FACULDADE BAIANA DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

MARIANA RIBEIRO MATOS

A IN (EFETIVIDADE) DA LEI 13.709/18 NA PROTEÇÃO DE DADOS PESSOAIS POR MEIO DO INSTITUTO DO CONSENTIMENTO

Salvador
2020

MARIANA RIBEIRO MATOS

A IN (EFETIVIDADE) DA LEI 13.709/18 NA PROTEÇÃO DE DADOS PESSOAIS POR MEIO DO INSTITUTO DO CONSENTIMENTO

Monografia apresentada ao curso de graduação em Direito, Faculdade Baiana de Direito, como requisito parcial para obtenção do grau de bacharel em Direito. Orientador: Prof. Diogo Guanabara

Salvador
2020

TERMO DE APROVAÇÃO

MARIANA RIBEIRO MATOS

A IN (EFETIVIDADE) DA LEI 13.709/18 NA PROTEÇÃO DE DADOS PESSOAIS POR MEIO DO INSTITUTO DO CONSENTIMENTO

Monografia aprovada como requisito parcial para obtenção do grau de bacharel em Direito, Faculdade Baiana de Direito, pela seguinte banca examinadora:

Nome:_____

Titulação e instituição:_____

Nome:_____

Titulação e instituição:_____

Nome:_____

Titulação e instituição:_____

Salvador, ____/_____/ 2020

AGRADECIMENTOS

Ao concluir essa grande etapa da minha vida acadêmica, me pego analisando a quão grata sou por ter tantas pessoas que me apoiam e vibram com as minhas conquistas. Olhando pra trás, desde o meu primeiro dia de aula na faculdade, me sinto orgulhosa do quanto amadureci, tanto academicamente, quanto no âmbito pessoal e do caminho que tracei nestes anos.

Agradeço primeiramente a Deus, por permitir que tudo ocorresse da melhor forma possível e por sempre me guiar pelo melhor caminho. À minha mãe, meu maior exemplo de fé e da vida, por todo amor e apoio incondicional, desde sempre. À Jeu, Bê, Malu e Lu, por tantos momentos de alegria e incentivo. Aos meus avós Regina e Aécio, responsáveis por uma família tão abençoada e unida, e que sempre se fizeram presentes em todas as etapas da minha vida. Aos meus tios (Lane, Rejane, Sina, Ninha e Ricardo) por serem tão atenciosos e queridos.

À Dan, por todo o companheirismo, amor, compreensão e por sempre me motivar a nunca desacreditar do meu potencial. Às minhas amigas da vida (Paulinha, Carol, Yna, Gui, Nanda, Neca, Jô, Mah, Mila, Lu, Doria, Lari e Vick) por sempre serem tão leais, amigas – no sentido real da palavra, e me proporcionarem tantos momentos felizes.

Às amigas que fiz na faculdade, mas que se tornaram amigas pra vida: Bia, Mariah e Gabi. Não poderia deixar de agradecer a todos que conheci no Jessup e no Vis Moot, e, e em especial, aos meus colegas de grupo, agradeço por terem feito parte da melhor experiência acadêmica que vivenciei na faculdade. Agradeço também a todos os advogados que me acompanharam durante as minhas experiências de estágio e que atuaram como peças essências para a minha formação acadêmica.

Por último, mas não menos importante, agradeço a todos os professores da Faculdade Baiana de Direito por tanta dedicação à docência, bem como a todos os funcionários que trabalham com tanta dedicação para que todas as atividades do dia a dia funcionem da melhor forma. Em especial, ao professor Ermiro Neto, pelo incentivo inicial no tema a ao meu orientador, Diogo Guanabara, por todas as observações, disponibilidade e ajuda para a finalização desta monografia.

“Nada é tão nosso como os nossos sonhos.”
Friedrich Nietzsche

RESUMO

A presente monografia tem como objetivo a análise do instituto do consentimento como instrumento de garantia da proteção de dados frente à Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). Como resultado direto de uma sociedade capitalista pautada na maximização de lucros, os dados pessoais, que antes eram tidos apenas como informações pessoais, passaram a assumir uma nova identidade, caracterizando-se como verdadeiros insumos. Diante da compreensão da complexidade dos efeitos que a má utilização de dados pessoais pode causar na vida do titular, após quase uma década de debates, em 2018, a Lei 13.709/2018 foi sancionada. Com forte influência do Regulamento Geral de Proteção de Dados Pessoais, mais conhecido como GDPR, a LGPD, corroborando com a ideia de que dados pessoais não são meros bens de cunho patrimonial, demonstra que o seu arranjo normativo se fundamenta na mitigação dos riscos desde antes da operação e que, portanto, intende a modificação da cultura de tratamento de dados pessoais. Sob a perspectiva da lei objeto de análise desta pesquisa, o consentimento atua como instrumento que viabiliza uma maior carga participativa do titular no processo de tratamento de seus dados pessoais. Portanto, além de uma análise sistemática da LGPD para uma melhor compreensão acerca do papel de protagonista do titular de dados, a presente monografia destina-se a uma análise da efetividade da referida lei em relação à garantia da proteção de dados por meio do consentimento, analisando os seus limites de tal instituto, bem como a sua interferência na atuação dos agentes de tratamento.

Palavras-Chave: Proteção de Dados Pessoais. Tratamento de Dados Pessoais. Consentimento. Autodeterminação informativa. LGPD. GDPR.

ABSTRACT

The current thesis aims to analyze the effectiveness of the new Brazilian data protection regulation in regard to the consent of the data holders as a device to enhance their participation on the processing of their personal data and therefore, guaranteeing them an adequate protection. As a direct result of a capitalist society based on the maximization of profits, personal information gained a new identity. Nowadays, those types of information are seen as true inputs. Acknowledging the possibility of innumerous bad consequences for individuals who have their personal data managed irregularly, almost after a decade of discussion on Brazil's Legislative Assembly, in 2018, the Law 13.709/2018, better known as LGDP, was sanctioned. The law's high influence of the European Union´s General Data Protection Regulation (GDPR) can be clearly seen on one of its main ideas: mitigating the risks of the processing of personal data before the operation has initiated. Thus, the entire body of the Brazilian data regulation demonstrates that it intends a drastic modification of the actual culture of processing personal information, corroborating with the idea that personal data aren´t mere assets of patrimonial nature. Therefore, the consent, due to its own characteristic of acting as an agreement to another´s proposition, on the perspective of the law being examined, proceeds as an instrument that empowers individuals of having an appropriate control of their personal data. By regulating this mechanism properly, the law guarantees a higher participation of the data holder on the processing of their personal data. Ultimately, for a better comprehension of the idea of the data holder as the main character of the LGPD, the law must be analyzed systematically. As the present study intends to examine the efficacy of that law in relation to ensuring data protection through consent, the study of the institutes' limits and impacts on the work of the controllers and processors is essential.

Key-Words: Data Protection. Consent. Processing. Constrollers. Processors. Effectiveness. LGPD. GDPR.

LISTA DE ABREVIATURAS E SIGLAS

CC- Código Civil

CDC – Código de Defesa do Consumidor

CPF – Cadastro de Pessoas Físicas

CF/88 – Constituição Federal de 1988

GDPR – *General Data Protection Regulation*

LCP – Lei do Cadastro Positivo

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

PL – Projeto de Lei

STJ – Superior Tribunal de Justiça

STF- Supremo Tribunal Federal

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

UE- União Europeia

FCRA - *Fair Credit Reporting Act*

FTC - *Federal Trade Comission*

MP – Medida Provisória

SUMÁRIO

1 INTRODUÇÃO

Vivemos em uma sociedade que se orienta e que tem a sua economia movimentada pela nova identidade advinda de dados pessoais. Como consequência direta de um sistema de coleta e tratamento massivo e desenfreado, estes dados deixam de serem apenas informações pessoais e se tornam verdadeiros insumos, seja pela sua utilização no direcionamento da publicidade online, influenciando no hábito do usuário ao escolher o que mostrar e o que não mostrar, na descriminação de planos de saúde, seguros de vida, seleções de emprego ou até mesmo no resultado de campanhas políticas, como indica o famoso caso Cambridge Analytica. Neste sentido, resta evidente que inúmeros efeitos negativos podem decorrer da crescente utilização de algoritmos para a realização de inferências, prognoses, avaliações sobre os indivíduos, dentre outras atividades, principalmente diante da opacidade e ausência de transparência nas decisões automatizadas.

Neste cenário digital, sem fronteiras geográficas, onde se torna cada vez mais raro não possuir acesso às redes sociais, em conjunto com um sistema de exploração de dados criado com o intuito de maximização de lucros, se encontra a alta probabilidade de violação aos dados pessoais, que, mesmo que obtidos no meio online, não deixam de se caracterizar como um prolongamento do indivíduo. Tendo em vista a possibilidade de estigmatização do titular de dados ao ser segmentado com base no tratamento das suas informações, a exemplo da criação de estereótipos e limitação de direitos (segregação), o direito à proteção de dados, além de não se limitar ao direito à privacidade, acaba abarcando diversos outros direitos da personalidade. Diante da compreensão da complexidade dos efeitos que a má utilização de dados pessoais pode causar na vida do titular, após quase uma década de debates, em 2018, a LGPD foi sancionada. No que pese a referida lei ainda não estar em vigor, demonstra um grande avanço para o sistema jurídico brasileiro, principalmente diante da importância de uma regulação no tema, atuando de forma impeditiva a condutas autoritárias e danosas por parte dos agentes de tratamento.

Diante disto, ou seja, da importância de uma tutela especializada de dados pessoais para a proteção da identidade e personalidade das pessoas, o presente trabalho objetiva a análise do instituto do consentimento frente à proteção de dados pessoais sob o regime jurídico instituído pela LGPD. Estes signos identificadores dos cidadãos devem projetar de maneira correta e precisa as informações para que os dados pessoais extraídos da rede de computadores

projetem fidedignamente a identidade do indivíduo, pois a má utilização destes pode acarretar em danos irreparáveis ao titular de dados. Neste panorama, o segundo capítulo deste trabalho tem por objetivo apresentar uma noção geral e histórica das leis de proteção de dados pessoais que influenciaram de forma direta e indireta na criação da Lei Geral de Proteção de Dados no Brasil. Além do mais, de forma introdutória, abordar os conceitos importantes para a compreensão da referida Lei, assim como os seus fundamentos e princípios.

Por ser a regulamentação do tratamento de dados pessoais o cerne da LGDP, o terceiro capítulo deste trabalho visa à análise das condições de legitimidade para a sua realização. Além da necessidade de amparar a sua atividade em uma das bases legais previstas no art. 7º da Lei e de seguir os princípios regulados no art.6º, deve o agente cumprir com os seus deveres e garantir que os direitos dos titulares de dados sejam observados. Diante disto, o referido capítulo irá abordar de forma específica o papel dos agentes de tratamento, dos encarregados e da Autoridade Nacional de Proteção de Dados neste processo.

Ao decorrer da análise dos capítulos anteriores, principalmente diante do fato de seis dos nove princípios elencados no art. 6º da LGPD estarem diretamente focados na atuação do titular de dados, resta claro o papel de protagonismo deste sujeito na Lei. Assim, o legislador se esforça ao máximo, ao criar um regramento específico para o consentimento, para garantir que o usuário utilize de tal mecanismo para fazer escolhas conscientes, racionais e autônomas acerca do tratamento de seus dados pessoais. A utilização do consentimento como instrumento para a tutela dos dados pessoais diante dos impactos diretos na atuação dos agentes de tratamento à luz da LGPD deve ser observado não só como base de tratamento propriamente dita, mas também tendo em vista a sua relação direta com os deveres impostos aos agentes de tratamento e com os princípios que direcionam as operações de tratamento de dados pessoais.

Assim, o último capítulo deste trabalho irá abordar, além dos impactos causados na atividade de tratamento pelo consentimento, seja como ato legitimador da referida atividade, por meio da possibilidade de revogabilidade do consentimento ou da hipótese de término do tratamento, a natureza de tal instituto e a sua trajetória normativa, visando uma maior clareza em relação ao mencionado papel de protagonismo do titular de dados frente à LGDP. A responsabilidade na esfera civil e administrativa dos agentes de tratamento, mesmo não estando a sua configuração limitada às infrações legais relacionadas ao consentimento do titular de dados, acaba se configurando com uma fonte auxiliar no fortalecimento do indivíduo por meio de uma maior rigidez ao cumprimento do regime jurídico dado consentimento na LGPD e por

isso, este tema também será abordado no último capítulo. Por fim, para uma real compreensão acerca da efetividade do consentimento como instrumento capaz de garantir o titular uma devida proteção aos seus dados pessoais, este capítulo analisará os limites de tal instituto, tanto aqueles cognitivos que advém da própria complexidade do fluxo informacional, quanto os limites impostos pela própria lei em análise.

2 A PROTEÇÃO DE DADOS PESSOAIS: DESTINATÁRIOS, CLASSIFICAÇÃO E SUA ESTRUTURA NA LGPD

No contexto de uma sociedade e uma economia movidas pelo fenômeno da datificação[1], há, como consequência direta, o prolongamento da pessoa por meio dos seus dados digitais[2]. Neste sentido, os dados pessoais extraídos das redes sociais durante toda a interação do usuário com a rede passam a fornecer um rico retrato da personalidade daquele indivíduo. As emoções, por exemplo, são facilmente extraídas através da utilização de *emoticons*, da emissão de posicionamento sobre determinado assunto ou até mesmo pelo ato do indivíduo mencionar nas redes sociais como está se sentindo. Estamos, a todo o momento, gerando informações e dados pessoais através de uma simples busca no *Google*, uma compra efetuada em algum site da internet que demonstra o nosso gosto e até mesmo através da nossa localização geoespacial. Em decorrência da segmentação dos indivíduos com bases nas suas informações encontradas nas redes digitais e da criação de estereótipos capazes de influenciar nas decisões automatizadas surge a necessidade de uma abordagem expressa nos ordenamentos jurídicos a respeito da proteção dos dados pessoais.

A utilização de decisões automatizadas com base na biografia digital dos indivíduos já é uma realidade presente nas diferentes tomadas de decisões, como a do processo para a concessão de crédito[3], processos seletivos[4] e até mesmo no direcionamento de diferentes tipos de

---

[1] Conforme explica Danilo Doneda, o termo 'fenômeno da datificação' se refere a "pôr em dados- praticamente toda a vida de uma pessoa". (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 85)

[2] Há como exemplo a pesquisa feita pela *National Academy of Sciences*, onde 58.000 voluntários disponibilizaram os seus dados e em específico, os seus *likes* no *Facebook*. O propósito era comprovar que muitas características da personalidade das pessoas, como religião, opção social e posicionamento político, podem ser previstas através da análise dos seus *likes* no *Facebook*, ou seja, do seu comportamento *online*. Buscou-se demonstrar a capacidade dos dados coletados *online* serem precisos e o seu nível de evasividade, que chegou a resultados extremamente coerentes com a realidade dos perfis analisados. Referente a etnia dos cinquenta e oito mil voluntários, entre os caucasianos e afrodescendentes, houve uma coerência de 95% com a real etnia dos indivíduos estudados. O sexo foi identificado em 93% dos casos e com uma identificação menor, a orientação sexual dos homens deu a taxa de 88% e entre as mulheres a de 75%. Já a religião, a taxa de acerto entre a distinção de cristãos e muçulmanos foi de 82%. Por fim, a posição política dos indivíduos analisados deu uma taxa de 85%, distinguindo-os em Democratas ou Republicanos. (KOSINSKI, Michael. *Private traits and attributes are predictable from digital records of human behavior.* ***Proceedings of the National Academy of Sciences,*** vol. 110, n. 15, 2013, p. 5802-5805)

[3] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. ***Big data:*** *a revolution will transform how we live, work and think.* New York: Hougton Miffin Publishing, 2013, p. 176.

[4] SOLOVE, Daniel J. ***The digital person****: technology and privacy in the information age*. New York: New York University Press, 2004, p.46.

mercadorias com base na capacidade econômica do consumidor[5], prática conhecida como *profiling*[6]. Neste sentido, a categorização das pessoas tendo em vista a análise dos seus dados pessoais e a capacidade de repercussão destas informações nas suas oportunidades sociais é entendida, de acordo com Viktor Mayer – Schoneberger, como a "ditadura dos dados". De acordo com o autor, as pessoas datificadas (titulares dos dados) seriam os potenciais vítimas dessa estrutura movida pelo *Big Data*, onde os algoritmos deixam de influenciar apenas na publicidade direcionada e passam a influenciar na vida das pessoas de maneira direta, decidindo a respeito das suas oportunidades[7].

Há ainda, como uma das técnicas de coleta de dados pessoais, o *data mining*, que consiste na busca de tendências e padrões de informações em grande quantidade e em "estado bruto" através de instrumentos estatísticos e matemáticos[8]. Essa técnica, por exemplo, é utilizada pela agência de investigação norte-americana (FBI) para o rastreamento de e-mails[9]. A dinâmica do aumento da capacidade de coleta, armazenamento e processamento de informações diante do desenvolvimento abrupto das técnicas de tratamento tem como consequência o acréscimo da quantidade de informação disponível sobre os indivíduos em diversas bases de dados[10]. Destarte, estas informações podem influenciar de maneira direta na vida das pessoas, pois, nas palavras de Danilo Doneda, "uma simples busca na Internet pelo

---

[5] ODLYZKO, Andrew. *Privacy, economics, and price discrimination on the internet.* ***Fifth International Conference on Eletronic Commerce,*** *pp. 355-366, N. Sadeh, ed., ACM, 2003.* Disponível em: http://ssrn.com/abstract=429762. Acesso em: 14 jun. 2020.

[6] "Tudo é calibrado com base nesses estereótipos; inclusive, o próprio conteúdo acessado na Internet. Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível, direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes, ocasionais e fortuitas, que escapariam dessa catalogação." (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 88)

[7] The dangers of failing to govern big data in respect to privacy and predictions, or of being deluded about the data's meaning, go far beyond trifles like targeted online ads". (MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. ***Big data:*** *a revolution will transform how we live, work and think.* New York: Hougton Miffin Publishing, 2013, p. 151)

[8] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 154.

[9] GEORGITON, Peter V. The FBI's Carvnivore: how federal agents may be viewing your personal e-mail and why there is nothing you can do about it. ***Ohio State Law Journal,*** vol. 62, n. 06, 2001, p. 1831-1867.

[10] "A capacidade tecnológica de memorizar informações pessoais concernentes às pessoas é praticamente ilimitada (...). Estas informações, se cruzadas com outras fontes de dados, podem determinar um perfil da pessoa, completo ou parcial, sobre o qual os indivíduos em questão não têm controle, e a verdade não pode ser confirmada. (...) A possibilidade de adquirir informações e de exercitar influencia foi incrementada até graus jamais conhecidos". (PANEBIANCO, Mario. *Bundesverfassungsgerich, dignitá umana e diritti fondamentali*. ***Diritto e Societá,*** n. 02, 2000, p. 187)

nosso nome ou pelo de pessoas conhecidas pode, em vários casos, elucidar o significado prático do registro aleatório de informações a nosso respeito[11]".

Ainda, percebe-se que, diante das diversas circunstâncias, o perfil obtido no meio eletrônico pode ser a única parte da personalidade de determinado indivíduo visível a outrem. Neste sentido, o protagonismo dos dados pessoais na sociedade da informação transformou a coleta e tratamento de dados pessoais em verdadeiros insumos. Ainda em 1995, em decisão, o Ministro Ruy Rosado de Aguiar ilustra perfeitamente este cenário de vinculação entre o possível controle de dados pessoais através do seu tratamento:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta publica e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita a sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, se quer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo[12].

2.1 NOÇÕES GERAIS E CLASSIFICAÇÕES ESPECÍFICAS

Preliminarmente, em seu capítulo I, a LGPD demonstra que se preocupa e regulamenta apenas o tratamento[13] de dados pessoais, que são definidos como quaisquer informações relacionadas à pessoa natural identificada ou identificável (art. 5º, I, da LGPD). Na mesma lógica do fato jurídico, o dado pessoal terá repercussão jurídica quando atraí o qualificador pessoal. Além dos dados pessoais, a Lei se refere expressamente aos dados pessoais sensíveis no inciso II do art. 5º e aos dados pessoais anônimos no inciso III do art. 5º. Cumpre ressaltar que, apesar de estarem sujeitos a prerrogativas diferenciadas, até mesmo os dados pessoais considerados públicos ou tornados públicos pelos titulares estão sobre proteção da Lei. Neste sentido, os §3 e §4 do art. 7º, respectivamente, preveem que:

---

[11] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 154.

[12] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 22.337/RS. Relator: Ministro Ruy Rosado de Aguiar. Data de julgamento: 20 mar. 1995.

[13] "O tratamento de dados pessoais engloba uma multiplicidade de situações, sendo assim considerado o tratamento, conforme previsto no art. 5º, X, da LGPD, como toda operação realizada com dados pessoais, como exemplo, as relacionadas à "coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

No que se refere aos termos utilizados pela Lei para caracterizar a pessoa natural (identificada e identificável), Catarina Sarmento Castro explica que "entende-se por identificado o indivíduo que já é conhecido, e por identificável a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros[14]". Neste ponto, resta evidente que a proteção não atinge diretamente os dados de pessoas jurídicas, planos estratégicos, *softwares*, patentes, algoritmos, documentos confidenciais, dentre outros tipos de informações/documentos que não estejam relacionados à pessoa natural[15]. Não significa, no entanto, que estes tipos de informações não possuem tutela, havendo como alguns dos exemplos de diplomas legais que os amparam a Lei de Direitos Autorais (Lei 9.610/1998), a Lei de Propriedade Industrial (Lei 9.279/1996) e a Lei de Software (Lei 9.609/1998).

As leis de proteção de dados se caracterizam como um conjunto de normas que acabam por proteger outros direitos[16]. Neste sentido, a LGPD demonstra logo em seu art. 1º que objetiva a proteção dos diretos fundamentais da liberdade e da privacidade, possibilitando o livre desenvolvimento da personalidade da pessoa natural identificada ou identificável. Apesar da proteção de dados pessoais estar intrinsicamente ligada ao direito à privacidade, não se limita a ele. Considerando a possibilidade de estigmatização das pessoas ao serem segmentadas com base no tratamento das suas informações, a exemplo da criação de estereótipos e limitação de direitos (segregação), o direito à proteção de dados também abarca diversos outros direitos da personalidade.

Em entrevista à imprensa do STJ (2019), Ronaldo Lemos afirmou que estávamos vivendo a era dos dados e que estes são a representação do indivíduo no meio virtual. Sendo assim, "dados" e "informações" podem ser considerados pontos de referência para a compreensão da sociedade da informação. A relação entre informação e dado é inegável, e, neste ponto, Danilo Doneda se refere aos dados pessoais como uma informação em potencial, uma pré-

---

[14] CASTRO, Catarina Sarmento. **Direito da informática, privacidade e dados pessoais.** Coimbra: Editora Almedina, 2005, p. 70-71.

[15] Neste ponto, cumpre observar que, quando alguns destes documentos que não estão sob o campo de proteção da LGPD contiverem dados pessoais, eles estarão tutelados pela legislação, cabendo à análise dos dados pessoais estruturados e não estruturados.

[16] "A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio". (RODATÁ, Stefano. **A vida na sociedade da vigilância.** DONEDA, Danilo; DONEDA, Luciana Cabral (Trad.). Rio de Janeiro: Editora Renovar, 2008, p. 17).

informação, que para se tornar uma informação de fato terá que passar por um processo de elaboração[17]. O processo de elaboração a que se refere o autor retrata a figura do banco de dados[18], elemento essencial no processo de tratamento de dados pessoais. Ainda, caracterizando o tratamento indistinto pela LGPD, a definição de informação pessoal no art. 4º, IV da Lei 12.527/2011 (Lei de Acesso à Informação) também se conceitua como toda informação relacionada à pessoa natural identificada ou identificável.

2.1.1 Dados anônimos

Diferentemente dos dados pessoais, os dados pessoais anônimos fazem referência a pessoas indeterminadas[19] e, portanto, possibilitam uma maior capacidade protetiva aos seus titulares. Seguindo a lógica da definição de dados pessoais como a informação relacionada à pessoa identificável ou identificada (art. 5º, I, da LGPD), os dados anônimos, caracterizados pela inexistência de vínculo entre os dados e o seu respectivo titular (art. 5º, III, da LGPD), fogem da tutela jurídica prevista na Lei Geral de Proteção de Dados exatamente por não serem identificados ou identificáveis[20]. Neste sentido, por se encontrarem fora do escopo de aplicação da LGPD, conclui-se que há uma maior liberdade no tratamento de dados anonimizados.

---

[17] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 137.

[18] "Os bancos de dados consistem, basicamente, em conjuntos de informações organizadas segundo uma determinada lógica" Nesse mesmo sentido, MANNINO, Michael V. Projeto, desenvolvimento de aplicações e administração de banco de dados. Trad. Beth Honorato. São Paulo: McGraw-Hill, 2008, p.3: "Os bancos de dados contêm uma enorme quantidade de dados sobre muitos aspectos da nossa vida: preferências de consumo, uso de telecomunicações, histórico de crédito, hábitos ao assistir à televisão e assim por diante. A tecnologia de banco de dados ajuda a consolidar essa massa de dados e transformá-la em informação útil para a tomada de decisão. Os gestores usam a informação recolhida nos bancos de dados para tomar decisões de longo prazo como investir em fábricas e equipamentos, escolher a localização de lojas, adicionar novos itens ao estoque e entrar em novos negócios." (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 137)

[19] "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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[20] "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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

Acontece que, conforme explica Bruno Bioni, "sempre existirá a possibilidade de uma base de dados anonimizada ser agregada a outra para a sua reidentificação[21]". Neste sentido, há uma entropia da informação, caracterizada pela possibilidade de reversibilidade da anonimização de dados pessoais através do uso de uma informação auxiliar. A própria Lei Geral de Proteção de Dados prevê essa possibilidade quando estabelece como exceção à regra de não consideração de dados anônimos como dados pessoais quando "o processo de anonimizacão ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido[22]".

Há como exemplo de dados pessoais anônimos os dados estatísticos. Estes, em específico, devem ser analisados com ressalva do tamanho do espaço amostral que está ocorrendo o tratamento, uma vez que a redução no número de dados sob a análise pode levar à identificação dos titulares[23]. A possibilidade de reidentificação dos dados até então anônimos é demonstrada através da pesquisa efetuada por Arvind Narayanan e Vitaly Shmatikov no caso *Netflix Prize*. Em 2006, com o objetivo de aprimorar o seu algoritmo de sugestão de filmes, a maior provedora de *streaming* de filmes do mundo criou um concurso que daria um milhão de dólares para quem conseguisse melhorar em pelo menos 10% o aproveitamento da plataforma. Desta forma, disponibilizaram a sua base de dados com todas as notas das avaliações de filmes feitas pelos seus usuários no período de 1998 a 2005 e as suas respectivas datas, suprimindo, no entanto, os nomes dos usuários avaliadores[24].

