42, § 2º da LGPD)

3.3. Obrigação de meio versus obrigação de resultado

Finalmente, cabe considerar se as obrigações atribuídas aos agentes de tratamento de dados na LGPD são de meio ou resultado. Tal discussão relaciona-se diretamente ao

³⁶ TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC*. In: LIMA, Cíntia Rosa Pereira de (Coord.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020, p. 322.

tema aqui proposta, pois, na prática, no caso de uma obrigação de resultado, a não consecução do resultado almejado implica uma presunção de culpa em relação ao inadimplemento.

O princípio da responsabilidade e prestação de contas prescreve que deve haver pelos agentes de tratamento de dados pessoais a “demonstração (...) da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”. O dispositivo chega a ser prolixo, já que duplica o uso do termo eficazes-eficácia.

Tais adjetivos abrem margem interpretativa para considerar que a LGPD atribuiu uma obrigação de resultado, na medida em que indica normativamente que não basta apenas adotar – para usar o verbo de ambos os dispositivos – medidas a evitar o tratamento inadequado de dados, mas, tais ações devem ser eficientes.

Por outro lado, o conceito de *privacy by design*,³⁷ previsto no artigo 46 da Lei, prevê que 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”.

Por sua vez, o já citado artigo 50 da LGPD prevê que a aptidão dessas medidas deve ser ajustada de acordo as características da atividade de tratamento de dados em questão, em especial “a gravidade dos riscos” que dela derivam para o titular.

Esses outros dois dispositivos parecem prescrever uma *norma de conduta* que encerra uma obrigação de meio. Isto porque enuncia-se quais elementos devem ser considerados para que um fim seja alcançado, mas sem vincular o sujeito passivo dessa obrigação à consecução deste objetivo.

A análise aqui apresentada aponta para uma possível dubiedade na moldura normativa da LGPD quanto ao tipo de obrigação que foi alocada aos agentes de tratamento de

³⁷ BIONI, Bruno Ricardo. *Abrindo a caixa de ferramentas da LGPD para dar vida ao conceito ainda elusivo de Privacy by design*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Org.). *Direito & Internet IV: Sistema de Proteção de Dados Pessoais*. São Paulo: Quartier Latin, v. 1, 2019.

dados. Um olhar mais focado nos adjetivos trazidos pelo princípio da responsabilidade e prestação de contas abre caminho para uma possível obrigação de resultado, enquanto os dispositivos relacionados a *privacy by design* e boas práticas indicam uma obrigação de meio que poderia, em última análise, modular o referido termo *eficiência* contido no referido princípio.

4. Conclusão

A despeito da adoção de um regime de responsabilidade civil subjetiva, a LGPD parece ter facilitado a configuração do dever de indenizar. A respeito da presunção automática-legal da culpa do lesante, a qual pode ser somada à inversão do ônus da prova em juízo quanto aos demais pressupostos da responsabilidade civil. Se isto for, ainda, combinado com uma interpretação elástica em torno da noção de tratamento irregular, especialmente quanto à obrigação dos agentes de tratamento de dados pessoais adotarem as técnicas “disponíveis à época do tratamento” que se desdobrem em um alto nível de diligência quanto ao estado da arte e da técnica como já o vem fazendo parte da doutrina consumerista, então se tornará extremamente difícil o agente de tratamento de dados afastar a sua culpa.³⁸

Deve-se, assim, avançar para além da análise binária do regime jurídico de responsabilidade civil da LGPD, julgando-o de natureza objetiva ou subjetiva. Isto porque não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. O resultado parece ir no sentido de um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade.

Bibliografia

ABREU, Jacqueline de Souza. *From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp*. Columbia Journal of Transnational Law Online Edition, 17 de outubro de 2016.

³⁸ SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil: da erosão dos filtros da reparação à diluição dos danos*. 4ª ed. Atlas Jurídico: São Paulo, 2015, p. 221: “E, mesmo no Brasil, onde a matéria era tradicionalmente regida pela responsabilidade subjetiva, as cortes já recorriam a expedientes bastante objetivistas, como a presunção, tomada em sentido quase absoluto, de responsabilidade do motorista que atinge a parte traseira do automóvel alheio (...) por meio da simples adoção de parâmetros bastante elevados e rígidos de comportamento diligente, ou ainda por força de uma inversão insuperável do ônus probatório da demonstração de culpa”.

ACCIOLY, Hildebrando; NASCIMENTO E SILVA, G. E. do; CASELLA, Paulo Borba. *Manuel de Direito Internacional Público*. 24^a ed. São Paulo: Saraiva, 2019.