Acontece que, no ano posterior, Arvind Narayanan e Vitaly Shmatikov identificaram dois usuários que participaram do concurso através do cruzamento de dados disponíveis na Internet *Movies Databases*/IMDB. O IMDB é um site que tem como objetivo o compartilhamento de impressões sobre filmes em geral, onde as pessoas, na maioria das vezes, utilizam o seu nome verdadeiro ao acessarem e emitirem as suas opiniões. Portanto, o elemento que caracterizava os dados utilizados no concurso da *Netflix* como dados anônimos, foi desvendado através dos nomes contidos nas avaliações do site *Internet Movies Databases*,

---

[21] BIONI, Bruno. **Xeque-mate:** o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: Editora Saraiva, 2015, p. 28.

[22] "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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[23] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 201.

[24] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust. ***De-anonymization of large sparse datasets.*** 2007. Disponível em: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf. Acesso em: 14 jun. 2020.

demonstrando a possibilidade de agregação de duas bases de dados distintas para a reidentificação dos dados anonimizados.

Para mitigar os riscos de reidentificação do titular de dados pessoais anônimos, como ocorreu no Caso *Netflix Prize*, o processo de anonimazação deve ocorrer através de técnicas específicas. A Opinião 05/2014, emitida levando em consideração a Diretiva 95/46[25] da União Europeia, prevê algumas destas técnicas que objetivam a eliminação dos elementos identificadores de uma base de dados. Dentre elas, destacam-se a: generalização[26] e a supressão[27]. No entanto, para Caio César. C. Lima[28], independentemente da técnica de anonimização utilizada, é importante garantir que ela não trará registros capazes de identificar o indivíduo ou sequer fazer algum *link* com ele.

2.1.1.1 O filtro da razoabilidade na LGPD

Diante da possibilidade de dados anonimizados serem reidentificados e transformarem-se em dados pessoais,[29] as leis que adotam a teoria Expansionista[30] em detrimento da teoria

[25] EUROPEAN COMISSION. ***Article 29 Working Party.*** Disponível em: https://ec.europora.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 15 mar. 2020.

[26] Em relação aos tipos de generalização, método utilizado para que o grau de identificabilidade do sujeito seja reduzido/eliminado, Bruno Bioni explica: "generalização do nome completo**:** constaria apenas o prenome, desde que fosse observado que os nomes da base de dados não são comuns. O objetivo é evitar que um nome possa ser atribuído a um indivíduo em específico; generalização da localização geográfica: em vez de disponibilizar o número completo do CEP, seriam divulgados apenas os seus primeiros dígitos. Assim, haveria uma localização menos detalhada, a fim de quebrar o vínculo de identificação desta informação com um sujeito; generalização da idade: em vez de divulgar a idade exata, seria divulgada a faixa etária para viabilizar a categorização dos indivíduos como jovens, adultos ou idosos (coluna "E") e, por outro lado, inviabilizar a sua individualização, dado o universo de pessoas que se enquadram naquela mesma faixa etária". (BIONI, Bruno. Dados "anônimos" como antítese de dados pessoais: o filtro da razoabilidade. **Revista GENJurídico,** 2019. Disponível em: http://genjuridico.com.br/2019/10/11/dados-anonimos-antitese-dados-pessoais/. Acesso em: 15 abr. 2020)

[27] Há como exemplo a supressão do CPF, "por ser um identificador capaz de diferenciar até mesmo pessoas homônimas, sendo um identificador único; logo, a sua disponibilização, ainda que parcial –e.g., cinco primeiros dígitos –, não seria prudente". (BIONI, Bruno. Dados "anônimos" como antítese de dados pessoais: o filtro da razoabilidade. **Revista GENJurídico,** 2019. Disponível em: http://genjuridico.com.br/2019/10/11/dados-anonimos-antitese-dados-pessoais/. Acesso em: 15 abr. 2020)

[28] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 201.

[29]: "Torna-se cada vez mais recorrente a publicação de estudos que demonstram ser o processo de anonimazação algo falível. (...) A agregação de diversos 'pedaços' de informação (dados) poder revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico". (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 63-65)

[30] A teoria Expansionista define o conceito de dados pessoais com base no alargamento da sua qualificação, sendo o titular uma pessoa identificável, indeterminada e, portanto, estabelecendo um vínculo mediato, impreciso ou inexato. (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 63-65)

Reducionista[31] e, ao mesmo tempo, diferenciam os dados pessoais dos dados anônimos, correriam o risco de serem redundantes e contraditórias. Levando-se em consideração que os dados anônimos são potencialmente inidentificáveis, a dicotomia estabelecida entre os dois tipos de dados leva à tautologia das leis que adotam o conceito expansionista de dados pessoais[32]. Para não gerar tal incoerência, a LGPD estabeleceu o critério da razoabilidade para delimitar a elasticidade do conceito expansionista, ou seja, determinar até que ponto os dados pessoais são identificáveis. Sob o ponto de vista da LGPD, a reversão do processo de anonimização e a caracterização destes dados como dados pessoais deve se dar por meios próprios e com esforços razoáveis[33].

No que tange o filtro da razoabilidade utilizado pela LGPD, assim como pela GDPR[34], Bruno Bioni explica que:

> Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo identificável. Essa vinculação deve ser objeto de um "esforço razoável", sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável. Ao *contrário sensu*, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o "filtro da razoabilidade" barra o seu enquadramento como aquele relacionado a uma pessoa identificável[35].

Portanto, o legislador brasileiro, ao invés de apontar um método específico, utilizou o conceito da razoabilidade. Por ser a utilização da razoabilidade para delimitar a utilização do termo 'identificável' um conceito indeterminado, pode se adequar ao próprio desenvolvimento da tecnologia. Contudo, delimitou a discricionariedade deste exercício interpretativo através da utilização de três fatores delimitativos da razoabilidade: a) custo; b)

---

[31] A teoria Reducionista se refere ao titular de dados como uma pessoa específica, identificada, com vínculo imediato, direito e preciso. (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 63-65)

[32] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 68.

[33] "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual forem submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido." (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[34] "Personal data which have undergone pseudonymisation (…) should be considered to be information on an identifiable natural person whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used (...)To ascertain whether means are reasonably (...) should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology". (UNIÃO EUROPEIA. ***General Data Protection Regulation.*** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[35] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 65-65.

tempo; c) estágio da tecnologia adotada[36]. Sendo assim, a reversão do processo de anonimização deve ser analisada com base nos seus custos e morosidade, de acordo com as tecnologias disponíveis à época.

2.1.1.2 Dados pseudominizados

A pseudonimização é uma técnica de anonimização considerada por grande parte da doutrina como ineficiente e superficial[37], pois, conforme define o §4º do art. 13 da LGPD[38], trata-se de hipótese onde o próprio agente de tratamento possui os meios próprios para a transmutação do dado anonimizado em dado pessoal. Ou seja, ao ponto em que o dado pessoal apenas perde a possibilidade de associação aos seus titulares através da substituição de identificadores indiretos ou diretos, como o nome e CPF, tais pseudônimos continuam sendo um retrato indireto dos indivíduos. Diferentemente do GDPR, que regulou essa técnica prevendo o relaxamento de algumas obrigações legais no tratamento de dados submetidos ao processo da pseudonimização, a LGPD sequer traçou incentivos para a sua adoção no tratamento de dados pelos agentes. Apenas citou de maneira assistemática, sendo inclusive uma das últimas inclusões na Lei pelo relator, deputado Orlando Silva[39].

---

[36] "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual forem submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve leva rem consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusive de meios próprios." (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[37] "Para muitos, a pseudonimização não é considerada uma técnica de anonimização. Isso porque se substituem, apenas, os identificadores diretos – e.g., nome, CPF, etc. – por pseudônimos – e.g., números aleatórios, de modo que a pessoa permanece sendo identificável em razão de tais pseudônimos serem um retrato detalhado indireto delas." (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 62)

[38] "Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. [...] § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro." (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[39] "Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados,

2.1.2 Dados pessoais sensíveis

Conforme define o art. 5º, II, dados pessoais sensíveis são dados que indicam informações acerca da origem racial ou étnica, convicção religiosa, saúde ou à vida sexual, dado genético ou biométrico, opinião política, dentre outras características vulneráveis, de pessoa natural, que quando submetidas a tratamento oferecem um conteúdo que poderá ser utilizado de forma discriminatória no futuro[40]. Um eventual incidente de segurança com os dados pessoais sensíveis poderá trazer consequências muito mais gravosas aos direitos dos titulares. Logo de início, fica evidenciado que, do próprio conceito de dados sensíveis extraído da LGPD, o seu tratamento deve ser precedido de um cuidado ainda maior por parte dos agentes de tratamento. Demonstrando tal preocupação, a Lei estabelece algumas restrições ao tratamento de dados pessoais sensíveis, dentre elas, destacam-se as vedações ao tratamento dos dados em referência para a execução de contrato, proteção de crédito e com base no interesse legítimo do agente de tratamento.

Ainda, é fundamental a proteção dos dados pessoais que, embora não qualificados como dados sensíveis, a depender do tratamento que são submetidos, revelam informações que oferecem uma especial vulnerabilidade[41]. Laura Schertel Mendes entende que, a possibilidade de um dado insignificante revelar informações sensíveis ocorre através de "um tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias[42]". No julgamento sobre a Lei do Recenseamento, por exemplo, o Tribunal Constitucional Alemão afirmou que, diante das tecnologias disponíveis que permitem correlacionar diferentes tipos de dados, possibilitando a previsão de

---

bem como considerem os devidos padrões éticos relacionados a estudos e pesquisa. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020).

[40] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 142.

[41] 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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[42] MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de Brasília, Brasília, Distrito Federal, 2008, p. 62. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf. Acesso em: 10 abr. 2020.

comportamentos e acontecimentos, um dado, que antes era considerado como insignificante, pode revelar aspectos considerados sensíveis[43].

Em razão do conteúdo destas informações oferecerem uma especial vulnerabilidade e apresentarem maiores riscos aos seus titulares, a LGPD, assim como o GDPR[44], dedica um regime jurídico mais protetivo para os dados pessoais sensíveis, inibindo as possíveis práticas discriminatórias[45]. O regime jurídico brasileiro, ao invés de proibir a utilização de dados sensíveis, estabelece em seu art. 11, de maneira taxativa, oito hipóteses legais que podem ser utilizadas pelos agentes para a operação do seu tratamento de forma legítima.

2.2 A EVOLUÇÃO NA PROTEÇÃO DE DADOS PESSOAIS

Como consequência da crescente e contínua evolução das tecnologias de tratamento de dados pessoais[46], as relações sociais se apresentam de uma nova forma. Neste novo viés, o dado pessoal se tornou o elemento principal para o desenvolvimento da economia[47], caracterizando-se, nas palavras do Professor Ronaldo Lemos[48] como o "novo petróleo". Ainda que a constante vivência no ciberespaço não seja o meio exclusivo e resultante da sociedade da informação, é, sem dúvidas, instrumento essencial neste processo[49]. No entanto, diante da

---

[43] MARTINS, Leonardo. **Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão.** Montevidéu: Fundação Konrad Adenauer, 2005, p. 244-245.

[44] "Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas". (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[45] "Tal tutela jurídica procura assegurar que o titular dos dados pessoais possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto. Com isso, pretende-se garantir a ausência de trações diferenciais nas relações sociais, a fim de possibilitar que o indivíduo desenvolva livremente a sua personalidade". (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 85)

[46] Como: Profiling, Data Mining, Scoring e Online Analytical Processing.

[47] SIQUEIRA JR., Paulo Hamilton. **Teoria do Direito.** São Paulo: Editora Saraiva, 2009, p.218.

[48] LEMOS, Ronaldo. **Debater a Lei Geral de Proteção de Dados é refletir sobre o futuro, afirma Ministro Salomão.** 26 ago. 2019. Disponível em: **http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Debater-a-Lei-Geral-de-Protecao-de-Dados-e-refletir-sobre-o-futuro--afirma-ministro-Salomao.aspx.** Acesso em: 29 jun. 2020.

[49] "Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente, que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais. Há uma nova compreensão (mais abreviada) da relação entra tempo-espaço, o que outrora acarretava maior cadência às interações sociais." (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 04)

capacidade do processamento de dados disponibilizados nas redes sociais revelarem verdadeiramente uma parcela da personalidade dos indivíduos, é que se consolida ainda mais a necessidade de uma legislação de proteção de dados pessoais no Brasil.

Diante da complexidade dos efeitos que a má utilização de dados pessoais pode causar na vida do titular, a tutela jurídica dos dados pessoais não pode ser entendida como uma mera evolução do direito à privacidade[50]. Diferentemente, o direito à proteção de dados pessoais passa a ser pressuposto para que a pessoa não seja controlada pelos agentes de tratamento, que não tenha a sua autonomia privada cerceada e em última análise, a inibição do livre desenvolvimento da sua personalidade[51]. A respeito da necessidade da normatização do direito à proteção de dados pessoais, Bruno Biondi se refere a tal direito como um "novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação[52]".

Por certo, a regulamentação sobre a proteção de dados pessoais é elemento essencial para uma maior compreensão acerca da relação do consentimento do titular de dados com o processo tratamento de dados pessoais. Assim, faz-se necessário a análise da evolução na proteção de dados nos modelos de *common law* e *civil law*, para que haja um maior entendimento acerca das leis que influenciaram de forma direta na normatização da proteção de dados no Brasil e principalmente na criação da LGPD. No entanto, cumpre destacar que essa divisão entre modelos normativos de proteção de dados pessoais entre os sistemas de *common law* e *civil law* não é taxativa[53].

---

[50] "A proteção de dados pessoais, em suma, propõe o tema da privacidade, porém, modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão". (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 173)

[51] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 128.

[52] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 90.

[53] "A diversidade entre os sistemas de *common law* e *civil law* certamente exerceu influencia no desenvolvimento de diferentes regimes de proteção de dados pessoais, sendo que uma certa resistência de países da esfera common law em vincular a matéria aos direitos fundamentais ou a modelos como o da tutela da dignidade pode ser mencionada como sintomática da diferença entre enfoques. Ao mesmo tempo, deve-se ter em conta que essa divisão não é taxativa e que países que fazem parte da geografia do *common law*, como a Austrália, a Nova Zelândia e o Canadá, entre outros, apresentam hoje características mistas em suas disciplinas de proteção de dados pessoais, denotando em alguns casos, uma aproximação real de elementos do modelo europeu –além do caso do Reino Unido que, mesmo após sua saída de União Europeia, deverá continuar sob o efeito direto da normativa europeia". (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 186)

2.2.1 O modelo europeu de proteção de dados pessoais

Atualmente, o modelo europeu de proteção de dados pessoais, reconhecido pela sua sistematicidade, está ordenado basicamente pelo *General Data Protection Regulation* (GDPR), que foi, inclusive, a principal fonte de inspiração para a LGPD[54]. O regulamento europeu, que objetiva a harmonização do até então fragmentado sistema de proteção de dados pessoais na União Europeia, estruturado através de diretivas, reflete a necessidade de adaptação às novas tecnologias e aos modelos de negócio que são, em sua maioria, movidos por dados. Porém, entende-se que apenas em 1995 houve uma efetiva padronização no ramo da proteção de dados pessoais na União Europeia com a Diretiva 95/46/CE[55] do Parlamento Europeu e do Conselho.

Assim como a Convenção 108, a abordagem da proteção de dados como um direito fundamental é evidente na Diretiva 95/46/CE, sendo a própria expressão "direitos fundamentais" mencionada seis vezes nas suas considerações iniciais. Ainda, garante a proteção da pessoa em relação ao tratamento de seus dados pessoais[56], visando à unificação normativa para a criação de um mercado interno na Europa[57], tendo em vista a circulação de dados pessoais[58]. Apesar de se situar na quarta geração das leis de proteção de dados pessoais[59], a referida Diretiva, na tentativa de operacionalização do consentimento, qualifica-o

---

[54] VIEIRA, Débora. O que você precisa saber sobre a lei geral de proteção de dados. **Migalhas,** 01 ago. 2018. Disponível em: https://www.migalhas.com.br/depeso/284723/o-que-voce-precisa-saber-sobre-a-lei-geral-de-protecao-de-dados. Acesso em: 29 jun. 2020.

[55] UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho,** de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20 maio. 2020.

[56] "Os Estados-membros assegurarão, em conformidade com a presente directiva, a proteccção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais". (UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho,** de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20 maio. 2020.)

[57] SWIRE, Peter; LITAN, Robert. ***None of your business.*** Washington: Brookings Institution Press, 2010, p. 25.

[58] "Consideranda 56: Considerando que os fluxos transfronteiras de dados pessoais são necessários ao desenvolvimento do comércio internacional; que a protecção das pessoas garantida na Comunidade pela presente directiva não obsta às transferências de dados pessoais para países terceiros que assegurem um nível de protecção adequado; que o carácter adequado do nível de protecção oferecido por um país terceiro deve ser apreciado em função de todas as circunstâncias associadas à transferência ou a uma categoria de transferências". (UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho,** de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20 maio. 2020)

[59] As gerações de leis de proteção de dados são aprofundadas no Capítulo 4.1, com enforque no instituto do consentimento.

como livre, informado, inequívoco, explícito e/ou específico[60], assim como o direito de controle de dados por parte do seu titular, ideias extraídas da Convenção 108 e das *guidelines* da OCDE. No entanto, conforme entende Bruno R. Bioni, a ausência do elemento de cooperação trazido pela Diretiva 95/46/CE nas *Guidelines* é o que diferencia a inserção em diferentes gerações de leis de proteção de dados pessoais[61].

Em 2002 foi aprovada a Diretiva 2002/58/CE do Parlamento e do Conselho Europeu, que atualmente se encontra em processo de atualização diante da futura *ePrivacy Directive* e que se refere à proteção da privacidade no setor das comunicações eletrônicas. Apesar de não trazer inovações na área de proteção de dados pessoais, a diretiva aborda questões específicas acerca dos serviços de comunicações eletrônicas, a exemplo do envio de mensagens eletrônicas não solicitadas, *cookies*[62], utilização de dados pessoais em listas telefônicas, dentre outros[63]. Ainda, indica as formas de consentimento consideradas adequadas[64], devendo, em todas as circunstâncias, ser exercido previamente ao tratamento de dados pessoais[65].

Apesar das diretivas serem um instrumento normativo comum da União Europeia para a realização da uniformização legislativa entre os países-membros, a sua incorporação e validade tem como pressuposto um processo de aprovação denominado de transposição. Ou seja, diferentemente das Regulamentações, que possuem aplicabilidade direta em todos os

---

[60] UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho,** de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20 maio. 2020.

[61] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 119.

[62] "Um cookie nada mais é que um pequeno arquivo de texto que contém uma etiqueta de identificação exclusiva, colocada no seu computador por um site. Neste arquivo, várias informações podem ser armazenadas, desde as páginas visitadas até os dados fornecidos voluntariamente ao site. Quando você visita em um site, informações pessoais, como seu nome, e-mail e interesses pessoais são armazenadas em um cookie e enviadas ao seu navegador da internet, que então as guarda para uso posterior. Da próxima vez que você for para o mesmo site, ele pode reconhecê-lo. Como você pode imaginar, estudar o comportamento do consumidor online —sabendo quando ele esteve em seu website, as páginas que visualizou, quanto tempo gastou em cada uma delas e quantas vezes voltou — é uma iniciativa extremamente poderosa de vendas e de marketing." (BATISTA, Adonis. Você sabe o que são cookies? Conheça os 3 tipos. **Blog Hariken.co,** 2019. Disponível em: https://blog.hariken.co/voce-sabe-o-que-sao-cookies-na-internet-conheca-os-3-tipos/. Acesso em: 20 jul. 2020.)

[63] UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho,** de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20 maio. 2020.

[64] UNIÃO EUROPEIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho,** de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações eletrônicas (Directiva relacionada à privacidade e às comunicações electrónicas). 12 jul. 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058. Acesso em: 20 jul. 2020.

[65] UNIÃO EUROPEIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho,** de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações eletrônicas (Directiva relacionada à privacidade e às comunicações electrónicas). 12 jul. 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058. Acesso em: 20 jul. 2020.

países-membros da UE, as diretivas precisam ser incorporadas aos ordenamentos jurídicos de cada um dos países[66], dificultando o objetivo de um direito comunitário e de um Mercado Comum Digital[67]. Portanto, neste aspecto, nasceu à necessidade de uniformização legislativa, que veio a se concretizar por meio do GDPR, tendo em vista, principalmente, a ineficácia das leis de direito interno para a proteção de dados diante a possibilidade de coleta e tratamento de dados pessoais fora da soberania dos estados.

2.2.2 O sistema norte-americano de proteção de dados pessoais

O caráter fragmentado do modelo norte-americano referente à proteção de dados pessoais decorrente de um modelo legislativo formado pela divisão de competências entre governo federal e estados se torna ainda mais acentuado diante da ausência de um tratamento particularizado pela Suprema Corte e da discrepante variação no nível de proteção de dados pessoais de um estado para outro[68]. Embora os Estados Unidos não possuam uma lei geral de proteção de dados a nível federal, há leis sobre o tema a nível estadual, assim como diversas leis federais que envolvem a privacidade e a segurança de dados e informações.

O estado da Califórnia, por exemplo, foi o primeiro a criar uma agência para a proteção da privacidade nos Estados Unidos[69], caracterizando-se como um dos estados com o mais alto nível de proteção aos dados pessoais no país, em contraposição a estados como Delaware, Kansas, Kentucky, North Carolina e Texas, que se caracterizam como os estados com níveis de proteção de dados mais baixos aplicados no país. Ainda, recentemente, em 2018, foi aprovada a *California Consumer Privacy Act*, que visa à regulamentação da proteção de dados na Califórnia. No que se refere à ideia de um perfil protetivo conferido às informações pessoais (i*nformational privacy)*, a atuação da Federal Trade Comission para a coibição de práticas desleais no comércio merece destaque. A lei antitruste criada pela FTC ainda em

---

[66] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 187.

[67] O *Digital Single Market* é uma estratégia firmada pela Comissão Europeia que visa à facilitação do acesso ao mundo digital tanto para os indivíduos, quanto na área dos negócios. No campo dos negócios, o DSM adequa as dinâmicas do mercado digital, havendo como consequência o crescimento da economia digital na Europa.

[68] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 247.

[69] A Agência para a proteção da privacidade – The Office of Privacy Protection possui uma linha de atuação baseada em 4 áreas básicas de responsabilidade que são estabelecidas no California Business and Professions Code: "assisting consumers with identity theft and other privacy –related problems; providing information and education on privacy issues; working with law enforcement on investigations of identity theft and other privacy-related crimes; recommending policies and practices that protect individual privacy rights.

1914 apresentava diversos pontos essenciais para a proteção de dados pessoais, como exemplo da *do-not-call list* – uma lista de números eletrônicos de pessoas que não possuem interesse em receber propostas comerciais por telefone[70].

Embora o sistema normativo europeu se destaque como fonte do principal e mais completo conjunto de leis sobre proteção de dados pessoais, o *right to privacy*, que possui relação intrínseca com a proteção de dados, foi desenvolvido originalmente na jurisprudência e doutrina norte-americana. Sendo extremamente valorizada e prezada pelo cidadão norte-americano[71], o desenvolvimento do ordenamento em relação à privacidade demonstra como é tratado o tema de proteção de dados pessoais. Dentre as diversas leis federais que tutelam a privacidade e segurança de dados e informações, destacam-se, o *Fair Credit Reporting Act*, o *Privacy Act* de 1974[72] e o *Cable Comunications Policy Act* (CCPA)[73].

A importância do FCRA vem da sua forte influência na legislação brasileira na referida matéria[74] e da sua relação com os *Fair Information Practices Principles*[75]. A lei estabeleceu obrigações de segredo e correção para os operadores de cadastro de crédito e consumo no tratamento de dados financeiros dos consumidores. Ainda, determinou as condições e casos de possibilidade de revelação de dados pessoais dos consumidores por parte dos operadores. Os casos permitidos pela lei são, alternativamente, cumprimento de ordem judicial, com o consentimento do consumidor ou quando existem razões para se acreditar que se pretende utilizar estas informações para verificações concernentes a qualquer requisição do interessado de crédito, seguro, emprego, benefícios do governo, dentre outros.

A relação da proteção de dados pessoais com o direito à privacidade pode ser vista no Privacy Act de 1974, que se caracteriza como a primeira lei norte-americana que reconhece a existência de um direito geral de privacidade (*general right to privacy*). Apesar de aplicar

---

[70] FEDERAL TRADE COMISSION. **Do not call registry.** Disponível em: https://www.donotcall.gov/report.html. Acesso em: 18 abr. 2020.

[71] "*Americans cherish privacy. We spend a great deal of money and effort to obtain it. In youth we flee ou parents' homes for the privacy of a place of our own. We design homes for our privacy. As students we prefer apartments to dormitories (...) We strive to save enough money so we will be able to afford in our old age a care facility where we can have the privacy of our own apartment". ANDERSON, David. "The failure of American privacy law".* (BRASIL MARKENSINIS (Org.). **Protecting privacy.** Oxford: Oxford University Press, 1999, p. 139.)

[72] UNITED STATES OF AMERICA. **5 U.S CODE § 552.** Public information; agency rules, opinions, orders, records, and proceedings. Disponível em: https://www.law.cornell.edu/uscode/text/5/552. Acesso em: 10 maio. 2020.

[73] UNITED STATES OF AMERICA. **47 U.S. CODE § 521.** Purposes. Disponível em: https://www.law.cornell.edu/uscode/text/47/521. Acesso em: 10 maio. 2020.

[74] BENJAMIN, Antônio Herman de Vasconcellos. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto.** 5 ed. Rio de Janeiro: Editora Forense Universitária, 1997, p. 327.

[75] BENNET, Colin. ***Regulating privacy, data protection and public policy in Europe and the United States.*** Ithaca: Cornell University Press, 1992, p. 97.

somente a órgãos federais, tal lei apresenta alguns avanços, como a possibilidade de os cidadãos acessarem os seus dados pessoais em arquivos governamentais e retificá-los quando corresponderem à realidade. Ainda, verifica-se o instituto do consentimento como elemento central da lei, sendo somente possível a divulgação de informações pessoais pelos órgãos com o consentimento do interessado[76]. A violação desta regra imposta pelo Privacy Act de 1974 enseja sanções civis[77] e criminais[78].

Já o *Cable Communications Policy Act* de 1984, integra o conjunto legislativo referente às telecomunicações e estabelece um rol de direitos relativos aos dados pessoais dos assinantes de serviços de televisão a cabo. Como resultado, as operadoras destes serviços ficaram impedidas de coletarem informações pessoais dos seus assinantes que não sejam necessárias para a operação do sistema sem a autorização dos respectivos titulares dos dados. Ainda, são obrigadas a enviarem aos assinantes um relatório anual, detalhando quais são as informações em seu poder, bem como uma explicação acerca da utilização delas na empresa.

Não obstante, diante do fenômeno da circulação internacional de dados pessoais, há uma crescente pressão por uma legislação federal sobre proteção de dados nos Estados Unidos. Neste seguimento, conforme entende Danilo Doneda, "a forte demanda por uma regulação uniforme e segura nesse âmbito deixa clara a escassa eficácia de inciativas normativas nacionais que sejam isoladas e em desalinho com padrões internacionais[79]". Ainda, cumpre ressaltar que, uma tutela mais frágil de dados pessoais em determinada localidade compromete e prejudica a inteira estrutura composta também por países que proporcionam uma tutela reforçada[80].

---

[76] "No agency shall disclose any record which is contained in a system of records by any means of communicaton to any person, or to another agency, except pursuant to a written request by, or with the prior writeen consent of the individual to whom the record pertains (subject to 12 exceptions)." (UNITED STATES OF AMERICA. **5 U.S CODE § 552.** Public information; agency rules, opinions, orders, records, and proceedings. Disponível em: https://www.law.cornell.edu/uscode/text/5/552. Acesso em: 10 maio. 2020.)

[77] UNITED STATES OF AMERICA. **5 U.S CODE § 552.** Public information; agency rules, opinions, orders, records, and proceedings. Disponível em: https://www.law.cornell.edu/uscode/text/5/552. Acesso em: 10 maio. 2020.

[78] UNITED STATES OF AMERICA. **5 U.S CODE § 552.** Public information; agency rules, opinions, orders, records, and proceedings. Disponível em: https://www.law.cornell.edu/uscode/text/5/552. Acesso em: 10 maio. 2020.

[79] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 249.

[80] "Vide o caso dos 'paraísos financeiros', ou dos seus correspondentes na área dos dados pessoais, os centros de processamento de informações em locais nos quais o seu tratamento não é disciplinado pelo direito, verdadeiras 'zonas de não direito' no que se refere à proteção de dados pessoais, que funcionam como entrepostos para a realização de operações com informações pessoais que não seriam lícitas no local de origem dessa informação". (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 249)

2.2.3 O ordenamento jurídico brasileiro e a proteção de dados pessoais

A proteção de dados pessoais no ordenamento jurídico brasileiro veio a se estruturar em torno de um conjunto normativo unitário recentemente, por meio da LGPD. Ainda assim, por estar em seu período de *vacatio legis*, atualmente, a tutela dos dados pessoais é extraída de documentos esparsos, como o Código Civil (Lei nº 10.406/2002), a Lei do Cadastro Positivo (Lei nº 12.414/2011), a Lei de Acesso à Informação Pública (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014), como também é vinculada à cláusula geral da personalidade prevista na Constituição Federal. De forma extremamente importante, com o intuito de proporcionar ao cidadão um instrumento de conhecimento e retificação das suas informações pessoais armazenadas em bancos de dados de caráter público, foi instituído o *habeas data*[81]. O *habeas data* foi instaurado em um contexto reativo, onde tanto a sociedade, quanto o ordenamento jurídico estavam se recompondo de um período no qual diversas liberdades individuais foram extintas. Por ter nascido como um remédio para um problema específico, tal instituto não se demonstra plenamente eficaz ao ser aplicado em situações completamente diversas[82].

Ao decorrer do tempo, diversas limitações foram impostas na utilização deste instituto, sendo algumas delas superadas e outras não. Há como exemplo a superação do entendimento de que por se tratar o *habeas data* de ação personalíssima, morreria com o titular dos dados e, portanto, o entendimento jurisprudencial nos primeiros momentos de aplicação da ação era pela improcedência do pedido de *habeas data* formulado pelos parentes de pessoas mortas pelo regime militar que tentavam obter informações sobre os familiares desaparecidos[83]. Também, é objeto de discussão doutrinária e jurisprudencial a ambiguidade da expressão bancos de dados "de caráter público". Com base no art. 43 do CDC, que equipara a atuação

---

[81] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] LXXII - conceder-se-á *habeas data:* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jun. 2020.)

[82] "O habeas data foi criado com objetivos próprios, diferentes daqueles que inspiram os meios de garantia do direito à informação genericamente considerado". (DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. **Revista de la Faculdad de derecho de la Pontifícia Universidad Católica Del Peru**, n. 51, 1997, p. 99)

[83] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 274.

dos arquivos de consumo àquela de entidades de caráter público, entende-se, de forma majoritária tanto na doutrina, quanto na jurisprudência, pela extensão da abrangência da ação de *habeas data* para além dos órgãos públicos[84].

Sob o olhar de Danilo Doneda, a maior limitação do *habeas data* decorre do contexto no qual está inserido:

> Um sistema de proteção de dados pessoais que possui como instrumentos principais de atuação o recurso a uma ação judicial (e isso somente após o périplo administrativo) não se apresenta como um sistema adequado às exigências das matérias. Os problemas relacionados ao tratamento de dados pessoais, conforme observamos, processam-se cada vez mais "em branco", sem que o interessado perceba. Este, nas situações em que sabe ou suspeita da falsidade dos seus dados armazenados em algum banco de dados, ou do uso indevido que é feito deles – ou quando deseja simplesmente fazer uma verificação – encontra-se diante da necessidade de recorrer a uma incerta via administrativa (cujo não atendimento, aliás, não acarreta nenhuma penalidade objetiva ao responsável pelo armazenamento dos dados) e, no insucesso dessa tentativa, deve utilizar-se do *habeas data* que, diferentemente do *habeas corpus*, exige um advogado para sua interposição – um tratamento bastante inadequado para um interesse cuja atuação necessita de instrumentos promocionais[85].

Já o Código de Defesa do Consumidor, trouxe previsões tão modernas que foram utilizadas como inspiração para além das relações de consumo[86]. Tendo como a sua maior preocupação a utilização abusiva das informações sobre os consumidores em banco de dados, o CDC buscou estabelecer um equilíbrio na relação de consumo através da interposição de limites ao uso destas informações pelos fornecedores. Em seu artigo 43, elenca uma série de direitos e garantias para o consumidor em relação às suas informações pessoais que estão sob o controle do fornecedor em bancos de dados, possibilitando-os o direito de acesso, correção e até mesmo, em casos específicos, a comunicação escrita ao consumidor sobre o tratamento da informação pessoal. No que pese o grande avanço no campo de proteção de dados pessoais trazido pelas disposições do Código de Defesa do Consumidor, o seu campo de incidência é limitado pelas situações que se caracterizam como relação de consumo, ainda que se tenha na doutrina propostas de uma interpretação de caráter expansivo[87]. Trata-se, então, de uma tutela de certa forma limitada, impossibilitado que o CDC assuma a proporção de um sistema geral de proteção de dados pessoais.

---

[84] GAMBOGI CARVALHO, Ana Paula. O consumidor e o direito à autodeterminação informacional. **Revista de Direito do Consumidor,** n. 46, 2003, p. 77-119.
[85] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 275.
[86] TEPEDINO, Gustavo. **Temas de Direito Civil.** Rio de Janeiro: Editora Renovar, 1999, pp. 199-216.
[87] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 275.

Diante da ausência de uma regulamentação da internet no Brasil e uma tendência desta regulamentação por meio de leis penais, que não foi bem recepcionada pela sociedade civil, surgiu em 2014 a Lei 12.965, também conhecida como Marco Civil da Internet. Visando o afastamento da ideia de uma regulamentação da internet fundada em princípios penais, o MCI procurou regulamentar os direitos e garantias do cidadão nas relações travadas no âmbito da internet, distanciando tal regime tanto das técnicas de prescrição, quanto das técnicas restritivas de liberdade[88]. Conforme explica Bruno Ricardo Bioni, a utilização destas técnicas, por serem próprias do âmbito criminal, poderiam surtir efeitos inibitórios para as mudanças esperadas tendo em vista a dinamicidade da internet[89].

Dentre os direitos previstos pelo MCI, merecem destaque os direitos à proteção da privacidade e dos dados pessoais. Acontece que, diante do instituto da liberdade de expressão e da neutralidade da rede, a eficácia dos princípios do MCI é prejudicada. Comprovando a existência de uma barreira no cumprimento do direito à privacidade e à proteção de dados e a consequente necessidade de um texto normativo mais "duro", em junho do ano anterior à aprovação do MCI, surgiu o escândalo de espionagem da Agência Nacional de Segurança dos Estados Unidos, revelado pelo ex-analista Edward Snowden[90]. Este episódio causou impacto direto na normatização da internet no Brasil, acelerando o trâmite legislativo do MCI[91] através da adoção do regimento de urgência[92].

Mesmo com as diversas inovações trazidas pelo MCI no campo das relações jurídicas estabelecidas na internet[93], estes direitos e garantias não são capazes de fornecer ao titular de

---

[88] BRITO CRUZ, Francisco. **Direito, democracia e cultura digital:** a experiência de elaboração legislativa do marco civil da internet. Dissertação (Mestrado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, São Paulo, 2009, p. 29-53.

[89] BIONI, Bruno Ricardo. Projeto de Lei 215/2015, infanticídio aos recém-nascidos direitos digitais no Brasil. ***Digital Rights***, n. 28, out. 2015. Disponível em: https://www.digitalrightslac.net/pt/proyecto-de-ley-2152015-infanticidio-contra-los-recien-nacidos-derechos-digitales-en-brasil/. Acesso em: 17 mar. 2020.

[90] G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA.** Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 19 abr. 2020.

[91] TAVERES, Monica. Após espionagem, Dilma pede urgência de votação do Marco Civil da Internet. **Jornal O Globo.** 11 set. 2013. Disponível em: http://oglobo.globo.com/sociedade/tecnologia/apos-espionagem-dilma-pede-urgencia-de-votação-do-marco-civil-da-internet-9912712. Acesso em: 19 abr. 2020.

[92] O regimento de urgência estabelece que a votação de projeto de lei deva ser realizada no período de 45 dias. Caso contrário, haverá o trancamento da pauta de votações.

[93] "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de

dados pessoais uma efetiva proteção tendo em vista a velocidade e capacidade de armazenamento e compartilhamento de dados pessoais na rede de computadores. Retratando a referida ineficácia normativa do MCI, há como exemplo o não acolhimento da Apelação Cível nº70079524351/RS, proposta com o objetivo de indenização do *Facebook* pelo compartilhamento das informações que constavam no banco de dados da rede social com um aplicativo externo, o Lulu.

O Lulu coletava as informações públicas dos usuários que baixavam o aplicativo para a formação de um perfil *online*, atribuindo notas de 1 a 10 para a sua aparência física. O Tribunal de Justiça do Rio Grande do Sul entendeu que as informações compartilhadas para o Lulu eram informações públicas, não havendo que se falar em vazamento de dados pessoais[94]. Portanto, o TJRS desconsiderou que os dados pessoais disponibilizados no *Facebook* foram utilizados com fim diverso do original e sem o consentimento dos usuários, institutos reiterados e aprimorados na LGPD. O cenário relatado acima envolvendo o Facebook no Brasil, assim como o escândalo internacional de vazamento de dados dessa mesma rede social para a empresa britânica *Cambridge Analytica* em 2018[95], fez com que diversos países percebessem o caráter de urgência da instauração de leis de proteção de dados pessoais[96].

2.2.3.1 O processo de formulação da LGPD e a possível postergação em virtude do COVID-19

Logo após a publicação em maio de 2018 do Regulamento Geral de Proteção de Dados da União Europeia, o Senado Federal, após uma década de debates, aprovou no dia 10 de julho de 2018 o PLC 53/18. A sanção da Lei 13.709/2018 se deu em menos de um mês

---

gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: (BRASIL. **Lei nº 12.965,** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2020.)

[94] BRASIL. Tribunal de Justiça do Rio Grande do Sul. Apelação cível nº 70079524351. Relator: Gelson Rolim Stocker. 17ª Câmara Cível. Data de julgamento: 28 mar. 2019. Data de publicação: 02 abr. 2019.

[95] MEREDITH, Sam. *Here's everything you need to know about the Cambridge Analytica scandal.* **CNBC.** 2018. CNBC. Disponível em: https://www.cnbc.com/2018/03/20/ftc-reportedly-to-investigate-facebooks-useof-personal-data.html. Acesso em: 06 nov. 2019.

[96] SOMADOSSI, Henrique. O que muda com a Lei Geral de Proteção de Dados (LGPD). **Migalhas.** 24 ago. 2018. Disponível em: https://www.migalhas.com.br/depeso/286235/o-que-muda-com-a-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 01 jun. 2020.

após a referida aprovação, em 14 de agosto de 2018, consolidando-se na LGPD. Nas palavras de Laura Schertel Mendes[97], a contemplação do tema de proteção de dados em diversos outros diplomas legais caracteriza uma verdadeira "colcha de retalhos normativa". Atuando como resposta aos anseios decorrentes das diversas situações que podem se desenrolar com o tratamento irregular de dados pessoais, a LGPD assegurará o direito da pessoa humana de controlar as suas próprias informações e, consequentemente, proteger o princípio da dignidade da pessoa humana, assim como garantirá uma maior segurança nas relações travadas na internet, impedindo condutas danosas por parte de entidades privadas e do governo.

O processo de formulação da LGPD se iniciou em 2010, compreendendo duas fases de debates (2010 e 2015) referentes ao Anteprojeto de Lei de Proteção de Dados, elaborado sob a coordenação do Ministério da Justiça e da Cidadania. O início formal, no entanto, apenas se deu após o envio do Anteprojeto para a Câmara dos Deputados, consolidando-se no dia 13 de maio de 2016 através do Projeto de Lei 5.276[98]. Cumpre mencionar que, mesmo após diversos debates públicos realizados pelo Ministério da Justiça e da Cidadania acerca da pertinência da criação de uma autoridade para supervisionar a aplicação da lei, o texto enviado pelo Poder Executivo ao parlamento não se referia à criação da referida autoridade. No entanto, a inclusão da Autoridade Nacional de Proteção de Dados (ANPD) se deu em 2018, através da sua inclusão no relatório apresentado pela Comissão Especial da Câmara dos Deputados criada para analisar o PL 5276, sendo aprovado pelos plenários da Câmara dos Deputados e do Senado Federal e consolidando-se no PLC 53/18[99].

Em 14 de agosto de 2018 a LGPD foi sancionada, no entanto, a estrutura da ANPD (autarquia federal em regime especial) foi vetada pela Presidência da República. Neste sentido, reconhecendo a necessidade de uma autoridade nacional para garantir a efetividade da LGPD, em 27 de dezembro de 2018 o Poder Executivo publicou a Medida Provisória n. 869/2018[100].

---

[97] MENDES, Laura Schertel. **A Lei Geral de Proteção de Dados Pessoais:** um modelo de aplicação em três níveis. São Paulo: Editora Revista dos Tribunais, 2019, p. 44.
Caderno Especial LGPD. p.44. São Paulo: Ed. RT, novembro 2019.

[98] BRASIL. **Projeto de Lei nº 5276,** de 13 de maio de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília, DF. 13 maio. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 20 jun. 2020.

[99] BRASIL. **Projeto de Lei nº 53,** de 01 de junho de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF. 01 jun. 2018. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 20 jun. 2020.

[100] BRASIL. **Medida Provisória nº 869,** de 28 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2008, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e

A estrutura proposta desta vez pelo Poder Executivo enquadrava a ANPD como um órgão público e localizado dentro da estrutura da Presidência da República. Sendo assim, após muitas "idas e vindas", com diversas modificações feitas pela Comissão Mista ao avaliar a MP no Congresso Nacional, no dia 8 de julho de 2019, ela foi convertida na Lei n. 13.853.

No entanto, mesmo após a sanção da LGPD, nada é tão fácil quanto parece e a sua entrada em vigor, diante da forte tendência de postergação, é um dos grandes motivos de preocupação para os estudiosos na área da proteção de dados. Desde a sua promulgação em 2018, a LGPD já foi adiada uma vez pela Medida Provisória n. 869/2018 para agosto de 2020, ao ponto em que estava inicialmente prevista para fevereiro de 2020. A nova proposta de adiamento da entrada em vigor da LGPD se deu em 2019 (PL nº 5.762/2019) [101], mas, apenas com a recente pandemia do COVID-19 ganhou força. O Projeto de Lei da Câmara visa à prorrogação da entrada em vigor da LGPD para 15 de agosto de 2022, enquanto o Projeto de Lei do Senado (PL nº 1.027/2020[102]) se refere ao dia 16 de fevereiro de 2022.

Neste ponto, existem argumentos tanto em prol do adiamento, quanto aqueles que defendem a manutenção da entrada em vigor da LGPD. Dentre os argumentos utilizados para a postergação da LGPD, destacam-se as dificuldades econômicas que estão sendo enfrentadas pelas empresas em virtude do COVID-19, impossibilitando-as de se adequarem a Lei em tempo tão curto como também, o fato da ANPD ainda não ter sido criado e a consequente não publicação de diretrizes interpretativas a respeito das lacunas jurídicas presentes na LGPD. Para a parte da doutrina que defende a manutenção, indicam que, a postergação irá acarretar em impactos negativos no cenário internacional não só em relação ao comércio, como também no fator de cooperação entre os países, principalmente em relação ao compartilhamento de informações relevantes para o combate à pandemia[103]. No cenário interno, cumpre destacar o posicionamento do antigo ministro da saúde, Nelson Teich, que antes da sua nomeação afirmou, em artigo publicado em suas redes sociais, estar o sucesso do

---

dá outras providências. Brasília, DF. 28 dez. 2018. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 20 jun. 2020.

[101] BRASIL. **Projeto de Lei nº 5762, de** 30 de dezembro de 2019. Altera a Lei nº 13.709, de 2018, prorrogando a data de entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 15 de agosto de 2022. Brasília, DF. 30 dez. 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704. Acesso em: 20 jun. 2020.

[102] BRASIL. **Projeto de Lei nº 1027,** de 26 de março de 2020. Altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 16 de fevereiro de 2022. Brasília, DF. 26 mar. 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141225. Acesso em: 20 jun. 2020.

[103] JUNQUEIRA, Thiago; CHALFIN, Ricardo. Covid-19 e a postergação da LGPD: histeria ou sabedoria? **Revista Consultor Jurídico.** 21 abr. 2020. Disponível em: https://www.conjur.com.br/2020-abr-21/opiniao-covid-19-postergacao-lgpd-histeria-ou-sabedoria#sdfootnote4sym. Acesso em: 27 jun. 2020.

combate ao COVID-19 atrelado à "capacidade de colher dados críticos em tempo real, de incorporar e analisar essa base de dados atualizada, de ajustar as projeções quanto aos possíveis impactos das escolhas, rever as decisões e desenhar novas medidas e ações[104]".

2.2.3.2 A proteção de dados pessoais como um direito fundamental

De início, cumpre lembrar que, a CF/88 considera invioláveis a vida privada e a intimidade[105] e, portanto, estabelece a garantia de inviolabilidade referente às interceptações de comunicações eletrônicas, telegráficos ou dados[106]. Ainda, proíbe a invasão de domicílio[107] e a violação de correspondência[108]. Além das normas previstas na Constituição, existem diversas previsões sobre privacidade na legislação ordinária, sejam elas de natureza penal, processual, comercial, tributária ou no âmbito do direito civil. O Código Civil de 1916, por exemplo, já previa certas limitações ao direito de construir, levando em conta o direito de vizinhança e a privacidade[109]. Na seara tributária, o Código Tributário Nacional determina a

---

[104] TEICH, Nelson. ***COVID-19*: histeria ou sabedoria?** Disponível em: https://www.linkedin.com/pulse/covid-19-histeria-ou-sabedoria-nelson-teich/. Acesso em: 27 jun. 2020.

[105] Art. 5º [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jun. 2020.)

[106] 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; (BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jun. 2020)

[107] Art. 5º [...] XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; (BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jun. 2020)

[108] 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; (BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jun. 2020.

[109] "Art. 573. O proprietário pode embargar a construção de prédio que invada a área do seu, ou sobre este deite goteiras, bem como a daquele, em que, a menos de metro e meio do seu, se abra janela, ou se faça eirado, terraço ou varanda. [...] Art. 576. O proprietário, que anuir em janela, sacada, terraço, ou goteira sobre o seu prédio, se até o lapso de ano e dia após a conclusão da obra poderá exigir que se desfaça. Art. 577. Em prédio rústico, não se poderão, sem licença do vizinho, fazer novas construções, ou acréscimos as existentes, a menos de metro e meio de limite comum. (BRASIL. **Lei nº 3.071,** de 1º de janeiro de 1916. Código Civil dos Estados Unidos do Brasil. Rio de Janeiro, RJ. 01 jan. 1916. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L3071.htm. Acesso em: 10 abr. 2020.)

obrigação de sigilo para os agentes de fisco[110]. Já o Código de Processo Civil faz referência à proteção à privacidade ao estabelecer as ocasiões nas quais o processo deva correr sob o segredo de justiça [111].

No que pese a Declaração de Santa Cruz de La Sierra, documento firmado pelo governo brasileiro em 15 de novembro de 2003, se referir ao caráter de direito fundamental da proteção de dados pessoais em seu item 45, o reconhecimento da proteção de dados como um direito fundamental não é extraído de forma literal na CF/88. Diferentemente, conforme entendimento majoritário da doutrina, a autonomia e característica do direito fundamental da proteção de dados deriva do impacto negativo que o tratamento automatizado traz à proteção de um conjunto de direitos da personalidade, composto pela igualdade substancial, liberdade, dignidade da pessoa humana, assim como a proteção do direito à privacidade[112]. Neste sentido, o entendimento de um direito fundamental à proteção de dados é resultado da ideia de tratamento autônomo de proteção de dados pessoais[113], sendo esta uma tendência cada vez maior em diversos ordenamentos jurídicos[114].

Percebe-se que, essas disposições esparsas preveem a tutela de algum aspecto da proteção ao direto fundamental à privacidade. Até maio deste ano, o entendimento predominante na seara do STF, constantemente mencionado como precedente em diversos julgados, se pautava na

---

[110] "Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades." (BRASIL. **Lei nº 5.172,** de 25 de outubro de 1966. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília, DF. 25 out. 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em: 10 abr. 2020.)

[111] "Art. 189. Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos: I – em que o exija o interesse público ou social; II – que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes; III – em que constem dados protegidos por direito constitucional à intimidade; IV – que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo." (BRASIL. **Lei nº 13.105,** de 16 de março de 2015. Código de Processo Civil. Brasília, DF. 16 mar. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 maio. 2020.)

[112] DONEDA, Danilo. **A autonomia do direito fundamental de proteção de dados.** São Paulo: Editora Revista dos Tribunais, 2019, p. 27.

[113] "Para além da coincidência do léxico com os modernos instrumentos internacionais de tutela da privacidade, certo é que a proteção da dignidade humana e a inviolabilidade da intimidade e da vida privada numa sociedade da informação somente pode ser atingida hoje por meio da proteção contra os riscos do processamento de dados pessoais. Assim, quando se interpreta a norma do art. 5º, X, em conjunto com a garantia do habeas data e com o princípio fundamental da dignidade humana, é possível extrair-se da Constituição Federal um verdadeiro direito fundamental à proteção de dados pessoais. Entendemos que o reconhecimento desse direito fundamental não é apenas uma possibilidade; trata-se de uma necessidade para tornar efetivos os fundamentos e princípios do Estado democrático de direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal". (MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça,** 2018, p. 188)

[114] MAÑAS, José Luis Piñar. *El derecho fundamental a la protección de datos personales (LOPD). In:* MAÑAS, José Luis Piñar (Org.). ***Protección de datos de carácter personal en Iberoamérica.*** Valencia: Tirant Lo Blanch, 2005, pp. 19-36.

decisão de 2006 relatada pelo Ministro Sepúlveda Pertence, o qual se refere à inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com base nas garantias constitucionais, estando a natureza fundamental da proteção de dados restrita ao momento da sua comunicação. Ou seja, somente sob o momento da sua comunicação ou eventual interceptação, do grampo ou da escuta e essas situações representam apenas uma parcela dos problemas que decorrem da utilização das novas tecnologias no tratamento de dados. Diferentemente, ao prever a inviolabilidade de dados, a Constituição estaria se referindo à tutela do sigilo das comunicações e não do dado em si, sendo este o mesmo entendimento da tese de Tércio Sampaio Ferraz Junior[115].

Suprindo a necessidade de uma tutela efetiva aos dados pessoais na amplitude que o tema merece na atualidade, nos dias 06 e 07 de maio de 2020, foi proferida decisão histórica relatada pela Ministra Rosa Weber que reconheceu o direito a proteção de dados pessoais como um direito fundamental autônomo[116]. Sob o ponto de vista de Laura Schertel[117], a relevância de tal decisão para o campo de proteção de dados no Brasil, diante do fato de ter tornado expresso o caráter fundamental da proteção de dados pessoais, pode ser comparada ao julgamento da Corte constitucional alemã de 1983, emblemática decisão que estabeleceu o conceito de autodeterminação no país[118]. Suspendendo a aplicação da MP 954/2018, o julgamento do plenário, por meio de confirmação de Medida Cautelar nas Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6393, 6390, determinou não estarem mais as operadoras de telefonia obrigadas a repassarem ao IBGE dados em relação ao telefone móvel, celular e endereço dos seus consumidores. Neste ponto, percebe-se que a preocupação da Corte ao decidir neste sentido por maioria de 10 votos é fundamentada nos efeitos negativos

---

[115] "A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitimamente de dados incriminadores relativos a uma pessoa, ficaria impedido de cumprir o seu dever de denunciá-lo!". (FERRAZ JR, Tércio S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, vol. 88, 1993, p. 447)

[116] BRASIL. Supremo Tribunal Federal. Referendo na medida cautelar na Ação Direta de Inconstitucionalidade nº 6.389/DF. Requerente: Partido Socialista Brasileiro. Intimado: Presidente da República. Relatora: Ministra Rosa Weber. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em: 18 jul. 2020.

[117] MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais: novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. **Portal JOTA.** 10 maio. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020#_ftnref8. Acesso em: 18 jul. 2020.

[118] Os aspectos da decisão serão analisados no Capítulo 4.1.

relacionados à limitação das liberdades conquistadas diante da possibilidade de extensão da vigilância para além do momento/contexto autorizado.

Para um melhor entendimento acerca do impacto de tal decisão no ordenamento jurídico brasileiro, cumpre analisar os seus três pontos centrais. Do próprio voto da relatora, extrai-se um aspecto extremamente importante: o reconhecimento de que não há dados insignificantes para o processo de tratamento de dados, pois todo tipo de dado pode ser utilizado para a formação de perfis identificadores dos cidadãos. Os riscos da MP 954, dentre eles a coleta excessiva de dados e ausência de medidas de segurança, mencionados expressamente no voto da Ministra Relatora, se agravam ainda mais diante do fato do Brasil não ter uma lei de proteção de dados pessoais em vigor. Em relação à própria configuração de um direito fundamental à proteção de dados pessoais, a referida decisão clarifica os seus efeitos, relacionando-o como um direito subjetivo, de defesa do indivíduo e como um direito em sua dimensão objetiva, qual seja, o dever de proteção estatal nas relações privadas. Nos termos do 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 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[119].