BIONI, Bruno Ricardo. *Compreendendo o conceito de anonimização e dado anonimizado*. Cadernos Jurídicos – Direito digital e proteção de dados pessoais. São Paulo: Escola Paulista de Magistratura, ano 21, n. 53, janeiro-março 2020.

BIONI, Bruno Ricardo. *Nota do coordenador*. São Paulo: Revista do Advogado, n. 144, nov., 2019.

BIONI, Bruno Ricardo. *País precisa ser competitivo em uma economia de dados*. Valor Econômico, 19 jul 2018.

BIONI, Bruno Ricardo. *Abrindo a caixa de ferramentas da LGPD para dar vida ao conceito ainda elusivo de Privacy by design*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. (Org.). *Direito & Internet IV - Sistema de Proteção de Dados Pessoais*. São Paulo: Quartier Latin, v. 1, 2019.

BRUNO, Marcos Gomes da Silva. *Da responsabilidade e do ressarcimento de danos*. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de dados comentada*. São Paulo: Revista dos Tribunais, 2019.

CORDEIRO, António Menezes. *Tratado de direito civil português*, vol. II, t. III: gestão de negócios, enriquecimento sem causa, responsabilidade civil. Coimbra: Almedina, 2010.

CORDEIRO, António Barreto Menezes. *Repercussões do RGPD sobre a responsabilidade civil*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coords.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019.

CORDEIRO, António Barreto Menezes. *Da responsabilidade civil pelo tratamento de dados pessoais*. In: BARBOSA, Mafalda Miranda; ROSENVALD, Nelson; MUNIZ, Francisco (Coord.). *Desafios da nova responsabilidade civil*. São Paulo: Editora JusPodivm, 2019, p. 49-64.

COSTA, Luiz. *Privacy and the precautionary principle*. *Computer Law & Security Review*, 28 (2012), 14-24.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2019.

GUEDES, Gisela Sampaio da Cruz. *Regime de responsabilidade adotado pela lei de proteção de dados brasileira*. Caderno especial LGPD, p. 167-182. São Paulo: Revista dos Tribunais, nov. 2019.

MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova lei geral de proteção de dados*. São Paulo: Revista dos Tribunais, vol. 120, 2018, p. 469-483, nov.-dez. 2018.

MIRAGEM, Bruno. *Curso de direito do consumidor*. 6. ed. São Paulo: Revista dos Tribunais, 2016.

MIRAGEM, Bruno. *A internet das coisas e os riscos do admirável mundo novo*. Consultor Jurídico, 29 mar. 2017.

MORGENROTH, Sven. *GDPR Article 32: Security of Data Processing*. Disponível em: <<https://www.netsparker.com/blog/web-security/gdpr-article-32-security-data-processing/>>. Acesso em: 30 mar. 2020.

MULHOLLAND, Caitlin Sampaio. *Palestra no Webinar IBERC #2 – A Responsabilidade Civil na Lei Geral de Proteção de Dados*. Instituto Brasileiro de Estudos em Responsabilidade Civil – IBERC, 19 set. 2019.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)*. São Paulo: Saraivajur, 2018.

REINIG, Guilherme Henrique Lima. *A responsabilidade do produtor pelos riscos do desenvolvimento*. São Paulo: Atlas, 2013.

SCHERTEL, Laura Mendes; DONEDA, Danilo. *Reflexões iniciais sobre a nova lei geral de proteção de dados*. São Paulo: Revista dos Tribunais, vol. 120/2018, p. 469 – 483, Nov - Dez/2018.

SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil: da erosão dos filtros da reparação à diluição dos danos*. 4^a ed. Atlas Jurídico: São Paulo, 2015.

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 – Direito digital e proteção de dados pessoais. São Paulo: Escola Paulista de Magistratura, ano 21, n. 53, janeiro-março 2020.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC*. In: LIMA, Cíntia Rosa Pereira de (Coord.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020, p. 297-326.

ZANATTA, Rafael A. F. *Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor*. In: *Coletânea do Instituto de Tecnologia e Sociedade sobre a Lei Geral de Proteção de Dados Pessoais*. São Paulo: Revista dos Tribunais, 2019, no prelo.

civilistica.com

Recebido em: 5.6.2020
Aprovado em:
1.10.2020 (1º parecer)
5.10.2020 (2º parecer)

Como citar: BIONI, Bruno; 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, a. 9, n. 3, 2020. Disponível em: <<http://civilistica.com/responsabilidade-civil-na-protacao-de-dados-pessoais/>>. Data de acesso.