Há ainda de se ressaltar que, em 2019, com o objetivo da alteração dos artigos 5º, XV e 22, XXX da Constituição Federal, e a consequente inclusão da proteção de dados pessoais entre os direitos fundamentais, assim como a fixação de competência privativa da União para legislar a respeito desta tutela, foi Proposta a Emenda à Constituição nº 17[120], que possui o seguinte teor:

> 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

[119] BRASIL. Supremo Tribunal Federal. Referendo na medida cautelar na Ação Direta de Inconstitucionalidade nº 6.389/DF. Requerente: Partido Socialista Brasileiro. Intimado: Presidente da República. Relatora: Ministra Rosa Weber. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em: 18 jul. 2020.

[120] BRASIL. **Proposta de Emenda à Constituição nº 17,** de 03 de julho de 2019. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF. 03 jul. 2019. Disponível em:https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 18 jul. 2020.

> termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais; Art. 22. XXX – proteção e tratamento de dados pessoais.

Portanto, caso a PEC 17/2019 seja aprovada e, portanto, incorporada ao texto constitucional, o direito à proteção de dados será equiparado ao direito à privacidade, informação e transparência, sendo estes direitos fundamentais que possuem relação direta sobre dados pessoais. Caso não haja a inclusão de um direito à proteção de dados de forma explícita no rol de direitos fundamentais, sob a perspectiva de Danilo Doneda, deve haver, mais do que nunca, um forte posicionamento da doutrina e jurisprudência em prol da uma interpretação mais adequada dos incisos X e XII do art. 5º da CF/88[121]. Neste sentido, apesar da decisão mencionada acima caracterizar-se como um grande avanço jurisprudencial na esfera de proteção de dados pessoais no ordenamento jurídico brasileiro, por ter reconhecido expressamente a proteção de dados pessoais como um direito fundamental, há de ser observada a necessidade de definição de critérios para definir a aplicação, os limites do próprio direito, bem como os da sua violação[122].

2.3 FUNDAMENTOS E PRINCÍPIOS DA LGPD

Sob a perspectiva de que não existem dados irrelevantes, ante a projeção direta dos dados pessoais na personalidade do titular e da possibilidade de processamentos constantes e automatizados na sociedade da informação, a LGPD criará um regramento que se aplicará tanto a todos os setores econômicos, quanto ao setor público, estabelecendo princípios e limites ao uso, coleta, tratamento e compartilhamento de dados pessoais. Com isso, consequentemente alterará em partes o Marco Civil da Internet[123]. Neste sentido, as empresas devem adequar todos os seus setores às novas regras estabelecidas pela LGPD, adotando

---

[121] DONEDA, Danilo. **A autonomia do direito fundamental de proteção de dados.** São Paulo: Editora Revista dos Tribunais, 2019, p. 32.

[122] MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais: novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. **Portal JOTA**. 10 maio. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020#_ftnref8. Acesso em: 18 jul. 2020.

[123] "Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações: [...] X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; [...] II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

práticas de *compliance*[124]. Além do mais, a sua promulgação coloca o Brasil no cenário da economia digital mundial, possibilitando, por exemplo, a transferência internacional de dados entre países da União Europeia[125].

Logo em seu art. 1º, a LGPD, ao definir como objetivo a proteção dos direitos fundamentais de privacidade, de liberdade e o livre desenvolvimento da personalidade natural, demonstra que o legislador se preocupou com a necessidade do uso seguro e ético dos dados pessoais. Principalmente, diante de um sistema de exploração de dados criado com o intuito de maximização de lucros[126], pode-se dizer que a LGPD, logo de início, demonstra que tem como objetivo principal proporcionar aos titulares dos dados os seus direitos básicos ligados à autodeterminação informativa e consequentemente, resgatar a dignidade dos titulares.

Logo em seguida, em seu art.2º, a LGPD disciplina os fundamentos para a proteção de dados pessoais nos seguintes termos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;
>
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Os fundamentos, conforme explica Celso Ribeiros Bastos, "são inerentes ao Estado, fazem parte de sua estrutura[127]". Percebe-se que, o art. 2º deixa claro quais são os objetivos da Lei, indo eles além da privacidade e dos direitos consumeristas. Visando garantir uma ampla proteção ao titular dos dados, são mencionados expressamente os direitos humanos, o livre desenvolvimento da personalidade, a autodeterminação iformativa, dentre outros. No que pese a autodeterminação informativa aparentar-se como um instituto bastante utópico, se apresenta na LGPD como uma das formas de devolver ao titular o poder sobre o uso e

---

[124] VITAL, Alan. **Práticas de Compliance e a LGPD.** 2019. Disponível em: https://vitaladvocacia.com.br/praticas-de-compliance-e-a-lgpd/. Acesso em: 28 jun. 2020.

[125] Neste ponto, cumpre lembrar que o GDPR em sua Consideranda 6, restringe aos países do bloco europeu a transferência internacional de dados para países que possuam um elevado nível de proteção de dados.

[126] PASQUALE, Frank. ***The black box society:*** *the secret algorithm's that control money and information.* Cambridge: Harvard University Press, 2015, p. 146.

[127] BASTOS, Celso Ribeiro. **Curso de Direito Constitucional.** 15 ed. São Paulo: Editora Saraiva, 2020.

fluxo dos seus próprios dados. Nas palavras de Stefano Rodotà, a autodeterminação se caracteriza como um "poder permanente de controle sobre os seus próprios dados[128]".

Posteriormente, em seu art. 6º, a LGPD estabelece 10 princípios para o tratamento de dados no Brasil, mencionando logo de início em seu *caput* a necessidade de observância da boa-fé nas atividades de tratamento de dados pessoais e deixando claro que os dados pessoais não são meros bens de cunho patrimonial[129]:

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

Ao comentar sobre o entendimento de Ronald Dworkin acerca das características que diferenciam os princípios das regras e políticas, Newton de Lucca chega à conclusão de que os princípios gerais são, sem sombra de dúvidas, normas como todas as outras, caracterizando-se como as normas fundamentais, as mais gerais do sistema[130]. Cumpre ressaltar que, os princípios devem ser cumpridos em qualquer hipótese de tratamento, independentemente de estarem de acordo com as bases legais de tratamento de dados

---

[128] RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Editora Renovar, 2008.

[129] FRAZÃO, Ana. Lei Geral de Proteção de Dados Pessoais: direitos básicos dos titulares de dados pessoais. **Revista do Advogado nº 144,** AASP, 2019, p. 35.

[130] LUCCA, Newton de. Marco Civil da Internet: uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. *In:* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.) **Direito & Internet III:** Marco Civil da Internet. São Paulo: Editora Quartier Latin, 2015, p. 39.

pessoais[131]. Ao impor diversos cuidados e restrições ao tratamento de dados, a principiologia da LGPD demonstra uma prioridade dada à dimensão existencial, impedindo que os dados pessoais sejam limitados ao aspecto puramente patrimonial. O fato de nem mesmo o consentimento do titular dos dados ser capaz de afastar o cumprimento dos princípios demonstra claramente isso.

Os três primeiros princípios (finalidade, adequação e necessidade) se conectam entre si e forma, em conjunto com o princípio da transparência, a ideia central da LGPD, qual seja: a proteção dos direitos fundamentais da privacidade, liberdade e livre desenvolvimento da personalidade da pessoa natural através da tutela dos dados pessoais. Para Adalberto Simão Filho, o primeiro princípio do art. 6º é, provavelmente, o mais relevante na pratica, pois os traços característicos da proteção de dados pessoais estão fortemente presentes nele[132]. Pode-se dizer que, o princípio da finalidade estabelece os limites da legalidade no tratamento de dados, pois delimita a realização do tratamento lícito ao motivo que fundamentou essa coleta.

O princípio da adequação está diretamente relacionado ao princípio da finalidade, uma vez que, a legalidade do tratamento de dados está sujeita à compatibilidade com os propósitos iniciais que foram informados ao titular. Guardando relação direta com os dois princípios já mencionados, o princípio da necessidade limita a licitude do tratamento ao mínimo necessário para o alcance das finalidades. A ideia da *Data Minimization* prevê a avaliação de quais dados são de fato necessários, visando à utilização não excessiva de informações de cunho pessoal. Também, estabelece a necessidade de análise anterior ao tratamento da proporcionalidade entre a operação e os riscos para os direitos dos titulares que podem advir dela[133]. Essa ideia é ainda mais rígida no GDPR, que além de mencionar expressamente o conceito de *privacy by default*[134], prevê o princípio da minimização[135], ideia já mencionada expressamente como

---

131 "Portanto, além de o controlador avaliar o atendimento de ao menos uma das bases legais para o tratamento de dados pessoais, como obrigação legal, consentimento exercício regular de direito ou para execução de contratos, por exemplo, também deverá se atentar ao cumprimento de todos os princípios (...)" (VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 138)

132 DONEDA, Danilo. Princípios de proteção de dados pessoais. *In:* LUCCA, Newton de; SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e Internet III:** Marco civil de internet. São Paulo: Editora Quartier Latin, 2015, p. 378.

133 VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 144.

134 "O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares."

135 Art. 5º (1) c do GDPR: os dados pessoais são adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados ("minimização dos dados"). (UNIÃO EUROPEIA.

fundamento em um caso julgado pelo STJ[136]. Neste caso, o princípio da minimização foi utilizado como fundamento em decisão que declarou abusiva uma cláusula prevista em um contrato de prestação de serviço entre determinado banco e seus clientes. A cláusula autorizava o banco contratante a compartilhar os dados de seus consumidores com outras entidades financeiras sem que fosse dada a oportunidade ao titular dos dados de discordar do referido compartilhamento.

Visando um controle efetivo do uso de dados pessoais, o principio do livre acesso garante ao titular a possibilidade de consultar facilmente e gratuitamente informações sobre a forma, duração do tratamento e integralidade de seus dados pessoais. Reforçando o referido princípio, o art. 9º da LGPD estabelece como direito do titular a disponibilização das informações sobre o tratamento de seus dados de forma clara, adequada e ostensiva, entre outras, como: a identificação e as informações de contato do controlador; finalidade específica do tratamento; responsabilidades dos agentes que realizarão o tratamento e dos direitos do titular expressos no art. 18 da lei que serão abordados mais a frente.

Diante dos impactos negativos que podem derivar de qualquer imprecisão[137], como um dado desatualizado ou equivocado, o princípio da qualidade dos dados estabelece medidas que devem ser adotadas pelos controladores como forma de garantir a precisão dos dados e até mesmo a sua atualização, quando necessário. Fortalecendo o objetivo da LGPD de garantia a um tratamento de dados ético, o princípio da transparência prevê a obrigação de fornecimento de informações claras e de fácil acesso não só sobre o tratamento, assim como dos seus respectivos agentes de tratamento.

Por ser a violação de dados pessoais uma das situações mais críticas no processo de tratamento, a LGPD decidiu incluir a obrigatoriedade de utilização de medidas técnicas e administrativas por parte dos agentes de tratamento aptas a proteger os dados pessoais de

---

Regulamento Geral de Proteção de Dados. Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[136] "Destaque-se que o art. 5º daquele documento (GDPR) consagra, entre os princípios fundamentais relativos aos dados pessoais, que a recolha dos dados somente poderá existir com fins específicos, além de estabelecer a minimização dos dados (apenas aquilo que for estritamente necessário), sempre para um fim concreto, além de estabelecer que referido processo seja transparente, leal e lícito" (BRASIL. Superior Tribunal de Justiça Recurso Especial nº 1348532-SP 2012/0210805-4. Relator: Ministro Luis Felipe Salomão. Quarta Turma. Data de julgamento: 30 nov. 2017. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2017/2017-11-09_08-03_E-abusiva-clausula-que-obriga-cliente-de-cartao-de-credito-a-fornecer-dados-a-terceiros.aspx)

[137] "Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação da participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta". (VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 149)

violações, sejam elas propositais ou não. O princípio da segurança prevê, inclusive, que a ausência da segurança esperada pelo titular, dentro das circunstâncias cabíveis[138], classifica o tratamento como um tratamento irregular. Cumpre observar que, a segurança adotada pelos diversos agentes de tratamento não é a mesma, pois essa garantia deve ser proporcional ao risco do tratamento. Levando em consideração a natureza das informações tratadas em conjunto com o atual estado da tecnologia, a ANPD poderá estabelecer os padrões técnicos mínimos de tratamento[139], sendo estes já estabelecidos pelo MCI[140].

O princípio da prevenção está diretamente ligado à ideia da LGPD de mitigar os danos antes mesmo do tratamento. O que se espera deste princípio é a proteção da privacidade com base na trilogia que advém do conceito de *Privacy by Design* (PbD) de Ann Cavoukian, composta por: sistemas de tecnologia informação (*IT systems*); práticas negociais responsáveis (*accountable business practices*) e design físico e infraestrutura de rede (*physical and networked infrastructure*)[141]. O papel, tanto dos próprios agentes de tratamento, que são legitimados pela LGPD a formularem regras de boa prática e governança relacionadas a diversos aspectos do tratamento de dados pessoais[142], quanto da ANPD através do seu papel

---

[138] 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: 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.(BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[139] 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[140] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. [...] § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. (BRASIL. **Lei nº 12.965,** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2020)

[141] CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles. Disponível em: https://iab.org./wp-content/IAB-uploads/2011/03/fred_carter.pdf. Acesso em: 07, jun.,.2020.

[142] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL. **Lei nº 13.709,** de 14 de agosto de

fiscalizatório do cumprimento destas regras[143], são peças fundamentais parra o princípio da prevenção.

O princípio da não discriminação se preocupa com o tratamento para fins discriminatórios, proibindo-os, sejam eles automatizados ou não. Assim, conforme recomenda a Consideranda 71 do GPDR, o controlador deve aplicar as medidas técnicas adequadas, dentro das especificidades e contexto em que os dados são tratados, garantindo que os riscos discriminatórios serão descartados. Neste mesmo sentido, pelas práticas de *geopricing* e *geoblocking* para fins discriminatórios, com base na etnia e localização geográfica dos consumidores, o Ministério da Justiça sancionou o comércio eletrônico Decolar em R$ 7.500.000,00, por entender que tais práticas, por causarem um verdadeiro desequilíbrio nas relações de consumo, são abusivas[144]. Ainda, cumpre mencionar que, a vedação trazida pelo princípio da não descriminação não abarca as situações em que há a descriminação não intencional[145], como exemplo é o exemplo da coleta de informações por parte de companhias aéreas referentes às restrições alimentares dos seus clientes, por motivos de saúde ou religião, para que eles sejam servidos com a alimentação adequada.

O último princípio prevê a responsabilização e a necessidade de prestação de contas por parte dos agentes de tratamento. Em todo o ciclo de vida de tratamento de dados, o controlador e o operador responsável devem não só analisar a conformidade legal, como também, ponderar os riscos para a implementação do procedimento de proteção de dados adequado ao caso concreto. Primeiramente, deve o agente verificar se está agindo em conformidade com os

---

2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[143] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. [...] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados 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, poderá: [...] II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[144] BRASIL. Ministério da Justiça. **Decolar.com é multada por prática de *geopricing* e *geoblocking*:** decisão inédita do Departamento de Proteção e Defesa do Consumidor (DPDC) obriga empresa a pagar R$ 7,5 milhões. 18 jun. 2018. Disponível em: http://www. Justiça.gov.br/News/collective-nitf-content-51. Acesso em: 06 jun. 2020.

[145] VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 166.

princípios da LGPD, para em sequência analisar a natureza do dado pessoal (sensível ou não) e verificar se há ao menos uma das bases legais para tratamento previstas na lei. Por fim, além de todas as medidas de segurança que devem ser adotadas, os agentes de tratamento devem garantir que os direitos do titular sejam viabilizados, estando sujeitos às consequências administrativas e civis determinadas em Lei em caso de violação das referidas obrigações[146].

[146] "Este modo de aplicação da LGPD é nomeado por Laura Schertel Mendes como modelo de aplicação em três níveis: "Para a aplicação da LGPD, formulamos um modelo em três níveis: primeiro lugar, é preciso analisar quais são as condições de legitimidade para se realizar o tratamento de dados pessoais; em seguida, são estabelecidos os procedimentos para a garantia desse direito; e, por fim, se determinam quais as consequências administrativas e civis decorrentes da violação das fases anteriores". (MENDES, Laura Schertel. **A Lei Geral de Proteção de Dados Pessoais:** um modelo de aplicação em três níveis. São Paulo: Editora Revista dos Tribunais, 2019, p. 47)

3 DO TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais é conceituado pela LGPD de forma extremamente abrangente como "toda operação realizada com dados pessoais". Ou seja, engloba praticamente todos os tipos de operações que podem ser feitas com dados pessoais, se referindo a diversos exemplos em seu art. 5º, X, como: coleta, retenção, processamento, compartilhamento, e até mesmo o processo de eliminação[147]. Neste sentido, a regulamentação se inicia com a coleta do dado e se encerra com a eliminação ou descarte, nos termos dos artigos 15[148] e 16[149] da Lei. Ainda, de forma inicial a legislação já prevê que se aplica tanto ao tratamento de dados no meio digital, quanto em estado físico ou *off-line*, mesmo que estes não migrem para o meio digital ou *on-line*[150] ao mencionar no *caput* do art. 3º o termo "independente do meio" ao se referir ao tipo de operação de tratamento tutelado pela Lei[151].

---

[147] A fase da coleta se refere a obtenção, recepção ou produção de dados pessoais. A fase da retenção é caracterizada pelo arquivamento ou armazenamento de dados pessoais. O processamento de dados é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais. Todos eles independem do meio utilizado. O compartilhamento de dados é quando há transmissão, distribuição, comunicação, transferência, difusão e uso compartilhamento de dados pessoais. A fase de eliminação se caracteriza como qualquer operação visa apagar ou eliminar dados pessoais, assim como o descarte dos ativos organizacionais nos casos necessários ao negócio da instituição. (BRASIL. **Guia de boas práticas da Lei Geral de Proteção de Dados.** Brasília, DF. 2020. P. 41. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 10 jun. 2020.)

[148] Art. 15: O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II - fim do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[149] Art. 16: Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[150] "O caput do art. 3º da LGPD dispõe sobre a sua aplicação material, deixando claro que não se importa com o tipo de tecnologia empregada para a realização do tratamento, se por meio digital ou analógico, com o uso de inteligência artificial, de forma automatizada ou manualmente. Assim, aplica-se a LGPD para dados existentes em papel, no histórico de uma clínica hospitalar; na memória do computador de uma instituição financeira que armazena os dados bancários de seu cliente; em uma fita guardada pelo departamento de atendimento ao cliente de um agente de viagens; ou em imagens gravadas em circuito fechado de TV, por exemplo." (VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 52)

[151] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que [...] (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de

A LGPD é aplicável às pessoas físicas[152] e jurídicas que tratem dados pessoas, sejam eles de direito público ou privado[153]. A aplicação à pessoa natural está condicionada a existência de uma relação entre o tratamento e alguma atividade comercial ou profissional[154]. No que se refere à aplicação da LGPD às pessoas de direito público, o art. 23 prevê algumas especificidades, como a necessidade do tratamento ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que, dentre outros requisitos, forneçam informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso[155]. Já as atividades delegadas ao setor privado pelo Poder Público, como os serviços notariais e os de registro, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público[156], diferentemente das sociedades de economia mista e empresas

---

Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[152] Art. 2º A personalidade civil da pessoa começa do nascimento com vida; art.3º - No entanto, são absolutamente incapazes de exercer pessoalmente os atos da vida civil os menos de dezesseis anos; art.5º - A menoridade cessa aos dezoito anos completos, quando a pessoa fica habilitada à prática de todos os atos da vida civil; art. 5º, parágrafo único – Cessará para os menores, a incapacidade: I- pela concessão dos pais, ou de um deles na falta do outro, mediante instrumento público, independentemente de homologação judicial, ou por sentença do juiz, ouvido o tutor, se o menor tiver dezesseis anos completos; II- pelo casamento; III- pelo exercício de emprego público efetivo; IV- pela colação de grau em curso de ensino superior; V- pelo estabelecimento civil ou comercial, ou pela existência de relação de emprego, desde que, em função deles, o menor com dezesseis anos completos tenha economia própria. (BRASIL. **Lei nº 10.406,** de 10 de janeiro de 2002. Institui o Código Civil. 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 20 jun. 2020.)

[153]Art. 44. São pessoas jurídicas de direito privado: I- as associações; II- as sociedades; III- as fundações; IV- as organizações religiosas; V- os partidos políticos; VI- as empresas individuais de responsabilidade limitada. (BRASIL. **Lei nº 10.406,** de 10 de janeiro de 2002. Institui o Código Civil. 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 20 jun. 2020)

[154] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[155] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[156] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: [...] § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei. (BRASIL. **Lei nº 13.709,**

públicas sob o regime de concorrência quando não estiverem operacionalizando políticas públicas, que neste caso terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado[157].

Ampliando ainda mais a sua jurisdição, a aplicação da LGPD independe do país da sede ou do país onde estão localizados os dados tratados. Como consequência da internet, há uma considerável redução no impacto das fronteiras territoriais no que se refere ao fluxo internacional de dados, que passou a ocorrer de forma natural e quase que imperceptível aos olhos do homem-médio. Apesar do livre arbítrio de cada estado para regular os atos que foram praticados dentro do seu território de forma independente, a criação de legislações semelhantes se demonstra extremamente benéfica para a desburocratização do fluxo internacional de dados. Neste sentido, a LGPD prevê em seu art. 33, I, a permissão da livre transferência internacional de dados para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado nos parâmetros previstos na Lei. A proximidade da LGPD com o GDPR, tendo ambos as mesmas hipóteses de legalidade, se demonstra extremamente vantajosa para o Brasil, colocando-o no cenário da economia digital mundial, uma vez que a regulamentação europeia prevê a possibilidade de transferência dos dados pessoais para um país terceiro desde que a regulamentação deste país seja avaliada e considerada com nível de proteção adequada pela Comissão Europeia[158].

Na LGPD, as aplicações territoriais e extraterritoriais, que são hipóteses independentes entre si, estão condicionadas a algumas condições disciplinadas nos incisos do art. 3º:

---

de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[157] Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[158] Art. 45, do GDPR. Ao avaliar a adequação do nível de proteção do país terceiro, a Comissão levará em conta: respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência; b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

> I- a operação de tratamento seja realizada no território nacional.
> II- 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; ou
> III- os dados pessoais objeto do tratamento tenham sido coletados no território nacional
> §1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> §2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Tendo em vista o limite da soberania de cada país estar associado à sua fronteira física, o primeiro ponto para a aplicação material da LGPD se refere ao espaço físico em que a operação de tratamento ocorre. Ou seja, para aplicação da lei, a operação tem que ser realizada em território nacional, seja a operação uma coleta, recepção, utilização, transmissão, arquivamento, dentre outras, independentemente da entidade ser localizada no Brasil. Ou seja, informações a respeito do lugar da coleta de dados, da nacionalidade e residência dos indivíduos que têm os seus dados tratados, são irrelevantes para a aplicação do inciso I, pois a sua aplicabilidade se refere à necessidade da operação de tratamento de dados ser realizada no território nacional[159] Ou seja, deverá cumprir a Lei brasileira quando a empresa opera o tratamento de dados em território nacional.

A aplicação extraterritorial da LGPD está definida pelos incisos II e III. Para Marcel Leonardi, a competência jurisdicional deve levar em conta os efeitos locais das informações disponibilizadas na internet e não os efeitos do local onde estão armazenados os dados[160]. Neste sentido, o inciso II prevê que, independentemente da sede física do responsável pelo tratamento dos dados pessoais, quando no caso concreto as eventuais lesões aos titulares cause impacto no Brasil, seja pelo fato dos indivíduos estarem localizados no Brasil ou o foco do produto ou serviço ser o mercado brasileiro, a atividade estará dentro do campo de proteção da LGPD. Nesta mesma linha de raciocínio se posicionou a 4ª Câmara de Direito Criminal do TJ/SP em importante julgado:

> Uma ordem emanada de um juiz de Direito integra a soberania nacional, não possuindo superiores na ordem externa e nem iguais na ordem interna. Se o Facebook opera no Brasil, está sujeito às leis brasileiras. Nesse cenário, é irrecusável

[159] "Portanto, se uma empresa com sede no Brasil desenvolveu um aplicativo de compartilhamento de bicicletas somente para usuários no EUA e Europa, disponibilizando o serviço somente para essas duas localidades, coletando dados pessoais apenas internacionalmente, sem quaisquer dados de brasileiros, como as atividades de processamento de dados pessoais são realizadas pelo controlador, no Brasil, portanto, em território nacional, aplicar-se-á a LGPD". VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 58.
[160] LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Editora Saraiva, 2012, p. 247.

> que o fato das informações solicitadas estarem armazenadas em outro país obstaculize o cumprimento de determinação emanada da autoridade impetrada[161].

Cumpre destacar a imprecisão técnica presente na redação dos incisos explicados acima. No inciso I, o termo "operação de tratamento" utilizado para se referir ao estabelecimento que tratam dados pessoais no território nacional é completamente amplo, tendo em vista que abarca o dever de cumprimento da LGPD aos agentes estrangeiros, mesmo que não tenham sede no Brasil, mas que "operam" dados no Brasil. O inciso III basicamente diz que: não importa a atividade do agente de tratamento de dados no Brasil, seja atividade de fornecimento de bens e serviços ou o tratamento de dados de indivíduos localizados no Brasil, a LGPD se aplica a mera coleta de qualquer dado pessoal localizado em território nacional. Conforme entende Rony Vainzof, diante da atecnia do inciso primeiro, seria coerente a sua correção com base no critério do estabelecimento do agente de tratamento e a como consequência, a eliminação do inciso III, pois assim a aplicação extraterritorial da LGPD seria apenas com a comprovação de que "o agente de tratamento estrangeiro tenha como objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional" e não com "a mera coleta de qualquer dado pessoal em território nacional" [162].

Portanto, em razão das apontadas falhas dos incisos analisados, o inciso II que se refere à aplicação extraterritorial da lei independentemente da localização geográfica do agente e da atividade de tratamento exercida, desde que os dados de indivíduos se localizam no território nacional, acaba se tornando sem efetividade[163]. Ainda, a aplicabilidade extremamente ampla da LGPD é um grande risco, podendo causar um grave impacto negativo na economia e na prestação de serviços no Brasil, tendo em vista que diversas empresas de tecnologia impediram que residentes da UE utilizassem os seus serviços e a aplicabilidade extraterritorial do GDPR é mais restrita do que a LGPD. Em razão da competência para deliberar sobre a

---

[161] BRASIL. Tribunal de Justiça de São Paulo. Mandado de Segurança nº 2073993-57.2014.8.26.0000. Relator: Desembargador Edison Brandão. Data de julgamento: 16 dez. 2014.

[162] VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 64.

[163] "Invariavelmente, tanto as aplicações mais básicas quanto às mais modernas e avançadas, tratam (ou seja, coletam) algum tipo de dado pessoal. Sites institucionais, revistas digitais, pesquisas de hotéis, passagens aéreas, locação de carros, aplicativos fitness e de acompanhamento de saúde, jogos e brincadeiras on-line, todos eles tratam dados pessoais. Redes sociais e globais de cooperação e produção de valor são construídas a partir de serviços movidos por dados, assim como a grande parte das startups. Caso todas essas novas empresas tomem conhecimento que um mero acesso oriundo do Brasil pode implicar o dever de cumprimento e respectivas sanções da LGPD, certamente bloqueariam o acesso visando mitigar esse risco". (VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 55)

interpretação da LGPD[164], cabe à atuação da Agência Nacional de Proteção de Dados para trazer mais clareza à redação deste inciso, diminuindo a sua amplitude.

Diferentemente, o GDPR, já atento à imprecisão técnica que poderia advir das hipóteses de aplicação territorial, prevê a sua aplicação de forma mais precisa. Ou seja, também em seu art. 3º estabelece a sua aplicação ao tratamento de dados pessoais: efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento situado no território da UE, independentemente da localização do tratamento, seja dentro ou fora da União, mitigando o risco de sobreposições[165]; quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a titulares que se encontram na UE ou ao controle de comportamento destes titulares, mesmo quando o agente de tratamento não está situado dentro da UE[166].

Além do mais, há as situações em que ocorre o tratamento de dados pessoais, mas não cabe a aplicação da LGPD, conforme prevê o art.4º, nos seguintes termos:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao

---

[164] Art. 55-J. Compete à ANPD: [...] III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[165] Art. 3º Âmbito de aplicação territorial. 1.. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[166] Art. 3º, 2.O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

> atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> §2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 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.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

3.1 OS AGENTES DE TRATAMENTO E A AUTORIDADE NACIONA L DE PROTEÇÃO DE DADOS

Para fins de aplicação da LGPD, os agentes de tratamento são aqueles responsáveis pelo exercício de tratamento de dados pessoais, seja ele o controlador ou operador. A distinção entre ambas as espécies de agentes de tratamento demonstra-se extremamente importante, principalmente diante da clara divisão de responsabilidade entre controladores e operadores de dados pessoais[167]. Conforme já mencionado, ambas as categorias de agentes podem ser pessoa natural ou física, de direito público ou privado. O controlador se caracteriza como aquele a quem compete às decisões referentes ao tratamento de dados pessoais, como as

[167] 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: 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; 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. § 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. § 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. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. 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. 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: 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. 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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

condições, finalidades e os meios de processamento[168]. Já o operador é o sujeito que realiza o tratamento de dados, quem efetivamente "põe a mão na massa", em nome do controlador[169]. Cumpre destacar que, para a identificação de cada um dos agentes é necessário fazer uma análise fática específica, havendo ainda a possibilidade de "co-controladores"[170]. Desta forma, é possível que uma mesma pessoa jurídica figure como controlador e operador em situações distintas, pois estas figuras (controlador e operador) não são fixas.

A expressão "controlador" é utilizada mais de 50 vezes na LGPD, enquanto a expressão "operador" é utilizada menos de 20 vezes em seu texto. Essa breve análise numérica de quantas vezes cada agente de tratamento é mencionado no corpo da LGPD demonstra as diversas atribuições dadas ao controlador, principalmente por ser o agente que efetivamente exerce o papel decisório. Além de assumir a responsabilidade de assegurar a base legal para o tratamento de dados[171], o controlador é também o responsável pela garantia dos direitos dos titulares de dados[172], sendo o agente que representa de fato a coleta e tratamento de dados diante dos titulares – identificando-o pessoalmente[173] e provendo as informações

---

[168] Art. 5º Para os fins desta Lei, considera-se: [...] III - dado anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[169] Art. 5º [...] V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[170] "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 13.o e 14.o, 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 contato para os titulares dos dados". (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[171] Nas hipóteses dos artigos 7º e 11. Assunto aprofundado no capítulo 3.2.

[172] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[173] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...] III - identificação do controlador;

necessárias[174]. Ou seja, é o controlador que mantém as relações diretas com os titulares. E, mais importante, o controlador é o responsável por indicar o encarregado pelo tratamento de dados pessoais - pela atividade de delegação, na maioria das vezes de cunho contratual, criando uma espécie de mandato para o operador[175].

Conforme as condições básicas para que o sujeito figure como operador indicadas pelo documento técnico do *Article 29 Working Party*[176], que foi utilizado como inspiração na LGPD[177], o operador deve necessariamente ser uma entidade jurídica separada do controlador e ter de fato o comando do tratamento de dados pessoais. Este comando, no entanto, conforme prevê o art. 39 da LGPD, deve ser realizado em conformidade com as instruções fornecidas pelo controlador. Ou seja, as suas atribuições estão diretamente relacionadas ao cumprimento do mandato de tratamento de dados pessoais instituído pelo controlador. No que se refere a uma subcontratação de "suboperadores", por não haver menção expressa no sentido de proibir tal contratação na LGPD e nem no GDPR, o entendimento predominante é pela sua possibilidade, ainda mais diante dos diversos informes que vem sendo publicados por Autoridades de Proteção de Dados Pessoais acerca do regramento da relação jurídica entre os operadores e os "suboperadores"[178].

A título de ilustração, uma rede de lojas contrata uma empresa de serviços de Tecnologia da Informação para armazenar os dados de seus clientes. O motivo por trás do armazenamento,

---

(BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[174] Art. 9º [...] V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[175] Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.

[176] EUROPEAN COMISSION. ***Article 29 Working Party.*** Disponível em: https://ec.europora.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 15 mar. 2020.

[177] ZANATTA, Rafael A. F. **Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor.** São Paulo: Editora Revista dos Tribunais, 2019, p. 186.

[178] INGLATERRA. Information Comissioner's Office. **Informe.** Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#5. Acesso em: 18 abr. 2020.

seja ele relacionado à criação de um sistema de fidelidade ou só para manter o contato dos clientes, bem como o período de armazenamento, serão decisões feitas pela rede de lojas, exercendo, neste caso, a função de controladora. Enquanto a rede de lojas se caracteriza como a figura central quanto à tomada de decisões referentes aos dados pessoais, a empresa de TI é a responsável pelo armazenamento de fato dos dados, pelo seu comando e, portanto, exerce a função de operadora. Cumpre mencionar que, por ser característica intrínseca da própria natureza do trabalho do operador a escolha dos meios técnicos a serem utilizados, pode-se dizer que possui certa liberdade na tomada de decisões. Porém, no que pese ser a empresa de TI a responsável pela escolha dos meios técnicos mais adequados para o melhor desempenho da função, qual seja, um armazenamento seguro e acessível, não é possível atribuir a ela a qualidade de controladora. O controle sobre o conteúdo do banco de dados, bem como o porquê do seu armazenamento continuam sendo atividades cabíveis à rede de lojas.

3.1.1 A figura do encarregado

Ainda, na relação de tratamento de dados pessoais há a figura do encarregado, que apesar de ser expressamente regulamentado na Seção II do Capítulo VI da LGPD, possuindo inclusive uma espécie de micro regime jurídico, foi alvo de polêmicas desde a aprovação da referida Lei[179]. O encarregado deve ser identificado publicamente e preferencialmente, no sítio eletrônico do controlador[180]. As suas funções são previstas na Lei de forma clara, possuindo o

[179] "Inicialmente o texto legal previa o encarregado como pessoa natural indicada pelo controlador que deveria atual como canal de comunicação entre o controlador e os titulares e a autoridade nacional. Com a Medida Provisória869/2018, assinada por Michel Temer, em dezembro de 2018, abriu-se a possibilidade de o encarregado ser também pessoa jurídica, tal como acontece na União Europeia (é possível até mesmo que Municípios e entes da Administração Pública indiquem escritórios de advocacia e consultorias para a figura do encarregado.) Com a votação do relatório final da Comissão Especial que analisou a MP 869/2018 entre março e abril, definiu-se que o encarregado é simplesmente 'pessoa indicada pelo controlador' para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados Pessoais. Com a votação do Projeto de Lei de Conversão 07/2019, houve ampliação das regras sobre os encarregados, atribuindo-lhes estabilidade profissional (apenas em sentido normativo) e determinando que deverá ser detentor de conhecimentos jurídicos e regulatórios sobre proteção de dados pessoais." (ZANATTA, Rafael A. F. **Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor.** São Paulo: Editora Revista dos Tribunais, 2019, p. 188).

[180] Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

encarregado quatro funções distintas[181]. A primeira consiste em resolver os problemas relatados pelos titulares e prestar a eles os esclarecimentos necessários. Também, é o responsável por receber as comunicações da ANPD, figurando como uma espécie de canal de interação institucional entre a agência e o controlador. A terceira se refere a uma atividade interna, devendo o encarregado orientar os funcionários e contratados a respeito das práticas que devem ser adotadas para uma efetiva proteção de dados pessoais.

Diante da *expertise* necessária para exercer a terceira função principalmente, surge o questionamento acerca da necessidade deste indivíduo ter formação jurídica. Em maio de 2019, ficou determinado com a votação da versão da MP 869/2018 que o encarregado, mesmo quando for da área de tecnologia, ainda assim deve possuir não só conhecimento jurídico em geral, como também a compreensão especifica do sistema regulatório de proteção de dados pessoais. Por fim, a quarta função do encarregado se refere à execução das atribuições definidas pelo controlador ou estabelecidas em normas complementares. Cumpre destacar que, essas quatro funções são claramente descritas na LGPD, mas a lei não se refere às atividades exercidas pelo encarregado de maneira taxativa[182].

Portanto, a relação jurídica tutelada pela LGPD é composta, essencialmente, pelos agentes de tratamento e os titulares de dados pessoais, podendo ou não haver a presença dos encarregados. O titular de dados é definido como "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"[183]. Portanto, a pessoa jurídica, independentemente do seu campo de atuação, não é titular de dados para fins de proteção da LGPD[184]. Percebe-se

---

[181] Art. 41. [...] § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[182] Como exemplo, segue outras diversas funções do Encarregado: "orientar os colaboradores da entidade da qual é Encarregado, a respeito das práticas relacionadas à proteção de dados pessoais; assessorar os responsáveis pelo tratamento de dados pessoais na emissão de relatórios de impacto à proteção de dados pessoais, emitindo opiniões e pareceres que possam embasar tais relatórios; recomendar as salvaguardas para mitigar quaisquer riscos aos direitos dos titulares de dados pessoais tratados pela empresa, inclusive salvaguardas técnicas e medidas organizacionais". (BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019, p. 316)

[183] Art. 5º Para os fins desta Lei, considera-se: [...] V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[184] Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. (BRASIL. **Lei nº 13.709,** de 14

ainda, da leitura do art.1º[185], a preocupação do legislador em caracterizar o titular dos dados como parte vulnerável na relação composta por ele e os agentes de tratamento ao utilizar o verbo "proteger" na sua redação[186]. Tendo em vista a atual capacidade computacional de processamento de dados como um dos resultados do Big Data, da Internet das Coisas e da Inteligência Artificial[187], a LGPD busca de alguma forma mitigar os riscos, estabelecendo normas bem definidas sobre o tratamento de dados pessoais, que serão aprofundadas mais a frente[188].

3.1.2 A Autoridade Nacional de Proteção de Dados

Visando a fiscalização, regularização e normatização da relação jurídica mencionada no tópico anterior (3.1), após muitas modificações na LGDP, a Autoridade Nacional de Proteção de Dados foi constituída. Pode-se dizer que, diante da dificuldade de acompanhamento do tratamento e dos efeitos deste pelos seus titulares, além de outros diversos aspectos que dificultam a efetividade da proteção de dados, uma Autoridade para a proteção de Dados se demonstra extremamente benéfica e necessária. Uma breve análise destas modificações é essencial para o entendimento acerca da ausência de autonomia administrativa e financeira da

---

de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[185] 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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[186] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** São Paulo: Editora Revista dos Tribunais, 2018, p. 59.

[187] "(6) A rápida evolução tecnológica e a globalização criaram desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registraram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção de dados pessoais. (7) Essa evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiando por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[188] Ver tópico 3.3.

ANPD, destoando da forte tendência internacional de criação de autoridades de proteção de dados independentes[189].

Inicialmente, a Autoridade foi incluída no texto legal do Projeto de Lei 527/2016 como uma autarquia federal em regime especial. No que pese o texto ter sido aprovado pelos plenários da Câmara dos Deputados e do Senado Federal, foi vetado pelo Presidente da República, sob o argumento de que a competência para propor aumento de despesas em projeto de lei é do Poder Executivo e não do Poder Legislativo. Neste sentido, mesmo quando sancionada em 2018, as disposições referentes à estruturação da ANPD foram vetadas.

Diante da clara necessidade de uma alguma espécie de autoridade para garantir a efetividade da LGPD, o Poder Executivo publicou a Medida Provisória 869/2018, criando a ANPD. Após passar pela análise da Comissão Mista no Congresso nacional, no dia 8 de julho de 2019 a referida MP foi convertida na Lei 13.853 de 2019. Com as modificações conferidas pela Lei 13.853/2019, a ANPD, por se caracterizar como um órgão da administração pública federal, integrante da Presidência da República, possui apenas autonomia técnica e decisória[190]. Ainda, no que se refere à sua natureza, há de se mencionar o seu caráter transitório, tendo em vista a previsão de uma análise, que ocorrerá em até dois anos da entrada em vigor da sua estrutura regimental, acerca da possibilidade da sua transformação pelo Poder Executivo em uma "entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República[191]".

No que se refere à importância da independência e autonomia das Autoridades de Proteção de Dados tanto para o setor público, quanto para o setor privado, Danilo Doneda explica[192]:

> A independência dessas autoridades é um atributo fundamental para que sua missão seja exitosa. Essa independência é importante não somente para a tutela do cidadão, como também para a estruturação de todo o sistema normativo de proteção de dados, que compreende aspectos da regulação do próprio fluxo de dados. Também para o

[189] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 307.
[190] Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)
[191] Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)
[192] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 315.

> setor privado uma Autoridade afigura-se como útil por diversos motivos, como manter padrões persistentes de aplicação da lei – diferentemente de tribunais, que são em geral chamados a decidir sobre situações particulares. Essa consistência, aliás, também é importante para impedir que empresas que eventualmente não cumpram com uma legislação de proteção de dados tenham vantagens competitivas em relação às demais, com prejuízo para os cidadãos. Ainda, a Autoridade possui um arsenal mais específico de medidas regulatórias à sua disposição do que os tribunais, inclusive com medias de caráter preventivo como aconselhamento ou advertências, chegando até um regime sancionatório próprio, adaptado á natureza da matéria e com metodologia própria. Isso, somado ao fato de que a centralização da matéria em uma Autoridade evita o risco da fragmentação da interpretação da lei entre tribunais e mesmo outros órgãos administrativos com competências eventualmente concorrentes, garante a uniformidade dos direitos do cidadão e a segurança jurídica na aplicação da legislação de proteção de dados.

A Autoridade Nacional de Proteção de Dados possui uma estrutura organizacional composta por cinco diferentes órgãos. Há o Conselho Diretor, que é órgão máximo de direção, composto por cinco diretores com mandato de quatro anos escolhidos e nomeados pelo Presidente da República após aprovação do Senado Federal nos ditames do art.51, inciso III, alínea 'f' da Constituição Federal. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por 23 representantes de diferentes órgãos públicos, sendo a quantidade de representantes de cada órgão especificada no art. 58-A da LGPD, ainda, faz parte da estrutura da ANPD uma Corregedoria, Ouvidoria e um órgão de assessoramento jurídico próprio.

Dentre as atividades conferidas à Autoridade Nacional de Proteção de Dados, destacam-se as de: zelar pela proteção de dados pessoais, fiscalizar a atuação dos agentes de tratamento e aplicar sanções administrativas[193] quando for configurado o tratamento irregular de dados pessoais; facilitar a vida dos cidadãos (e titulares de dados pessoais) através da implementação de mecanismos simplificados para o registro de reclamações acerca do tratamento de dados em desconformidade com a LGPD, assim como auxiliar o exercício do controle dos titulares sobre os seus dados pessoais. A ANPD é também a encarregada por promover ações de cooperação com as autoridades de proteção de dados pessoais de outros países, facilitando a transferência internacional de dados e, consequentemente, impulsionando negócios entre o Brasil e os países que possuem um sistema de proteção de dados adequado.

[193] Ver Tópico 4.5.2.

3.1.2.1 O Relatório de Impacto à Proteção de Dados

A Autoridade Nacional de Proteção de Dados, como órgão da administração pública responsável por zelar, fiscalizar e implementar o cumprimento da LGPD em todo o território nacional, possui competência para editar e solicitar os Relatórios de Impacto à Proteção de Dados Pessoais (RIPD). Estes relatórios, que são de responsabilidade do controlador, se caracterizam como documentos extremamente importantes para a demonstração de que o tratamento está sendo efetuado em conformidade com a lei. Portanto, conforme definição dada pelo art.5º, XVII, deve constar no RIPD a "descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco". No entanto, o controlador tem que respeitar o conteúdo mínimo do RIPD, qual seja: a descrição dos tipos de dados coletados, a metodologia utilizada pela empresa tanto para a coleta quanto para a garantia de segurança das informações sobre sua posse e a sua análise a respeito das salvaguardas e mecanismos para a mitigação dos possíveis riscos[194].

O RIPD poderá ser solicitado nos casos em que há a possibilidade de ocorrer impacto na privacidade de dados pessoais, como exemplo, há o tratamento de dados realizado para fins de segurança pública, defesa nacional, segurança dos Estados ou atividades de investigação e repressão de infrações penais, sendo estas as atividades de tratamento que não estão sob o escopo de aplicação da LGPD[195] e nos casos de tratamento irregular por agentes do Poder Público[196]. No que pese ser de responsabilidade do colaborador a elaboração de Relatórios de

---

[194] 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[195] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[196] Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.; 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

Impacto à Proteção de Dados Pessoais nos casos previstos em lei, a Autoridade Nacional de Proteção de Dados é legitimada a solicitar a sua elaboração a qualquer momento[197].

Assim como na LGPD, o GDPR, com base na ideia de mitigação dos riscos, prevê a obrigatoriedade de elaboração de Relatórios de Impacto à Proteção de Dados Pessoais nos casos de utilização de novas tecnologias que, diante do contexto, natureza e finalidade do tratamento, poderão implicar em risco à liberdade e aos direitos dos titulares[198]. No entanto, diferentemente da LGPD, o GDPR estabelece que o controlador, nos casos em que o RIPD indique a impossibilidade de atenuação dos riscos, mesmo com as medidas adequadas, deve, antes de iniciar a operação de tratamento de dados pessoais, consultar a Autoridade de Proteção de Dados Pessoais[199].

Visando a efetividade do princípio da prevenção previsto no art. 6º, VIII, o Guia de Boas Práticas da LGPD sugere que o RIPD seja elaborado antes de ser iniciado o tratamento de dados pessoais[200], mas levando em consideração todo o ciclo de vida dos dados. Portanto, nos casos em que há a necessidade do RIPD[201], é recomendado que o controlador, desde a fase

---

[197] 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[198] Art. 35. 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[199] Art. 36. 1. O responsável pelo tratamento consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35. o indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[200] 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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[201] O Guia de Boas Práticas da LGPD elenca diversos tipos de tratamento de dados pessoais, assim como situações decorrentes do tratamento, que caracterizam a necessidade de elaboração do Relatório de Impacto à Proteção de Dados Pessoais: "uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados; rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º); tratamento de dado pessoal sobre 'origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural' (LGPD, art. 5º, II); processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20); tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);

inicial do projeto que irá utilizar dados pessoais, elaborar tal relatório[202]. O RIPD deve, inclusive, ser incorporado dentro dos mecanismos de governança em privacidade coorporativa do controlador, tema desenvolvido na seção II do Capítulo VII da LGPD. As regras de boa prática e de governança são, no entanto, uma faculdade dos controladores e operadores, que possuem liberdade para formular ou não estas regras. Ao estabelecerem as condições de organização, o regime de funcionamento, procedimentos, padrões técnicos e as obrigações específicas para todos os envolvidos no tratamento, as regras criam uma espécie de autorregulação de acordo com as peculiaridades da empresa e, portanto, se demonstram extremamente benéficas[203].

Diante dos diversos tipos de organizações que efetuam o tratamento de dados e estão sujeitas às disposições da LGPD, não seria razoável estabelecer as mesmas normas de segurança para todas as empresas públicas e privadas e, portanto, é dada a possibilidade de que formulem as suas próprias regras. A falta de razoabilidade de uma regra geral de boa prática e governança fica clara ao comparar as regras a serem seguidas por um "mercadinho de bairro" e aquelas que devem seguir determinado hospital.

As fases de elaboração do RIPD consistem em: 1) identificar os agentes de tratamento (controlador e operador) e o encarregado, por ser ele o canal de comunicação entre os titulares dos dados e o controlador, assim como com a ANPD; 2) analisar a necessidade de elaboração do relatório; 3) descrever o tipo de tratamento de dados, especificando a sua natureza, escopo e finalidade; 4) identificar as partes interessadas para extrair delas opiniões acerca do que consideram importante ser observado no tratamento de dados; 5) descrever os mecanismos utilizados pela empresa para garantir que seja observado o tratamento proporcional e apenas

---

tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42); tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º); tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º); alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades." (BRASIL. **Guia de boas práticas da Lei Geral de Proteção de Dados.** Brasília, DF. 2020. P. 41. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 10 jun. 2020)

[202] BRASIL. **Guia de boas práticas da Lei Geral de Proteção de Dados.** Brasília, DF. 2020. P. 41. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 10 jun. 2020

[203] "No que pese estar se referido às questões da Internet, Marcel Leonardi faz algumas considerações relacionadas aos benefícios da autorregulação: "o sistema de autorregulação pelos próprios participantes funciona muito bem em fóruns e listas de discussão voltadas para um tópico ou interesse específico, que contam com um número limitado de usuários moderadores para fazer cumprir as regras estabelecidas. Isso não significa porem que essas 'comunidades' online estejam imunes ao sistema jurídico, nem que suas normas devem sempre prevalecer em caso de disputas entre usuários". (LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Editora Saraiva, 2012, p. 247.)

com os dados necessários; 6) identificar e avaliar os riscos, identificando em cada risco a sua probabilidade de ocorrência, nível e os seus possíveis impactos nos direitos dos titulares; 7) identificar as medidas para mitigar/tratar os riscos encontrados; 8) formalizar o Relatório, recolhendo as assinaturas do responsável pela sua elaboração, pelo encarregado e pelas autoridades que representar o controlador e o operador. Cumpre mencionar que, apesar do controlador ser o responsável pela elaboração do RIPD, nada impede que delegue essa atividade para o encarregado ou qualquer outra pessoa com conhecimento técnico para tal. Ainda, é também de responsabilidade do controlador revisar o RIPD sempre que existirem mudanças que afetem diretamente o tratamento de dados pessoais pela instituição.

3.1.3 Das obrigações dos agentes

A elaboração de Relatórios de Impacto à Proteção de Dados pessoais é apenas uma das muitas atividades sob a responsabilidade dos agentes de tratamento de dados pessoais. No entanto, como já explicado no tópico acima (3.1.2.1), a elaboração do RIPD, quando necessário, é uma atividade de responsabilidade do controlador, não significando, no entanto, que não ele não possa delegá-la[204]. No que pese os agentes de tratamento de dados pessoais estarem sujeitos a grandes responsabilidades, estas se dividem, havendo deveres a serem cumpridos apenas pelo controlador, apenas pelo operador e aqueles que são de responsabilidade de ambos. Portanto, além da necessidade de atuar dentro de uma das bases legais de tratamento[205], de seguir os

[204] 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[205] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018.

princípios norteadores das atividades de tratamento previstos no art. 6º da LGPD e de garantir os direitos dos titulares de dados[206], os agentes de tratamento se deparam com diversas outras obrigações determinadas em lei.

O não cumprimento destas obrigações estabelecidas pela LGPD está relacionado a diferentes consequências que serão aprofundadas no Tópico 4.5 deste Trabalho. Além da previsão de multas em caso de violação dos princípios básicos de até 2% da receita anual da empresa, limitando-se ao valor de 50 milhões por infração[207], diante do valor que possui a proteção de dados para os consumidores, estas empresas estarão sujeitas a grandes danos às suas reputações. Neste sentido, a ANPD possui competência para solicitar a proibição de processamento temporária ou definitiva da atividade da empresa, a depender do caso concreto[208]. Quando configurado o dano material ou moral ao titular dos dados diante da violação da LGPD, estarão os agentes de tratamento sujeitos à responsabilização sob os termos do art. 42[209]. Além do mais, deve ser levado em consideração pelas empresas os altos custos para a implementação de medidas de remediação.

Em seu art. 9º, a LGPD demonstra o dever de compromisso com o princípio do livre acesso quando prevê que é de responsabilidade do controlador prover o acesso facilitado das informações acerca do tratamento ao titular de dados. Além da necessidade destas informações serem disponibilizadas de forma clara, o legislador também previu os tipos de informações que devem ser expostas ao titular. Dentre elas, o controlador possui o dever de informar o seu contato telefônico e dispor de forma adequada e ostensiva a finalidade do tratamento, a sua forma e duração de forma específica. Ainda, quando solicitado, o controlador está sujeito à prestação de contas ao titular respeito das suas informações que estão sob o seu tratamento[210]. Essa requisição poderá ser feita a qualquer momento, desde que

---

Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.)

[206] Assunto aprofundado no Tópico 3.2.

[207] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...] II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[208] Art. 52. [...] XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[209] Assunto aprofundado no Tópico 4.5.1.

[210] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos

o titular ou representante legalmente constituído por ele faça por meio de um requerimento expresso[211].

Caso haja a configuração das hipóteses que caracterizam o término de tratamento de dados[212], a exemplo do alcance da finalidade almejada, cabe ao controlador cumprir com o dever de descarte previsto no art. 16 da LGPD. A lei prevê ainda, de forma taxativa, quais situações permitem a continuação do tratamento mesmo após a configuração de uma das quatro hipóteses de término. São elas: o cumprimento de obrigação legal ou regulatória, transferência à terceiro (desde que respeitados os requisitos de tratamento de dados previstos em lei), estudo por órgão de pesquisa e a utilização dos dados de forma anonimizada pelo controlador.

No que se refere aos deveres que são de responsabilidade de ambos, tem-se que, tanto o controlador quanto o operador devem manter registro das operações de tratamento de dados que realizarem[213]. O registro, que visa o mapeamento das operações efetuadas, demonstra-se extremamente necessário para um planejamento de mitigação de riscos efetivo e corrobora com a necessidade de prestação de contas, princípio expresso no art. 6º, inciso X da LGPD. Diferentemente da regulamentação brasileira, o GDPR prevê de forma taxativa as hipóteses em que os agentes precisam registrar as operações de tratamento de dados pessoais[214]. No

---

dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[211] Art. 18. [...] § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[212] Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II - fim do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[213] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[214] De acordo com o artigo 30 (5) do GDPR, não estarão obrigadas a realizarem o registro das operações de tratamento de dados as empresas que preenche estes três requisitos cumulativamente: (i) empregam menos de 250 pessoas, (ii) não realizam processamento de alto risco (iii) nem de categorias especiais de dados e

que pese a LGPD não estabelecer critérios mínimos para a obrigatoriedade deste registro, nada impede que a ANPD futuramente venha a ajustar parâmetros mínimos. Diante dessa ausência regulatória na Lei, entende-se que, toda empresa que realiza atividades de tratamento de dados pessoais, independentemente do tipo de dado tratado, possui a obrigação de realizar o registo das suas operações.

Há também as questões práticas e técnicas que fazem parte do dia-a-dia dos agentes de tratamento. O controlador, por exemplo, deve indicar o encarregado, além de ser o responsável por estabelecer as condições, finalidades e os meios do processamento. Já o operador, não possui capacidade decisória, devendo seguir estritamente as instruções fornecidas pelo controlador[215]. No que pese a existência de uma relação de subordinação entre os agentes, o operador possui liberdade para adotar medidas para melhor adequação à LGPD, mesmo que não tenham sido instituídas pelo controlador. A adoção de medidas técnicas e organizacionais de segurança previstas no art. 46 da LGPD também devem ser consideradas pelo operador independentemente das instruções do controlador.

3.1.3.1 O dever de notificação e os incidentes de segurança

Ao dedicar o capítulo VII inteiramente para a regulamentação das medidas de segurança técnicas e administrativas que devem ser adotadas pelos agentes de tratamento, a LGPD demonstra a relevância do tema para a proteção de dados pessoais. Diante do alto risco do acesso não autorizado aos bancos de dados e do tratamento realizado de forma inadequada ou ilícita, a Lei estabelece os princípios da segurança e da prevenção e ainda, em seu artigo 46, se refere à necessidade de adoção de medidas de segurança pelo controlador e pelo operador. As medidas se classificam em medidas técnicas[216], que estão diretamente ligadas aos recursos

---

antecedentes criminais, e (iv) realizam processamento ocasional. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[215] Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[216] "As medidas técnicas são aquelas adotadas no âmbito da Tecnologia da Informação, com o uso de recursos informáticos dotados de funcionalidades voltadas à garantia da segurança da informação. São exemplos dessas tecnologias: ferramentas de autenticação de acesso a sistemas, mecanismos de segurança em softwares e hardwares, recurso de controle de tráfego de dados em rede, instrumentos detectores de invasões de sistemas, recursos de criptografia, segregação de servidores, ferramentas de prevenção à perda de dados, testes de vulnerabilidade, cópias de segurança, entre muitos outros." (JIMENE, Camila do Valle. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 329)

informáticos e medidas administrativas[217], sendo aquelas de natureza organizacionaia e jurídicas[218]. A utilização da conjunção adjetiva "e" no texto legal ao se referir aos dois tipos de medidas técnicas, demonstra que, para estar adequada à lei, a empresa que efetua o tratamento deve adotar soluções multidisciplinares para garantir a segurança dos dados em suas bases.

Para garantir a efetividade do disposto no caput do art. 46, a Autoridade Nacional de Proteção de Dados poderá dispor sobre padrões técnicos mínimos. Isso não significa, no entanto, que os agentes de tratamento só devem se preocupar com a adoção destas medidas após manifestação da ANPD[219]. Ao definir tais padrões a Autoridade deverá levar em consideração "a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis[220]". Essas medidas de segurança devem ser observadas tanto pelos agentes de tratamento quanto por qualquer outra pessoa que intervenha em uma das fases tratamento. Ainda, garante a proteção de dados pessoais desde a idealização do produto ou serviço até a fase de execução [221] e mesmo após o término do processo de tratamento[222].

---

[217] "As medidas administrativas são atividades realizadas no âmbito administrativo-gerencial dos agentes de tratamento, incluindo-se as de natureza jurídica. São exemplos de medidas administrativas: políticas corporativas para proteção dos dados pessoais, contratos de confidencialidade, políticas de privacidade de sites e aplicativos, capacitação dos empregados cujas atividades envolvam o tratamento de dados pessoais, controle de acesso aos arquivos físicos, entre outras". (JIMENE, Camila do Valle. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 329)

[218] É recomendado ainda, no campo da segurança administrativa dos dados pessoais, o desenvolvimento de Políticas se Segurança de Informação. Estas políticas visam impedir o acesso às informações pertencentes à base de dados da empresa por parte de terceiros não autorizados e funcionam como um conjunto de diretrizes internas, um código de conduta a ser seguido pelos empregados e prestadores de serviços. Há ainda as medidas administrativas previstas no §2º do art. 50 da LGPD.

[219] SOUZA, Carlos Affonso; PADRÃO, Vinicius. **Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais.** São Paulo: Editora Revista dos Tribunais, 2019, p. 216.

[220] 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[221] 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. [...] § 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[222] Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o

Portanto, a LGPD se refere à ocorrência dos incidentes de segurança quando há "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento ilícito[223]". Cumpre mencionar que, em seu art. 13, o decreto 8.771/16, que regulamenta o Marco Civil da Internet, estabelece diretrizes de padrões de segurança[224]. Ademais, conforme ensinamento de Adriano Lima[225], no campo da Tecnologia da Informação, a definição de incidente de segurança abrange a ameaça à segurança e a proteção das operações do negócio.

Neste sentido, nos casos em que há a presença de incidente de segurança e este pode acarretar em risco ou dano relevante para os titulares dos dados tratados, ao tomar ciência do ocorrido, o controlador deve, além de comunicar o titular, comunicar a ANPD[226]. No entanto, o legislador limitou os tipos de incidentes que devem ser obrigatoriamente comunicados: aqueles que podem acarretar ao usuário risco ou dano relevante[227]. Para Marcus Claudio

---

seu término. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[223] 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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[224] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança :I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[225] LIMA, Adriano. **Gestão da segurança e infraestrutura de tecnologia da informação.** São Paulo: Editora Senac, 2018.

[226] "O dever de notificação impõe a obrigação de informar, não só à autoridade nacional, mas, também, ao titular dos dados pessoais violados. Nesse sentido, em razão da assimetria de informações e de modo a privilegiar a transparência, a comunicação com o titular deve ser feita em linguagem clara e direta, respeitando os padrões estabelecidos pela LGPD. As comunicações de incidentes aos titulares deverão conter a descrição da natureza da violação, o nome e o contato do encarregado, as possíveis consequências da violação e a descrição das medidas que foram ou que serão adotadas para mitigar os possíveis efeitos adversos do incidente". (SOUZA, Carlos Affonso; PADRÃO, Vinicius. **Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais.** São Paulo: Editora Revista dos Tribunais, 2019, p. 224)

[227] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

Acquaviva[228], o dano se refere a um "prejuízo sofrido pelo patrimônio econômico ou moral de alguém". Ao definir o risco, Maria Helena Diniz estabelece três pontos essenciais à sua caracterização:

> 1. Possibilidade da ocorrência de um perigo ou sinistro causador de dano ou se prejuízo, suscetível a acarretar responsabilidade civil na sua reparação.
> 2. Medida de danos ou prejuízos potenciais, expressa em termos de probabilidades estatística de ocorrência e de intensidade ou grandeza das consequências previsíveis.
> 3. Relação existente entre a probabilidade de que uma ameaça de evento adverso ou acidente determinados, se concretize com o grau de vulnerabilidade do sistema receptor e seus efeitos[229].

Ao tomar ciência do incidente de segurança, o controlador deve comunicar a ANPD em prazo razoável a ser determinado pela Autoridade. No que pese o não estabelecimento de prazo específico pela LGPD, a notificação deve observar alguns padrões mínimos estipulados pelo §1º do art. 48. Portanto, ao comunicar à ANPD, o controlador tem o dever de mencionar algumas informações relacionadas ao incidente, dentre elas, a descrição da natureza dos dados[230], as informações sobre os titulares afetados, as medidas técnicas e de segurança que foram utilizadas e as que serão utilizadas para reverter ou mitigar os efeitos do prejuízo. O tempo gasto pelo controlador para investigar o ocorrido e verificar se de fato houve um incidente de segurança não será computado para fins de ciência e contagem de prazo. Destaque-se, ainda, que apesar do caput do art. 48 apenas se referir ao controlador, o operador, com base nos princípios da boa-fé e nas possíveis previsões contratuais neste sentido, possui a obrigação de comunicar a ocorrência do incidente ao controlador para que esse possa tomar as medidas cabíveis[231].

A verificação da gravidade do incidente pela Autoridade Nacional de Proteção de Dados é necessária para a adoção de medidas adequadas para reverter ou atenuar os efeitos do

---

[228] ACQUAVIVA, Marcus Claudio. **Dicionário jurídico brasileiro Acquaviva.** 9 ed. Rev., atual. e ampl. São Paulo: Editora Jurídica Brasileira, 1998, p. 421.

[229] DINIZ, Maria Helena. *Dicionário jurídico*. São Paulo: Saraiva, 1998. v.4. p. 215.

[230] No que se refere à importância do controlador comunicar informações detalhadas, à exemplo da natureza dos dados pessoais afetados, Camilla do Vale Jimene ensina: "Ao exigir a apresentação de tais informações pelo controlador, na medida em que emprega o verbo 'deverá', o legislador deixa claro que pretende obter um detalhamento do ocorrido, de modo que tenha subsídios que propiciem a avaliar o nível de gravidade do incidente e o quanto o agente estava preparado para proteger os dados. Compreender qual tipo de dado está envolvido no incidente e quem são os titulares envolvidos é essencial para poder mensurar a quais riscos estariam expostos e, via de consequência, quais seriam as medidas mais adequadas para reverter ou mitigar os prejuízos. Imaginemos um caso hipotético de vazamento de uma base de dados que continha números de cartões de crédito. Entender a natureza dos dados afetados (números de cartões de credito), ajuda a compreender os riscos relacionados (os titulares dos dados correm o perigo de serem vítima de fraudes) e quais as medidas seriam adequadas para reverter o risco (cancelamento dos cartões). (JIMENE, Camila do Valle. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 344)

[231] SOUZA, Carlos Affonso; PADRÃO, Vinicius. **Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais.** São Paulo: Editora Revista dos Tribunais, 2019, p. 223.

incidente. Além de não ser uma atividade mandatória, cabendo o livre discernimento da ANPD em aplicar a adoção destas medidas ou não, o rol previsto no §2º do art. 48 da LGPD (I- ampla divulgação do fato em meios de comunicação; e II- medidas para reverter ou mitigar os efeitos do incidente) não é taxativo. Para a análise da gravidade do incidente, será objeto de exame a comprovação de que as medidas utilizadas tornavam os dados indecifráveis para terceiros não autorizados, dentro do limite técnico da empresa que trata dados pessoais. Conforme explica Camilla do Vale Jimene[232], tudo indica que os meios adequados a que se refere o legislador no §2º são os métodos de criptografia.

3.2 DOS DIREITOS DOS TITULARES DE DADOS

De antemão, cumpre ressaltar que, a LGPD traz ao decorrer do seu texto inúmeros direitos aos titulares, inclusive através do estabelecimento de obrigações claras e específicas aos agentes de tratamento, tornando-se essencial a sua interpretação de forma sistemática. Já nos primeiros artigos da LGPD, são apresentados, entre outros, os direitos à liberdade; liberdade de expressão, informação, comunicação e opinião; inviolabilidade da intimidade, honra, imagem e autodeterminação informativa[233]. Os princípios previstos no art.6º da lei, por sua vez, estão diretamente ligados aos direitos dos titulares assegurados no art. 18. Neste sentido, a partir do art. 7º da LGPD, são evidenciados diversos direitos aos titulares de dados pessoais. A título de exemplo, tem-se o direito a revogação do consentimento nos casos em que o titular discorde das alterações referentes ao tratamento de dados (art. 8º, § 6º e 9º, § 2º) e o direito a não divulgação dos seus dados pessoais em pesquisas ou estudos sobre saúde pública (art. 13, §2º).

O cenário de massiva utilização de dados no dia-a-dia, cenário este nomeado por Frank Pasquale de *one way mirror*, onde os agentes de tratamento (governamentais e privados)

---

[232] JIMENE, Camila do Valle. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 347.

[233] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

sabem muito sobre os titulares de dados e os titulares nada sabe sobre eles[234], é uma das maiores preocupações da LGPD e diante disto, dedica inteiramente o seu Capítulo III para dispor sobre os direitos dos titulares de dados. Pode-se dizer que, um dos seus objetivos principais, em conjunto com a garantia de um direito à autodeterminação informativa efetiva, é o resgate da dignidade dos titulares. Já em seu primeiro artigo (art. 17) do Capítulo III, a Lei assegura a titularidade de dados a toda pessoa natural, se referindo, ainda, à garantia dos direitos fundamentais de liberdade, intimidade e privacidade. Cumpre ressaltar que, os direitos previstos no art. 18 serão exercidos "mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento[235]", de forma gratuita e em prazo a ser estabelecido pela ANPD[236].

Ao inserir a garantia de direitos previstos na Constituição Federal e vinculá-los à titularidade de dados, o legislador maximiza as garantias do titular de dados pessoais. Como já mencionado anteriormente, a correlação entre o direito da privacidade e a proteção de dados pessoais não significa que os problemas que decorrem da exploração de dados pessoais se limitam à violação do direito à privacidade[237]. Ainda, neste primeiro momento, tem-se que a pessoa jurídica não é titular de dados e, portanto, estes direitos não se aplicam a ela. Conforme explica Viviane Nóbrega Maldonado, a não proteção das pessoas jurídicas quanto aos dados corporativos decorre de um conjunto de razões históricas[238].

---

[234] PASQUALE, Frank. ***The black box society:*** *the secret algorithm's that control money and information.* Cambridge: Harvard University Press, 2015, p. 146.

[235] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[236] Art. 18. [...] § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[237] "Os problemas que decorrem da exploração de dados são muito mais extensos do que a mera violação da privacidade, especialmente se tal direito for compreendido sob a sua acepção clássica, ou seja, no sentido de intimidade e no direito de ser deixado só. Além da privacidade, há vários outros desdobramentos da personalidade que são colocados em risco pela economia movida a dados, como a própria individualidade e autonomia. Mai s do que isso, não é exagero afirmar que a própria democracia também passa a estar sob ameaça. (FRAZÃO, Ana. Lei Geral de Proteção de Dados Pessoais: direitos básicos dos titulares de dados pessoais. **Revista do Advogado nº 144,** AASP, 2019, p. 34)

[238] MALSONADO, Viviane Nóbrega. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 221.

No que pese o art. 18 apresentar nove direitos sob a titularidade dos indivíduos que tiverem os seus dados tratados, apenas o direito à portabilidade[239] é uma "inovação" no texto legal. Com a exceção deste direito, todos os outros oito já foram mencionados na LGPD, demonstrando que a estrutura do art. 18 é fundamentalmente sistematizadora. Neste sentido, muitos dos direitos se apresentam em uma zona de sobreposição, o que será evidente ao analisar cada um deles especificamente. Ao mesmo tempo, este artigo é fundamental para o entendimento acerca da impossibilidade do atendimento por parte dos agentes de todos os tipos de requisições feitas pelos titulares de dados. Não obstante, proporcionando uma maior segurança jurídica ao titular de dados, o §4º desse mesmo artigo reconhece a necessidade de o controlador processar as requisições feitas pelo titular, independentemente de ela ser despropositada ou ilegítima, sendo inadmissível ignorá-las.

Os direitos à confirmação da existência de tratamento e acesso aos dados fazem relação direta aos princípios do livre acesso (art. 6º, inciso IV), da qualidade dos dados (art. 6º, inciso V) e da transparência (art. 6º, inciso VI). O princípio da transparência também se faz presente na redação do art. 9º, que de forma implícita se refere à necessidade de o titular de dados ser informado acerca do início do processo de tratamento dos seus dados, mesmo que não tenha requerido essa informação ao controlador. Para garantir a efetividade destes direitos, o legislador prevê a necessidade tanto do controlador quanto do operador manterem registro de todas as operações de tratamento de dados pessoais que realizarem[240]. Enquanto o direito à confirmação da existência de tratamento se refere à mera possibilidade do indivíduo tomar conhecimento acerca da existência do tratamento dos seus dados pessoais, o direito ao acesso já pressupõe a existência desse conhecimento prévio[241].

---

[239] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[240] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[241] "1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar reclamação a uma

O titular de dados poderá também, exigir que os seus dados, quando incompletos, inexatos ou desatualizados, sejam corrigidos. Cumpre-se informar que, o direito à correção de dados é a versão brasileira do direito previsto no art. 16 do GDPR: o direito à retificação[242]. Diante do fato de que um mero erro referente à incompletude ou inexatidão de dados em determinada base poderá causar inúmeros dados ao titular desses dados, sendo essa uma preocupação do legislador e, portanto, tal garantia é reforçada com o princípio da qualidade dos dados (art. 6º, inciso V). Ainda, nos termos do §6 do art. 18 da LGPD, o responsável deverá informar aos agentes com os quais ele realizou o uso compartilhado dos dados acerca da requisição de correção feita pelo titular.

Em seu inciso IV, o art. 18 da LGPD traz três direitos de natureza diversa de forma conjunta ao estabelecer o direito de "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei". Neste sentido, a Lei se preocupa em definir cada um destes direitos, estando todos eles atrelados a um ponto em comum: a desconformidade com a LGPD. Em relação à anonimização, tem de ser levado em consideração que, no que pese ser um direito do titular, a Lei sempre se refere a tal instituto utilizando a expressão "sempre que possível", como pode se observar em seus artigos 7º, inciso IV; 11, inciso II, c; 13, *caput* e 16, inciso II. Portanto, o legislador demonstra a compreensão acerca do elevado grau de dificuldade operacional e técnica para o processo de anonimização e diante disso, se refere reiteradamente à "mera possibilidade". Viviane N. Maldonado[243], membro do Training Advisory Board da IAPP (International Association of Privacy Professionals), entende que, se para a hipótese de "estudos em saúde pública", por exemplo, o legislador não impõe a anonimizacao de dados ao controlador, por decorrência lógica, o direito do titular à anonimização de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, não é um direito absoluto, não sendo exigível a adoção do referido processo pelo controlador se esse se mostrar impossível.

---

autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados" (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[242] Art. 16. O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[243] MALDONADO, Viviane Nóbrega. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 225.

No que se refere ao bloqueio e eliminação de dados, tem-se que, enquanto o bloqueio se refere a uma suspensão temporária[244], a eliminação de dados se caracteriza como uma suspensão definitiva[245]. Neste ponto, aproximando-se ao direito de boqueio, o GDPR se refere ao direito à limitação do tratamento, o qual garante ao titular de dados à possibilidade de restringir o tratamento de dados em situações específicas previstas em seu art. 18[246]. Diferentemente, na legislação brasileira, o bloqueio está relacionado a uma das sanções administrativas inseridas no Capítulo VIII da referida lei[247]. Já o direito à eliminação de dados, se aproxima bastante do direito ao apagamento que era previsto na Diretiva Europeia 95/46. No entanto, o GDPR substituiu esse direito pelo direito ao esquecimento, previsto em seu art. 17 e que será objeto de análise posterior (3.1.4.2).

Aparecendo pela primeira vez no texto da LGPD, o direito à portabilidade dos dados demonstra a necessidade de regulamentação do cenário conhecido como *vendor lock-in,* onde os custos para a trocam de controlador é tão elevado que acaba compelindo o consumidor a permanecer vinculado a determinando ofertante, desmotivando a substituição. Trata-se de um direito que procura viabilizar um maior controle dos dados pessoais por parte do seu titular, reforçando a ideia da autodeterminação informativa. A portabilidade se refere unicamente às informações relativas ao próprio titular e, portanto, o titular, em posse de seus dados e do seu histórico, poderá exercer a livre opção na contratação de outros fornecedores. Ainda, o §7º do art. 18 esclarece que, o direito a portabilidade de dados não engloba os dados que já foram anonimizados pelo controlador. Para Ana Frazão, a previsão da portabilidade vai muito além

---

[244] Art. 5º Para os fins desta Lei, considera-se: [...] XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[245] Art. 5º [...] XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[246] Art. 18. 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações: a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; d) Se tiver oposto ao tratamento nos termos do artigo 21.o, n.o 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[247] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...] V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

de um direito do titular de dados, podendo influenciar positivamente no ingresso de novos entrantes ou *startups* no mercado, pois facilita a transferência de dados[248].

Assim como o inciso IV, o inciso VI, também conhecido como o direito ao esquecimento, se refere à eliminação de dados. O direito à eliminação possui relação direta com o término do tratamento de dados, pois esse artigo em específico diz respeito à eliminação de dados tratados de forma lícita e com o consentimento do titular, após o seu término. Ainda, prevê como exceção a sua aplicação as hipóteses previstas no art. 16 da LGPD, que se referem à conservação dos dados pelo controlador mesmo após o término do tratamento. Como exemplo, destaca-se a hipótese do inciso IV do artigo 16, que autoriza a manutenção dos dados pelo controlador desde que de forma anonimizada. Ou seja, o intuito da norma é garantir ao titular de dados que elimine os seus dados que estavam sob o controle de determinado agente de tratamento quando da retirada do consentimento.

Possui também o titular de dados o direito de receber informações acerca das entidades públicas e privadas com as quais o controlador realizou o compartilhamento das suas informações pessoais. A Lei permite o uso compartilhado de dados, conceituando-o em seu art. 5º, inciso XVI e, portanto, assegura ao titular de dados o fornecimento de informações das entidades com as quais o controlador original compartilhou os seus dados. Cumpre ressaltar que, nos casos em que a lei exige o consentimento para o tratamento de dados, o compartilhamento deste tem a sua legalidade atrelada ao consentimento expresso do titular para esse fim[249]. Possuindo relação direta com o princípio da transparência (art. 6º, inciso VI),

---

[248] "Além da proteção do titular de dados, o direito à portabilidade tem também importantes implicações concorrenciais, pois, partindo da premissa de que os dados são os mais importantes insumos da economia movida a dados – ou até mesmo *essential facilities* -, a portabilidade pode facilitar a transferência de dados para fins de ingresso de novos entrantes ou *startups* no mercado ou mesmo para estimular a competição entre rivais já existentes, evitando que o acumulo de dados por apenas um ou determinados *players* possa ser uma verdadeira barreira à entrada ou fator que comprometa a rivalidade com agentes menores." (FRAZÃO, Ana. Lei Geral de Proteção de Dados Pessoais: direitos básicos dos titulares de dados pessoais. **Revista do Advogado nº 144,** AASP, 2019, p. 41)

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

a intenção do legislador ao prever esse direito reforçou a importância de o titular ter pleno controle de seus dados pessoais.

Os últimos dois direitos previstos no art. 18 da LGPD estão intrinsicamente ligados à ideia do consentimento. O consentimento constitui uma das dez bases legais para o tratamento de dados pessoais, sendo definido no art. 5º, inciso XII da LGPD como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Uma interpretação conjunta dos incisos VIII e IX traz à tona o direito do consentimento livre e informado. Neste sentido, pressupondo que nem sempre haverá uma conduta ativa por parte do controlador em manter o titular informado, é assegurado ao titular dos dados à informação acerca da possibilidade de não fornecer o seu consentimento, como também, quais são as possíveis consequências que podem decorrer da negativa deste consentimento específico.

Por fim, é garantido ao titular a possibilidade de revogação do consentimento, nos termos do §5º do art. 8º da LGPD. A referência expressa ao §5º faz-se necessária para o esclarecimento de alguns pontos, dentre eles: a revogação a qualquer momento e o fornecimento de um procedimento gratuito e facilitado e a ratificação do tratamento de dados. Destarte, a revogação poderá ocorrer no instante seguinte ao fornecimento do consentimento e deve gerar como consequência imediata a cessação do tratamento de dados. Por óbvio, o controlador poderá continuar com o tratamento de dados sob outra base legal que não o consentimento do titular. Ainda, insta mencionar que, a revogação do consentimento não anula os efeitos dos atos praticados sob a égide do consentimento fornecido pelo titular de forma lícita e, diante disto, são ratificados os tratamentos realizados.

3.2.1 O direito à explicação na LGPD

Um possível direito à explicação decorre da crescente preocupação referente às decisões automatizadas[250]. Neste sentido, além dos direitos previstos no art. 18 da LGPD, o legislador

---

nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[250] FRAZÃO, Ana. O direito á explicação e à oposição diante de decisões totalmente automatizadas. **Revista JOTA.** 05 dez. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018#_ftn2>. Acesso em: 20 jun. 2020.

inseriu o direito do titular de dados, e, por conseguinte, pessoa natural, solicitar a revisão de decisões tomadas unicamente com base no tratamento automatizado de seus dados pessoais. O legislador exemplifica o que seriam essas decisões, como as decisões destinadas à definição de perfis pessoais, profissionais, de consumo, de crédito ou até mesmo os aspectos individuais de cada cidadão – aspectos da sua personalidade[251]. Para garantir a efetividade deste direito, sempre que solicitado, o controlador está obrigado a fornecer informações claras e adequadas a respeito da forma em que foi feito o tratamento automatizado, como critérios e procedimentos utilizados. No entanto, garante que sejam observados os segredos comerciais e industriais.

A garantia prevista no *caput* do art. 20 resulta dos inúmeros efeitos negativos que podem decorrer da crescente utilização de algoritmos para a realização de inferências e avaliações sobre os indivíduos, prognoses e avaliações, dentre outras atividades. Decisões automatizadas são caracterizadas, principalmente, pela sua opacidade e ausência de transparência e como se refere Ana Frazão[252] – verdadeiras *black boxes*. No entanto, o próprio §2º do art. 20 admite a hipótese do controlador não oferecer as informações solicitadas pelo titular de dados nos termos do §1º, apontando como consequência uma possível auditoria pela Autoridade Nacional de Proteção de Dados Pessoais para a verificação acerca da ocorrência de aspectos discriminatórios no tratamento de dados realizado de forma automatizada.

Neste sentido, percebe-se que, mesmo com a tentativa da LGPD de criar uma espécie de devido processo legal para proteger os titulares das diversos malefícios que podem decorrer do tratamento automatizado de seus dados pessoais, a própria Lei estabelece limites que dificultam a real efetividade desta garantia ao estabelecer a garantia de preservação de segredos comerciais e industriais. Diferentemente da LGPD, o GDPR, ao regular este mesmo tema em seu art. 22.2, além de estabelecer as hipóteses em que pode haver o tratamento automatizado, não se refere ao segredo comercial ou industrial.

Conclui-se que, a maior aproximação de um "direito a explicação" na LGPD está relacionada à garantia de revisão de dados tratados de forma automatizada. No entanto, a Lei proporciona

---

[251] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[252] FRAZÃO, Ana. O direito á explicação e à oposição diante de decisões totalmente automatizadas. **Revista JOTA.** 05 dez. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018#_ftn2>. Acesso em: 20 jun. 2020.

diversas ferramentas aos titulares que garantem o acesso e controle sobre os seus dados pessoais, não decorrendo apenas da autodeterminação informacional e do direito de acesso. Além do microssistema de garantias referentes às decisões automatizadas, a LGPD prevê 10 princípios que são extremamente relevantes para a garantia de que o titular possua meios para acompanhar o processo de tratamento dos seus dados. Neste ponto, destaca-se o princípio da transparência, possibilitando que o titular de dados requisite de órgãos públicos e privados informações acerca da utilização dos seus dados. Garantindo uma maior efetividade a este princípio, o legislador complementa-o através do art. 19 da LGPD ao determinar que "a confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular", de forma imediata e simplificada ou através de declaração completa indicando a origem dos dados, os critérios utilizados para efetuar o tratamento e a sua finalidade, a finalidade e a inexistência de registro. Tal declaração deve ser fornecida em até 15 dias, contados da data do requerimento do titular, possuindo o agente de tratamento o benefício de resguarda dos os segredos comerciais e industriais.

3.2.2 O direito ao esquecimento na LGPD

A problemática acerca da existência de um direito ao esquecimento no ordenamento jurídico brasileiro antecede a sanção da LGPD, havendo inclusive quem defenda a existência de tal direito no art. 7º, X, do Marco Civil da Internet por fazer menção expressa à exclusão de dados, mas sem estabelecer critérios para o seu exercício[253]. O direito ao esquecimento visa a limitação de certos aspectos da vida dos cidadãos ao passado. No entanto, a ausência de critérios sólidos na legislação, estabelecendo limites e o seu âmbito de aplicação, torna o entendimento acerca do que seria o direito ao esquecimento no Brasil extremamente incompleto, e, como consequência disso, tal instituto é aplicado de forma errônea pela jurisprudência e pela doutrina. Caio Cesar de Oliveira se refere à utilização de tal direito de forma deslocada e genérica em diversos casos, onde, ao invés de aplicar o direito ao esquecimento, poderiam ser invocados diversos outros direitos da personalidade, como exemplo dos direitos à imagem e à honra[254].

[253] LIMA, Cíntia Rosa Pereira. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. **Revista dos Tribunais,** vol. 946, 2014, p. 77-109.
[254] OLIVEIRA, Caio César de. **A Lei Geral de Proteção de Dados Pessoais e um 'direito ao esquecimento' no Brasil.** São Paulo: Editora Revista dos Tribunais, 2019, p. 135.

Neste ponto, cabe mencionar a notória decisão do Tribunal de Justiça da União Europeia no Caso Costeja (Costeja *vs* Google Espanha e Google Inc), que em 2014 decidiu pela desindexação do *link* no Google acerca de informações relativas à débitos previdenciários contraídos pelo Sr. Corteja Gonzalez. Este direito à desindexação, qual seja, a remoção de um *link* no provedor de busca, foi nomeado pelo Tribunal como direito ao esquecimento, sob o fundamento de que tais informações relativas ao Sr. Gonzalez, pelo próprio decorrer do tempo, não se mostravam mais relevantes. No que pese tal decisão ter sofrido diversas críticas, principalmente referentes ao fato de que a desindexação não garante o esquecimento do fato[255] e que um direito ao esquecimento utilizado sem limitações pode ser extremamente prejudicial para a história, tendo em vista o fato de memória coletiva, tal decisão deu notoriedade ao tema, que veio a repercutir no regulamento de proteção de dados da União Europeia.

Em seu art. 17, o GDPR faz menção expressa ao Direito ao Esquecimento como um direito do titular de dados de obter pelo agente responsável o apagamento de seus dados em tempo justificável. Este mesmo artigo estabelece as hipóteses de aplicação do referido direito, assim como os seus limites. A título de exemplo, o responsável pelo tratamento de dados estará obrigado a apagar os dados do titular que deixarem de ser necessários para a finalidade inicial ou quando foram tratados ilicitamente[256]. A respeito das exceções à aplicação do art. 17, o

[255] Neste ponto, Carlos Affonso Pereira de Sousa, professor da UERJ, explica o porquê do nome dado ao Direito ao Esquecimento não é adequado: "Existe um problema conceitual grave com o chamado direito ao esquecimento. Ele não é um direito nem gera o pretendido efeito do esquecimento. Afirmamos que o chamado direito ao esquecimento não é um direito por três motivos. De início, ele não encontra previsão no ordenamento jurídico brasileiro. Em segundo lugar, ele tem servido, na verdade, para dar nome a lesões a outros direitos fundamentais ou da personalidade, com a honra, privacidade e nome (...)". (SOUSA, Carlos Affonso Pereira de. Mau uso do direito ao esquecimento deve ficar no radar. **Revista Migalhas.** 10 maio. 2019. Disponível em: https://www.migalhas.com.br/quentes/300036/mau-uso-do-direito-ao-esquecimento-deve-ficar-no-radar-alerta-professor-carlos-affonso. Acesso em: 10 jun. 2020)

[256] Art. 17. 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do atigo 21.o, n.o 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.o, n.o 1. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

GDPR prevê o cumprimento de obrigações legais, para fins de investigação histórica e outros[257].

Não obstante a influência do GDPR na LGPD e do teor do enunciado 531[258] da VI Jornada de Direito Civil do Conselho da Justiça Federal, que por sua vez, expressa o entendimento de apenas uma parte da doutrina, o legislador brasileiro optou por não incluir o direito ao esquecimento na Lei Geral de Proteção de Dados. Mesmo assim, os tribunais brasileiros, destacando-se neste ponto o Superior Tribunal de Justiça, com quatro casos relevantes[259], têm se deparado com um suposto direito ao esquecimento. Pode-se dizer, no entanto, que em todos estes casos o direito ao esquecimento foi utilizado com fundamentos diversos[260], de forma descontextualizada e sem critérios, demonstrando a ausência de uniformidade e segurança jurídica e confirmando que o Brasil ainda não possui bases sólidas para confirmar a sua existência[261]. No Caso da Chacina de Candelária, por exemplo, o STJ reconheceu o direito ao esquecimento como "um direito de não ser lembrado contra a sua vontade", enquanto em outras decisões o mesmo termo é referido como o direito à correção cadastral, apagamento de fichas criminais ou até mesmo, proteção de dados pessoais.

A esse respeito, Luiz Fernando Marrey Moncau aponta que:

> [...] existe uma grande confusão conceitual em torno da ideia de um direito ao esquecimento. A ausência de uma definição clara implica em visões diferentes sobre

---

[257] "3. Os n.os 1 e 2 não se aplicam na medida em que o tratamento se revele necessário: a) Ao exercício da liberdade de expressão e de informação; b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado- -Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.o, n.o 2, alíneas h) e i), bem como do artigo 9.o, n.o 3; d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, na medida em que o direito referido no n.o 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial." (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[258] "A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento". (BRASIL. Conselho da Justiça Federal. **Enunciado 531.** Disponível em: https://www.cjf.jus.br/cjf/noticias/2013/abril/enunciado-trata-do-direito-ao-esquecimento-na-sociedade-da-informacao#:~:text=O%20Enunciado%20531%20diz%20que,%C3%A0%20dignidade%20da%20pessoa%20humana. Acesso em: 10 jun. 2020)

[259] São os casos: Chacina de Candelária (Recurso Especial 1.334.097/RJ); Aída Cury (Recurso Especial 1.335.153/RJ); Xuxa (Recurso Especial1.316.921/RJ) e DNP vs Google (Recurso Especial 1.660.168/RJ).

[260] "O termo 'direito ao esquecimento' vem sendo amplamente utilizado para tratar dos mais variados casos, como um gênero, em que determinado sujeito pleiteia a retirada, a desindexação ou não divulgação de fato ou informação especifica sobre si nos mais diversos meios de comunicação e provedores de aplicações de internet e pesquisa". (BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 1.010.606/RJ. Relator: Ministro Dias Toffoli. Recorrente: Nelson Curi. Recorrido: Globo Comunicação e Participações S/A. Disponível em: http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786. Acesso em: 10 jan. 2020)

[261] OLIVEIRA, Caio César de. **A Lei Geral de Proteção de Dados Pessoais e um 'direito ao esquecimento' no Brasil.** São Paulo: Editora Revista dos Tribunais, 2019, p. 146.

> o seu alcance,e scopo, sobre suas virtudes e problemas. Diante da multiplicidade dos fundamentos jurídicos utilizados para restringir a circulação de informação em nome de um direito ao esquecimento, seja no ambiente digital ou fora dele, não é raro observar analistas, jurisprudência e doutrina tratando rotulando as mais diversas possibilidades sob a mesma expressão[262].

Por conseguinte, por não possuir este tema o mesmo desenvolvimento e maturidade da Europa, o legislador agiu de forma correta ao não se referir expressamente a um "direito ao esquecimento", pois não deve o Brasil importar direitos estrangeiros sem uma verdadeira análise do cenário pátrio. Ainda, de acordo com Sergio Brando, o mau uso do "direito ao esquecimento", além de apresentar-se como um risco à liberdade de expressão, também pode possibilitar a reescrita da história e, por isso, deve ser usado de forma excepcional[263]. Diferentemente, o legislador brasileiro, ao invés de prever um conceito amplo e duvidoso, inseriu outros diversos direitos que serão efetivos para a real preocupação do titular, qual seja, o desejo por ser esquecido. Dentre garantias previstas no art. 18 da LGPD, que possibilitam tal tutela e as quais foram analisadas no tópico anterior a este, destacam-se: o direito à correção de dados eventualmente desatualizados ou incorretos, o direito à anonimizacao, a possibilidade de bloqueio e eliminação de dados tratados em desconformidade com a lei, a eliminação de dados desnecessários ou excessivos, dentre outros.

O direito à anonimizacao, por exemplo, possibilita a tutela de um desejo de ser esquecido, ao ponto em que, "dados anonimizados podem ser utilizados sem prejuízo a eventuais direitos da personalidade do titular de dados pessoais[264]". Partindo desta observação, notícias anonimizadas também podem ser publicadas sem causarem prejuízos aos titulares de dados, o que se pode observar no Caso Costeja narrado acima. Portanto, conclui-se que, apesar de tais ferramentas previstas na LGPD não serem sinônimas de um "direito ao esquecimento", estas preveem uma efetiva regulação, com limites e meios para se garantir que o titular de dados possua um maior controle de seus dados pessoais.

---

[262] MONCAU, Luiz Fernando Marrey. Direito ao esquecimento. São Paulo: Editora Thomson Reuters, 2018.

[263] "O direito ao esquecimento deve ser aplicado excepcionalmente diante dos riscos que representa à liberdade de expressão, à possibilidade de reescrita da historia e à defesa de interesses escusos, entre outros possíveis maus usos do instituto, apenas quando presentes, em conjunto, todos os seguintes critérios: violação à privacidade por meio de publicação de dado verídico, após lapso temporal, capaz de causar dano a seu titular, sem que haja interesse público, preservando-se em todo caso a liberdade de expressão e desde que não se trata de fato histórico, cuja demanda é direcionada, em última instância, ao Poder Judiciário, que deverá, se entender cabível, ordenar a sua remoção ao meio de comunicação onde a informação se encontra (e nunca ao motor de busca). (BRANCO, Sérgio. **Memória e esquecimento na internet.** Porto Alegre: Editora Arquipélago, 2017)

[264] OLIVEIRA, Caio César de. **A Lei Geral de Proteção de Dados Pessoais e um 'direito ao esquecimento' no Brasil.** São Paulo: Editora Revista dos Tribunais, 2019, p. 149.

3.3 AS BASES LEGAIS DE TRATAMENTO

A legalidade do tratamento está diretamente relacionada à necessidade de o controlador enquadrar a sua atividade em uma das dez bases legais reguladas pelo art. 7º da LGPD, as quais são taxativas. Apesar de haver a possibilidade de cumulação das bases legais, basta o atendimento de uma delas para legitimar o tratamento de dados. A dicotomia "público-privado" também se faz presente no tratamento de dados pessoais. As bases legais de tratamento de interesse privado são: o consentimento; o cumprimento de obrigação legal ou regulatória; a execução de contrato; o legítimo interesse; a proteção do crédito, a realização de estudos por órgão de pesquisa; o exercício regular de direitos em processos; a proteção da vida do titular e terceiros e a tutela da saúde. Já o Poder Público possui o seu campo de atuação limitado ao tratamento de dados para a execução de políticas públicas, ideia fortalecida pelo art. 23 da LGPD[265]. Cumpre mencionar que, não há hierarquia entre as bases legais, todas elas legitimam o tratamento, cabendo ao controlador definir a base legal apropriada no caso concreto de acordo com a finalidade do tratamento.

3.3.1 Do setor privado

As principais bases legais de tratamento que interessam as atividades empresariais são especificadas pelos incisos I, II V, IX e X do art.7º, nos seguintes termos:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do

[265] Art. 23: O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;II - (VETADO); e III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

> titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

O consentimento do titular de dados legitima o tratamento de dados e é o ponto focal deste trabalho, que será aprofundado ao decorrer do Capítulo 4. Apesar de ser apenas uma das dez hipóteses que legitimam o tratamento de dados pessoais, e, portanto, ser possível ocorrer o tratamento de dados sem o consentimento do titular desde que o a atividade exercida se enquadre em qualquer uma das outras nove hipóteses, o consentimento é considerado a principal base legal[266]. Conforme definição dada pelo art. 5º, inciso VII, o consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Destarte, a LGPD adotou como regra geral que legitima o tratamento de dados o consentimento inequívoco, com exceção das hipóteses de tratamento em situações "especiais", que demandam a necessidade do consentimento específico[267]. Via de regra, este instituto pode ser visualizado nas relações diretas entre o titular e os agentes de tratamento quando o titular aceita os termos de uso e política de privacidade nos *sites*, por exemplo. Porém, também é possível a utilização do consentimento como uma base legal de tratamento através da relação entre o titular e o controlador que trata os dados que foram compartilhados a ele pelo primeiro controlador, sendo este com quem o titular teve uma relação direta. Neste sentido, desde que o primeiro controlador obtenha o consentimento do titular para o compartilhamento dos dados, não haverá a necessidade do consentimento específico do titular para essa nova finalidade, podendo o segundo controlador utilizar o consentimento obtido pelo primeiro controlador como base legal, conforme prevê o §5º do art. 7º da LGPD[268]. Para Marcel Leonardi, diante dos múltiplos cenários de compartilhamento de dados, é praticamente inviável a obtenção do consentimento para todos os tratamentos futuros pelo primeiro

---

[266] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 179.

[267] Nos casos de tratamento de: dados pessoais sensíveis, de crianças, na transferência internacional de dados pessoais para países com nível inferior de proteção de dados pessoais e qunado há a participação de terceiros de forma indireta no tratamento de dados.

[268] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

controlador. Sendo assim, entende ser necessário que os demais controladores avaliem a possibilidade de utilização das outras bases legais para legitimar o seu tratamento[269].

Quando há determinação legal, seja por lei ou demais normas, o controlador possui legitimidade para realizar o tratamento de dados. O inciso II, no entanto, não abarca as obrigações assumidas contratualmente. Diante do fato de que as relações privadas não podem ser utilizadas como fundamento para o tratamento de dados pessoais, Caio C, Carvalho Lima se refere à relevância da precedência de uma efetiva validação acerca do cumprimento do contrato à luz da legislação vigente ao assinar os contratos[270]. Cumpre mencionar que, diante do fato de que o tratamento é legitimado diante da natureza das normas, ele estará limitado à finalidade destas normas[271].

Já a base legal trazida pelo inciso V, qual seja, quando necessário para a execução de contrato ou de procedimentos preliminares, possibilita o tratamento de dados fundamentado nas relações privadas. Ou seja, trata-se de hipótese na qual há a necessidade do tratamento de determinados dados pessoais para a execução das obrigações que foram contratualmente firmadas. No entanto, a legalidade deste tipo de tratamento está relacionada ao pedido do titular dos dados. Portanto, o tratamento fundado nesta base legal está sujeito ao cumprimento de dois requisitos cumulativos: a necessidade do tratamento para o cumprimento do contrato ou de procedimentos preliminares e a iniciativa de contratação do titular dos dados. Se um indivíduo efetua a compra de passagens aéreas em um site de agência de turismo, por exemplo, para que a agência preste o serviço solicitado pelo cliente, precisará compartilhar os dados do cliente com a companhia aérea. Para tanto, aplicando-se a ressalva da finalidade[272], tanto a empresa de turismo poderá utilizar como base legal de tratamento a execução de

---

[269] LEONARDI, Marcel. **Principais bases legais de tratamento de dados pessoais no setor privado.** São Paulo: Editora Revista dos Tribunais, 2019, p. 76.

[270] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 182-183.

[271] "Assim, por exemplo, para cumprir com suas obrigações de combate aos crimes de 'lavagem' de dinheiro, uma instituição financeira deverá realizar o tratamento de uma série de dados pessoais, tal como exigido pela Circular 3.461/2009 do Banco Central do Brasil. Esse tratamento, sob a vigência da Lei 13.709/2018, terá como base legal, justamente, o disposto no artigo 7º, inciso II, e é limitado a essa finalidade específica, sendo necessário recorrer a outra base legal caso se pretenda realizar o tratamento desses mesmos dados pessoais para outra finalidade". (LEONARDI, Marcel. **Principais bases legais de tratamento de dados pessoais no setor privado.** São Paulo: Editora Revista dos Tribunais, 2019, p. 77)

[272] "O tratamento realizado com apoio no artigo 7º, inciso V, é limitado a essa finalidade específica – execução de contrato ou de procedimentos preliminares – sendo necessário recorrer a outra base legal caso se pretenda realizar o tratamento desses mesmos dados pessoais para outras finalidades. (...) Não há, portanto, como justificar o tratamento de dados pessoais realizado para a execução de contrato ou de procedimentos preliminares relacionados ao contrato para finalidades distintas do objeto do contrato, pois, nessa hipótese, esse tratamento seria considerado incompatível com a finalidade original" (LEONARDI, Marcel. **Principais bases legais de tratamento de dados pessoais no setor privado.** São Paulo: Editora Revista dos Tribunais, 2019, p. 78)

contrato, como a companhia aérea ao efetuar o tratamento dos dados fornecidos pelo referido *website.*

Por não estar atrelado a uma finalidade específica, pode-se dizer que a base legal estabelecida no inciso IX do art. 7º é a mais flexível. Neste sentido, a LGPD autoriza o tratamento de dados pessoais quando "necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". No entanto, o legislador não prevê o que seria este legítimo interesse e diante disso, a utilização desta base legal representa um risco ao controlador, que por força do que dispõe o art. 10, §3º da LGPD, deve realizar um Relatório de Impacto à Proteção de Dados Pessoais. Além de o relatório estar sujeito à revisão pela ANPD, o controlador, antes da utilização do legitimo interesse como base legal para o tratamento de dados precisa efetuar um teste baseado em três etapas.

Primeiramente, deve identificar o interesse legítimo e se este é um interesse próprio ou de terceiros. Apesar do inciso IX do art. 7º se referir aos interesses legítimos do controlador ou de terceiro, o art. 10[273], que se dedica ao regular o tema mais detalhadamente, se refere apenas ao interesse legítimo do controlador, fazendo com que parte da doutrina entenda ter sido um equívoco do legislador a inclusão de terceiros como sujeitos legitimados a utilizar o legítimo interesse como base legal para o tratamento de dados pessoais. Diferentemente, na regulamentação europeia, tem prevalecido o entendimento da plena legalidade da utilização do interesse legítimo por terceiros[274]. Também, deve o controlador demonstrar a relação de

[273] Art. 10: O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.§ 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[274] "(47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratado com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do

necessidade entre o tratamento de dados e o alcance do interesse legítimo. E, por fim, realizar o teste de proporcionalidade para apresentar um real equilíbrio entre o legítimo interesse e as liberdades e direitos fundamentais do titular relacionados à proteção dos seus dados pessoais[275].

A última base legal de tratamento concernente ao setor privado se caracteriza como uma inovação trazida pela LGPD. As informações sobre inadimplência ou adimplência de determinado titular podem ser utilizadas para diversos fins, a exemplo da concessão ou não de crédito, e por isso, o legislador viu a necessidade de incluir essa base no rol taxativo do art. 7º, especificando, ainda, a importância de se observar a legislação pertinente[276]. No GDPR, por exemplo, o tratamento de dados pessoais para fins de proteção de crédito não constitui uma base legal específica. Caso o agente de tratamento necessite efetuar o tratamento para este fim, ele deve utilizar outra base legal, como o consentimento ou o cumprimento de uma obrigação legal para legitimar a sua operação. Apesar da LGPD não definir o conceito de proteção de crédito, deve ser feita uma interpretação extensiva deste conceito, abarcando as atividades de apoio, o oferecimento de serviços de crédito e também os procedimentos de concessão de crédito, pois eventual interpretação restritiva limitaria a aplicação desta base à finalidade de gerenciamento de risco de crédito[277].

As demais bases legais apresentadas ao longo do art. 7º da LGPD não são hierarquicamente inferiores a essas descritas acima e devem ser igualmente escolhidas pelos agentes quando forem as que mais se adequam a atividade de tratamento. Não faz sentido para órgãos de pesquisa, por exemplo, que utilizem o consentimento para o tratamento de dados com fins exclusivos de pesquisa. Não obstante, deve o órgão de pesquisa se enquadrar com a definição legal prevista pela própria LGPD em seu art. 5º, inciso XVIII[278] e, quando possível, dar preferência à utilização de dados anonimizados. Configurando-se como uma base de tratamento relacionada a questões mais graves, o inciso VII legitima o tratamento de dados pessoais para a proteção da vida ou incolumidade física do titular. A título de exemplo, em

---

responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional (...)". (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[275] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 184.

[276] Neste sentido, a legislação pertinente contempla a Lei do Cadastro Positivo

[277] LEONARDI, Marcel. **Principais bases legais de tratamento de dados pessoais no setor privado.** São Paulo: Editora Revista dos Tribunais, 2019, p. 84.

[278] Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

caso de acidentes aéreos e sequestros, a LGPD prevê como legal a obtenção de dados o via geolocalização na tentativa de localização dos indivíduos. A possibilidade de tratamento de dados para a tutela da saúde, hipótese prevista no inciso VIII do art. 7º, demonstra-se extremamente relevante para conter o avanço de pandemias, como o recente caso do COVID-19, ao ponto em que profissionais da aérea de saúde ou entidades sanitárias podem se valer desta base legal para o tratamento de dados.

3.3.2 Do setor público

A necessidade de ter o tratamento de dados pessoais ancorado em uma base legal também se aplica ao Poder Público e, visando uma maior segurança jurídica, a LGPD, ao definir os entes públicos submetidos à sua incidência, faz referência direta ao art. 1º, parágrafo único da Lei de Acesso à Informação[279]. No que pese as atividades de segurança, defesa nacional, atividades de investigação, segurança do Estado e atividades de repressão de infrações penais possuírem um regulamento jurídico próprio[280], as demais espécies de tratamento de dados realizadas por ente ou órgão público devem seguir a regra de adequação a uma base legal. Nada obstante o movimento por parte do Governo para retirar o Poder do campo de atuação da LGPD, a Administração Pública, ao longo dos anos, aderiu diversos meio tecnológicos visando a aproximação do governo com o cidadão,[281] estando entre um dos maiores meios de

[279] Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. (BRASIL. **Lei Federal nº 12.527,** de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 maio. 2020)

[280] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020_

[281] À título de exemplo, há aplicativos do INSS, FGTS, Bolsa Família. Há também aqueles que são utilizados par facilitar a vida do cidadão e retirar o costume do documento presencial, como o E-título, o Meu Imposto de Renda e a CNH Digital.

controle de dados no país[282]. Assim, o legislador se preocupou em regulamentar o tratamento de dados pelas pessoas jurídicas de direito púbico separadamente, no capítulo IV da LGPD[283], além de prever uma base legal específica no inciso III do art. 7º, nos seguintes termos:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

De forma geral, a relação jurídica entre o Poder Público e o titular de dados objeto do tratamento é caracterizado por uma maior assimetria de poder do que pelo setor privado devido a vários fatores, como os poderes garantidos à Administração Pública para a consecução de seus deveres e a grande quantidade de dados que detêm em seus bancos de dados[284]. Diante disso, a LGPD se preocupa em regular o tratamento de dados pessoais pelo poder público de forma clara e atualizada em nove artigos em seu capítulo IV (Tratamento de Dados Pessoais pelo Setor Público), legitimando o tratamento de dados pelo Poder Público que, desde que forneçam informações de forma clara, atualizada com fácil acesso aos cidadãos sobre a previsão legal, a finalidades, os procedimentos e as práticas que foram utilizados para a execução das atividades.

A atuação do Poder Público é excepcional e condicionada ao cumprimento da finalidade pública, sob a premissa de atendimento do interesse público. Celso Antonio Bandeira de Mello[285] define o interesse público como: "o interesse resultante do conjunto de interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da

---

[282] ROSSO, Angela Maria. LGPD e setor público: aspectos gerais e desafios. **Revista Migalhas.** Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios. Acesso em: 17 jun. 2020.

[283] "O tratamento de dados pessoais é um aspecto da execução das políticas públicas que mereceu da LGPD regulamentação específica decorrente do reconhecimento de que a massificação das relações travadas entre o Estado e os cidadãos, marcada pela voracidade na coleta de dados, tratados de forma não padronizada e, tampouco transparente, redunda no risco de o Estado violar direitos e garantias fundamentais do titular" (TASSO, Fernando Antonio. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019. p.246)

[284]Angela Maria Rosso explica um dos motivos dessa maior assimentria na relação entre o Poder Público e o titular de dados:"Dentre todos os concentradores de dados pessoais o Estado se sobressai, afinal de contas é ele que controla ainda que indiretamente a vida financeira, o acesso à saúde, eventuais processos judiciais colecionados durante a vida, dados educacionais, dados trabalhistas do cidadão entre outros. Além disso, o Estado é também um empregador gigante, são milhares de pessoas que vendem sua força de trabalho para os entes municipais, estaduais e federais da Administração Direta e Indireta. Mais do que isso, o governo é também o maior acionista de grandes empresas de tecnologia que a pedido dele operam com esses dados: os coletam, armazenam, utilizam, etc. Ou seja, deixar o setor público fora do alcance da LGPD seria um verdadeiro atentado aos direitos fundamentais". (ROSSO, Angela Maria. LGPD e setor público: aspectos gerais e desafios. **Revista Migalhas.** Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios. Acesso em: 17 jun. 2020)

[285] BANDEIRA DE MELLO, Celso Antonio. **Curso de Direito Administrativo.** 33 ed. São Paulo: Editora Malheiros, 2016. p. 62.

sociedade e pelo simples fato de o serem". Neste sentido, o tratamento de dados pessoais pelo Poder Público deve ser realizado exclusivamente para o atendimento da sua finalidade pública, na persecução do interesse púbico e pra cumprir com as suas competências e atribuições legais. Essa última obrigação prevista para legitimar o tratamento de dados pelo setor público (competências e atribuições legais) possui reação direta com a sua própria "razão de ser", pois o poder público existe para cumprir uma função legal e por isso, é investido de diversos poderes[286].

Os artigos, 25, 26 e 27 da LGPD, por sua vez, se preocupam em regulamentar as hipóteses em que pode ocorrer o compartilhamento de dados pessoais administrados pelo setor público. Ao descrever como e quando podem ser compartilhados estes dados pessoais, a Lei se refere a algumas peculiaridades, como a necessidade de serem mantidos em formato interoperável e estruturados para o uso compartilhado quando forem utilizados para a execução de políticas públicas, à prestação de serviços públicos, a disseminação e ao acesso das informações pelo público em geral e a descentralização da atividade pública. Conforme definição de Maria Sylvia Zanella di Pietro[287], a descentralização da atividade pública ocorre quando o Poder Público distribui as atividades de sua competência para outra pessoa, independentemente de ela ser pessoa física ou jurídica.

Neste sentido, a descentralização se caracteriza como uma exceção à regra geral do art. 26, da LGPD. Em regra, é vedado expressamente o uso compartilhado de dados pessoais que estão sob a posse da Administração Pública com entidades privadas. No entanto, a transferência é legítima quando for necessária diante do fim determinado para a execução descentralizada da atividade pública. O instituto do consentimento se faz presente na redação do art. 27, ao determinar como regra para a comunicação ou uso compartilhado de dados o consentimento do titular de dados. Como exceção, o próprio artigo se refere à exceção trazida pelo art. 26, assim como às hipóteses de dispensa do consentimento previstas em lei (como bases legais de tratamento) e quando os dados forem tornados manifestamente públicos pelo titular[288].

---

[286] TASSO, Fernando Antonio. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019. p. 252.

[287] DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo.** Rio de Janeiro: Editora Forense, 2018.

[288] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

3.3.3 Tratamento de dados sensíveis de crianças e adolescentes

Os diferentes efeitos e consequências do processo de tratamento de diferentes tipos de dados deu ensejo à criação de uma categoria específica de dados pessoais: os dados pessoais sensíveis. As informações que são expostas nesta espécie de dado, quando conhecidas e submetidas a tratamento, oferecem um conteúdo que poderá ser utilizado de forma discriminatória no futuro[289], pois revelam características vulneráveis dos indivíduos, como a sua orientação política ou religiosa, opção sexual, dados genéticos ou o seu estado de saúde[290]. Do próprio conceito de dados sensíveis nos termos do art. 5º, I, da LGPD[291], percebe-se que a circulação destas informações apresentaria um potencial utilização lesiva e discriminatória aos seus titulares. Sendo assim, o legislador se preocupou, diante da natureza "especial" do dado coletado, em criar um regramento específico para os dados pessoais sensíveis.

De início, cumpre mencionar que, apesar do tratamento de dados pessoais sensíveis apresentar um risco maior em relação à proteção de dados, assim como no tratamento de dados pessoais, não se limita à base legal do consentimento. Aqui, o legislador optou em legitimar o tratamento de dados pessoais sensíveis em oito hipóteses, conforme prevê o art.11 da LGPD. Mesmo diante da diferença conceitual entre dados pessoais e dados pessoais sensíveis, as referidas hipóteses são bastante semelhantes às bases legais previstas no art. 7º da LGPD. Tal semelhança pode ser observada diante da redação idêntica de quatro das oito bases legais para o tratamento de dados pessoais sensíveis – a alínea 'a' do inciso II (art. 11) repete a redação do inciso II (art. 7º); a alínea 'c' do inciso II (art. 11) repete a redação do inciso IV (art. 7º); a alínea 'd' do inciso II (art. 11) repete a redação do inciso VI (art. 7º); a alínea 'e' do inciso II (art. 11) repete a redação do inciso VII (art. 7º) e a alínea 'f' do inciso II (art. 11) repete a redação do inciso VIIII (art. 7º). Como o art. 7º já foi analisado no Capítulo XX, será feita a análise das hipóteses legais previstas exclusivamente no art. 11 da lei.

Diferentemente do art. 7º, que regula cada uma das bases legais separadamente em incisos, o art. 11 divide a sua redação em apenas dois incisos. Seguindo a mesma linha de raciocínio

---

[289] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 142.
[290] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 84.
[291] Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

utilizada no art. 7º, o legislador legitimou o tratamento de dados pessoais sensíveis para além do consentimento, posicionando tais hipóteses no segundo e último inciso do art. 11 da LGPD. De início, prevê que a legalidade do tratamento de dados sensíveis com fundamento em outras bases legais, além do consentimento, está diretamente relacionada à indispensabilidade do tratamento para atingir a finalidade desejada. Como já anteriormente referenciado, dentre as sete alíneas do inciso II, cinco possuem a idêntica redação de incisos do art. 7º - cumprimento de obrigação legal ou regulatória pelo controlador, exercício regular de direitos, realização de estudos por órgãos de pesquisa, proteção da vida ou da incolumidade física do titular ou de terceiros e a tutela da saúde. Neste sentido, há apenas duas legais para o tratamento de dados pessoais sensíveis que independem do consentimento do titular e que não possuem a mesma redação do tratamento de dados pessoais, estruturadas nas alíneas 'b' e 'g' do inciso II, nos seguintes termos:

> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

A alínea 'b' alude que os entes da administração poderão se valer de dados sensíveis nas situações que se qualificam como indispensáveis para a execução de políticas públicas, estando sujeitos a dar publicidade à dispensa do consentimento, nos termos do inciso I do *caput* do art. 23 da LGPD. Observa-se que, a redação desta alínea é mais restritiva do que o inciso III do art. 7º[292], que também legitima o tratamento de dados pela administração pública, ao ponto em que contratos, convênios e instrumentos congêneres não serão aptos a legitimar o tratamento de dados pessoais sensíveis. Portanto, apenas o tratamento desta espécie de dados pelo setor público se limita à execução de políticas púbicas previstas em leis ou regulamentos.

No que pese a alínea 'c' repetir a redação do disposto no art. 7º, IV, é de entendimento geral que deve haver um maior esforço por parte dos órgãos de pesquisa para garantir que os dados pessoais sensíveis sejam anonimizados para a realização de estudos. Independentemente da finalidade se relacionar a estudos por órgãos de pesquisa, tal fator não exime do

[292] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

acontecimento de danos ao titular de dados, pois os riscos já relatados também se aplicam neste caso. Ainda, visando à prevenção de fraude e a garantia da segurança dos titulares de dados no processo de identificação e autenticação de cadastro em sistemas eletrônicos, o legislador legitima o tratamento de dados pessoais sensíveis para este fim. Dentre as possíveis situações, que necessariamente estão diante do uso de sistemas eletrônicos, destaca-se o tratamento de dados para garantir a efetivação ou confirmação de transações bancárias e para combater fraude em processos de identificação[293].

Por fim, cumpre observar que, as disposições do art. 11 se aplicam amplamente, ou seja, a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis[294], estando a sua não aplicação atrelada à existência de disposição em contrário em legislação específica. Ainda, a própria lei já prevê a possibilidade de regulação futura pela ANPD referente ao compartilhamento de dados pessoais sensíveis entre controladores com o objetivo de obter vantagem econômica, que poderá inclusive, ser vedada por tal autoridade após serem ouvidos os órgãos setoriais do Poder Público diretamente impactados[295]. Fora esta hipótese, é vedado o compartilhamento de dados pessoais sensíveis referentes à saúde visando a obtenção de vantagem econômica, exceto nas hipóteses de portabilidade de dados, desde que consentido pelo titular de dados ou quando necessário para a prestação de serviços de saúde suplementar de forma adequada[296].

---

[293] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 199.

[294] "Como exemplo, temos a situação de que determinada companhia que realiza o transporte privado de passageiros passa a aplicar inteligência em sua massa de dados, com o objetivo de identificar a religião, preferência políticas ou sexuais dos seus consumidores, a partir da confirmação dos endereços de início ou término das corridas." (
LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 200)

[295] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[296] Art. 11. [...] § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: [...] II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

Reconhecendo a hipervulnerabilidade das crianças[297] e a vulnerabilidade dos adolescentes, a LGPD também dispõe de forma específica acerca do tratamento dos seus dados pessoais em seu artigo 14. De início, informa a necessidade dos agentes de tratamento, no processo de tratamento de dados, agirem com o melhor interesse possível, levando-se em conta os termos do próprio art. 11 e, principalmente, as normas protetivas previstas na Constituição Federal, na Lei 8.069/1990 (Estatuto da Criança e do Adolescente)[298] e na Convenção sobre os Direitos da Criança. Criança, conforme definição dada pelo Estatuto da Criança e do Adolescente é a pessoa com até doze anos incompletos. Adolescente, para fins desta mesma lei, é aquele entre doze e dezoito anos incompletos. Há também a necessidade de adequação das ações direcionadas ao cumprimento dos deveres de informação de transparência no tratamento de dados pessoais de crianças e adolescentes, tendo em vista a capacidade peculiar de compreensão destes titulares, que se encontram em fase de desenvolvimento[299].

No que se refere às crianças, o tratamento de seus dados pessoais está atrelado ao consentimento específico[300] e destacado[301] de pelo menos um dos pais ou pelo responsável

---

[297] "No caso da criança, a vulnerabilidade é um estado a priori, considerando que vulnerabilidade é justamente o estado daquele que pode ter um ponto fraco, que pode ser 'ferido' (vulnerare) ou é vítima facilmente. [...] Estudos recentes demonstram a importância de crianças e adolescentes na definição dos hábitos de consumo dos adultos, tanto em relação a produtos de interesse do menor, quanto da própria família. Esse 'poder' da criança e do adolescente nas decisões de compra familiar, por sua vez, contrasta com a vulnerabilidade que apresentam em relação à atuação negocial dos fornecedores no mercado, por intermédio das técnicas de marketing. Neste sentido, se os apelos de marketing são sedutores aos consumidores em geral, com maior intensidade presume-se que sejam em relação às crianças e adolescentes. Estes se encontram em estágio da vida em que não apenas permite que se deixem convencer com maior facilidade, em razão de uma formação intelectual incompleta, como também não possuem, em geral, o controle sobre aspectos práticos da contratação, como os valores financeiros envolvidos, os riscos e benefícios do negócio. Daí resulta que estejam em posição de maior debilidade com relação à vulnerabilidade que se reconhece a um consumidor *standard*. Esta vulnerabilidade agravada da criança é reconhecida no âmbito da publicidade, sendo que o próprio CDC estabelece o caráter abusivo da publicidade que venha a aproveitar-se da deficiência de julgamento da criança (art. 37, §2º)." (MIRAGEM, Bruno. **Curso de direito do consumidor.** 6 ed. Rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2006. p. 131-132)

[298] Art. 70. É dever de todos prevenir a ocorrência de ameaça ou violação dos direitos da criança e do adolescente. [...] Art. 71. A criança e ao adolescente têm direito a informação, cultura, lazer, esportes, diversões, espetáculos e produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento. (BRASIL. **Lei nº 8.069,** de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF. 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 08 jun. 2020)

[299] TEFFÉ, Chiara Spadaccini de. **Tratamento de dados pessoais de crianças e adolescentes: proteção e consentimento.** São Paulo: Editora Revista dos Tribunais, 2019, p. 115.

[300] "[...] antes da coleta dos dados, no contrato, na política de privacidade ou em outro documento relacionado, houver detalhamento sobre o ciclo de vida do tratamento dos dados pessoais, com referência objetiva e clara sobre todos os limites e as finalidades em relação aos quais os dados serão tratados, inclusive sendo granular, cabendo ao usuário a seleção sobre o tratamento que deseja efetivamente autorizar. O conceito de 'específico', pois, engloba, de certa forma, os consentimentos informado e livre, não sendo suficiente obter o consentimento do titular como uma 'carta em branco' (diante da obrigatoriedade de extenso detalhamento dessa operação) e sem dar ao titular o poder de escolha efetiva sobre o tratamento dos seus dados". (LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 209)

legal (art. 14, §1º). Cumpre observar que, sempre que a lei mencionar a necessidade do consentimento para a legitimidade do tratamento de dados pessoais, além das especificidades de cada artigo, trata-se do consentimento na forma do art. 5º, XII, qual seja: livre, informado, inequívoco e para a finalidade previamente acertada. Como absolutamente incapaz, nos termos do Código Civil[302], a sua representação é obrigatória, sob pena de nulidade absoluta do ato praticado. A garantia de que este consentimento foi dado pelo responsável da criança é, sem dúvidas, um grande desafio para os controladores. Neste sentido, Chiara Spadaccini de Teffé indica que, assim como o GDPR, que regula sobre o tratamento de dados pessoais de crianças em seu artigo 8º, a questão do consentimento do responsável pela criança na LGPD é motivo de muitos questionamentos na doutrina:

> Pondera a doutrina que se, por um lado, o controlador não pode tratar dados antes do consentimento, por outro, precisará de tais dados para contatar o responsável legal pela criança. Afirma-se que os controladores deverão estar atentos e passar a exigir a data de nascimento do usuário, a fim de apurar a sua verdadeira idade, para, se for o caso, suspender o tratamento de seus dados até a obtenção do consentimento do responsável. (...) Por exemplo, como as empresas verificarão se a pessoa que forneceu o consentimento é realmente um dos responsáveis? Não está claro na lei em que se constituirá, o 'esforço razoável' por parte do controlador e quem avaliará a tecnologia implementada e o esforço desempenhado por ele. Certamente, algumas empresas, pelo porte e pelo poderio econômico, estarão em posição muito melhor para investir nas medidas necessárias. Outros desafios a se cogitar são as chances de as medidas de implementação ocasionarem maior processamento de dados pessoais, em contrariedade ao princípio da minimização dos dados; além do risco de que crianças desenvolvam estratégias para contornarem a regra relativa ao consentimento parental. Questiona-se, ainda, qual seria a extensão dos espaços de liberdade na Internet a serem assegurados às crianças sem a interferência de seus pais[303].

Na hipótese de tratamento do §1º, os controladores precisam dar publicidade aos seus atos, compartilhando informações sobre os tipos de dados coletados, bem como a sua forma de utilização e os procedimentos que garantem o exercício dos direitos dos titulares indicados pelo art. 18 da LGPD. Como exceção do consentimento a que se refere o §1º, a Lei indica no §3º do art. 14 a possibilidade de coleta de dados pessoais de crianças em apenas duas hipóteses: quando a coleta for necessária para contatar os pais ou responsável legal ou quando for fundamental para proteger a criança. Demonstrando prestígio aos princípios da

---

[301] [...] for clara a identificação do usuário em relação ao tratamento que será realizado com seus dados pessoais. Isso é especialmente relevante quando o consentimento estiver contemplado dentro de documento que contemple outras autorizações, situações em que o trecho relacionado ao tratamento de dados pessoais deve ser realçado, em relação às demais partes do texto, do vídeo ou do áudio". (LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 209)

[302] Art. 3º São absolutamente incapazes de exercer pessoalmente os atos da vida civil os menores de 16 (dezesseis) anos. (BRASIL. **Lei nº 10.406,** de 10 de janeiro de 2002. Institui o Código Civil. 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 20 jun. 2020)

[303] TEFFÉ, Chiara Spadaccini de. **Tratamento de dados pessoais de crianças e adolescentes: proteção e consentimento.** São Paulo: Editora Revista dos Tribunais, 2019, p. 114.

necessidade, finalidade e adequação, o §4º do art. 14 demonstra ser necessário observar a ideia de minimização dos dados pessoais de crianças. Portanto, os controladores não devem condicionar a partição de crianças em jogos, aplicações de internet e outras atividades de fornecimento de informações pessoais além das estritamente necessárias à atividade, sendo o desrespeito a tal previsão, mesmo na presença do consentimento do responsável, considerado abusivo. Também, devem os controladores realizar todos os esforços razoáveis para verificar que o referido consentimento foi de fato dado pelo responsável da criança, sendo consideradas as tecnologias disponíveis (art. 14, §5º).

Ao não tratar do tema em relação aos dados pessoais de adolescentes, o legislador abre espaço para diversas opiniões divergentes na doutrina. De forma geral e predominante, entende-se que o tratamento de dados pessoais de adolescentes não está sujeito às restrições previstas no §1º do art. 14. Portanto, prevalece o entendimento acerca da legitimidade do tratamento de dados atrelado à obtenção do consentimento ordinário dos adolescentes. Corroborando com tal entendimento, o Relatório da Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei 4.060/2012[304] declara existir uma exigência mais elevada de consentimento no tratamento de dados pessoais de crianças, quando comparado com o tratamento de dados pessoais de adolescentes. Ainda, referente ao tratamento de dados pessoais de adolescentes, para Caio C. Carvalho de Lima[305], apesar do §4º não mencionar expressamente a sua aplicação para o tratamento dos referidos tipos de dados pessoais, deve-se entender pela sua aplicação, diante do fato de que a garantia prevista em tal artigo trata-se de uma extensão de princípios que possuem ampla aplicação (finalidade, necessidade e adequação).

[304] "Ademais, responsáveis que lidem com dados de crianças e adolescentes deverão manter pública informação sobre os tipos de dados coletados, como estes são utilizados e os procedimentos para o exercício dos direitos dos titulares". (BRASIL. Câmara dos Deputados. Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei nº 4060, de 2012 [Tratamento de Dados Pessoais]. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=. Acesso em: 10 jun. 2020)

[305] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 210.

4 O INSTITUTO DO CONSENTIMENTO E A PROTEÇÃO DE DADOS PESSOAIS

Apesar da licitude do tratamento de dados na LGPD não estar relacionado exclusivamente ao ato exclusivo de vontade do titular, diante das demais bases legais já analisadas no Capítulo 3 deste Trabalho, entende-se o consentimento como a mais importante delas. Corroborando diretamente com o direito à autodeterminação informativa, o consentimento funciona como, no termo utilizado por Laura Schertel Mendes[306], uma "mola propulsora" da estrutura de proteção de dados pessoais e desta forma, por constituir um conjunto de autorizações e proibições, atua como instrumento regulador da atividade dos agentes de tratamento em diversos aspectos que serão abordados ao decorrer deste Capítulo. Nas palavras de Giorgio Resta, "quem consente não exprime propriamente a ausência de interesse na proteção [de seus dados pessoais], nem a ela renuncia, porém lança mão de um verdadeiro ato de exercício do direito da autodeterminação na esfera das escolhas pessoais[307]".

Ao ponto em que atua como forma de implementação do direito à autodeterminação informacional[308], o consentimento faz com que os titulares não sejam meros fornecedores de dados pessoais, passando a atuar de forma ativa em todo o processo de tratamento de dados pessoais. Neste sentido, ao mesmo tempo em que se apresenta como mecanismo para o exercício da autodeterminação, legitima o tratamento de dados pessoais. Essa dupla funcionalidade do consentimento acaba gerando uma divergência na doutrina no que se refere à sua natureza, tema que será abordado mais a frente (tópico 4.2). A título de exemplo, ambas as funcionalidades do consentimento podem ser vistas em uma simples situação comum do dia a dia: compras online. Ao realizar a compra de um sapato, a realização de tal negócio jurídico está atrelada à concordância do indivíduo tanto com os termos de uso, quanto com a política de privacidade de determinada loja. Neste sentido, o consentimento, ao mesmo tempo em que é utilizado como um instrumento para que o indivíduo exerça a sua autonomia de vontade, irá implicar na legitimidade da referida loja em tratar os seus dados pessoais, seja

---

[306] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 71.

[307] RESTA, Giordio. *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali.* ***Rivista Critica del Diritto Privato***, 2000, p. 307.

[308] "Para que o indivíduo possa exercer o seu papel de autodeterminação informativa, faz-se necessário um instituto jurídico por meio do qual se expresse a sua vontade de autorizar ou não o processamento de dados pessoais: o consentimento. Este é o mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão" (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 60)

para a customização de propagandas, conteúdos, análise de dados comportamentais, dentre outras diversas possibilidades que variam de caso a caso.

Devem, ainda, serem destacados dois aspectos essenciais de tal instituto para uma real ponderação das suas características: a sua qualidade de acessoriedade e da sua aparente inofensividade. Ao ponto em que está sempre ligado a uma situação específica para fundamentá-lo, o consentimento se apresenta como um elemento acessório, característica que pode ser claramente visualizada em situações corriqueiras do dia comum, como na realização de um contrato de adesão (termo de uso de sites) e na inscrição de um curso online, por exemplo. Percebe-se, que, muitas das vezes, sequer é dado ao titular a opção de não fornecer as suas informações, sendo esta única alternativa para a utilização dos serviços ofertados. O segundo atributo está diretamente ligado à conexão feita por Jeffrey Rosen entre a atividade de fornecer informações pessoais a sites na internet ao que Georg Simmel chama de "fenômeno do estranho". O autor se refere à presença da ideia de uma maior facilidade de as pessoas revelarem informações confidenciais a estranhos, justamente pela consequente ausência de julgamento por parte de desconhecidos e pessoas não intimas, induzindo a uma falsa segurança neste aspecto e no ato de consentir às operações de tratamento de dados[309].

Conforme define a LGPD em seu art. 5º, inciso XII, o consentimento se caracteriza como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". O que intende o legislador, ao relacionar a validade do consentimento com tais adjetivações é garantir que o usuário utilize de tal mecanismo para fazer escolhas conscientes, racionais e autônomas acerca do tratamento de seus dados pessoais. Portanto, a utilização do consentimento como instrumento para a tutela dos dados pessoais, diante do seu caráter personalíssimo, deve ser observada a partir dos seus efeitos em casos concretos.

4.1 A TRAJETÓRIA NORMATIVA DO CONSENTIMENTO NAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS

Para o entendimento acerca do papel de protagonismo do consentimento na LGPD, anterior a analise análise das leis esparsas que também regulam o referido tema no ordenamento jurídico

[309] "There is no reason for most of us to fear the disclosure of disaggregated bits of personal information to faceless Web sites, because those Web sites, by and large, have no motive or opportunity to collect the data into a personal narrative that could be disclosed to anyone who actually know us". (ROSEN, Jeffrey. ***The unawanted gaze.*** New York: Random House, 2000. p. 198)

brasileiro, é essencial o entendimento do que a doutrina nomeia de "gerações" de leis de proteção de dados, pois atuaram de maneira fundamental para o atual papel de protagonismo do titular de dados por meio do consentimento[310]. Neste processo de elevação do consentimento do titular de dados que se iniciou a partir da segunda geração de leis, a estratégia de proteção de dados utilizada possuía relação direta com o papel ativo do titular de dados no processo, e assim, nele foi depositado o dever de proteger as suas informações pessoais. Passou a se utilizar a técnica do consentimento do titular de dados para legitimar a coleta, utilização, compartilhamento, processamento, dentre todas as outras etapas de tratamento de dados[311]. Sendo assim, cabe à análise das gerações anteriores para a compreensão acerca da solidificação de tal instituto ao decorrer da história.

Juntamente com a Lei do Land de Hesse de 1970, a lei nacional de proteção de dados pessoais da Suécia, conhecida como *Datalog*, compõe parte das leis de primeira geração de proteção de dados pessoais. Na República Federal da Alemanha, ainda no ano de 1997, já havia uma cultura de proteção de dados, onde os estados (*Landers)* possuíam liberdade administrativa e normativa para a criação de medidas para a proteção de tal instituto. Em 1970 foi criada a Lei do Land de Hesse, tornando-se pioneira na normatização desta matéria ao estabelecer uma autoridade para a proteção de dados pessoais (*Datenschutzbeauf-trager*), que tinha como objetivo o controle da utilização de dados dos cidadãos pela administração pública[312]

Igualmente à autoridade criada para a proteção dos dados da sociedade alemã, a *Datalog* de 11 de maio de 1973 criou o *Dataispektionen* – instituto inspetor e regulador do uso de dados pessoais. A referida lei nacional sueca foi resultado de estudos de alto nível efetuados pelo Estado Sueco desde 1963, que propunha a implementação de um número de identificação único para os cidadãos através da ligação dos bancos de dados com o registro civil das imobiliárias, de veículos e empregatícios. Acontece que, assim como na Alemanha, a sociedade sueca não recepcionou a ideia de um Registro Total da População, causando reação contrária e impulsionando a promulgação da primeira lei mundial de proteção de dados pessoais[313].

---

[310] "A principal diferença em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, armazenamento e a transmissão e não apenas como a opção entre tudo ou nada" (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 42)

[311] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 129.

[312] FROSINI, Vittorio. ***Contributi ad um diritto dell'informazione.*** Napoli: Liguiro, 1991, p. 191.

[313] BENNETT, Colin. ***Regulating Privacy*****.** Ithaca: Cornell University Press, 1992, p. 47.

Da análise de ambos os casos, percebe-se que, o núcleo dessas primeiras leis regulatórias de dados pessoais era um possível controle pelos órgãos públicos através da concessão para a criação de centros de tratamento pelo Estado e pelas suas estruturas administrativas. Sobre as leis de primeira geração de dados pessoais, Danilo Doneda[314] entende que:

> Estas leis de proteção de dados de primeira geração não demoraram muito a se tornarem ultrapassadas, diante da multiplicação dos centros de processamento de dados, que tornou virtualmente difícil propor um controle baseado em um regime de autorização, rígido e detalhado, que demandava um minucioso acompanhamento. Suas normas, que estabeleciam em minúcias alguns aspectos de funcionamento dos bancos de dados, não poderiam acompanhar a explosão do número destes, além do que o paradigma de alguns grandes centros computacionais estava destinado a mudar.

Posteriormente, na segunda metade da década de 70, ultrapassada a preocupação baseada no controle dos dados pessoais diante do constante crescimento dos centros de processamento de dados, surgem as leis de segunda geração. Essa geração de leis se preocupou em garantir aos cidadãos a possibilidade de exercício da proteção de dados pessoalmente, através da ideia de garantia de uma liberdade negativa. A partir deste momento, a exigência do consentimento do titular tornou-se elemento essencial à legitimação do tratamento de dados e, portanto, a autorização para o exercício de tal atividade regulava a sua i(legalidade). A caracterização de uma mudança total no contexto das leis de primeira geração decorre da percepção de que seria inviável utilizar as mesmas estratégias que estavam sendo utilizadas anteriormente, tendo em vista que a ideia de uma única e centralizada bases de dados foi diluída pela presença de bancos de dados descentralizados, tanto na esfera pública, quanto na esfera privada[315].

Diante da utilização de dados pessoais por terceiros e da ausência de instrumentos para a defesa direta dos interesses dos indivíduos, as leis de segunda geração estabeleceram diversos instrumentos para a tutela dos dados pessoais, como mecanismos de identificação do uso indevido de informações pessoais e uma maior liberdade de fornecimento ou não destes dados[316]. Ou seja, um papel que antes era de titularidade do Estado, passa a ser do próprio

---

[314] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 176.

[315] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 111.

[316] A preocupação das leis de segunda geração referente à utilização de informações pessoais de maneira irregular é demonstrada fielmente no Caso SIFAR. Em 1971, após denúncia feita pela imprensa, foi confirmado por uma Comissão Parlamentar de Inquérito que o banco de dados mantido pelo ex-serviço secreto italiano era utilizado pela FIAT desde 1948 no processo de seleção de seus empregados. As informações de 150 mil cidadãos contidas no banco de dados do SIFAR incluam, além de seus dados pessoais, as suas opiniões e atividades políticas. A vinda à tona deste caso influenciou de forma direta no posicionamento da Itália acerca da regulamentação da proteção de dados pessoais em seu país. Ainda assim, até a obrigação de transposição da Diretiva 95/46/CE, o único respaldo legal referente ao tratamento de dados pessoais se encontrava na doutrina e jurisprudência italiana, sendo um dos últimos países europeus a legislar sobre a matéria. (BELLAVISTA, Alessandro. *Quale legge sulle banche datti?* **Rivista Critica del Diritto Privato,** n. 03, 1991, p. 691)

cidadão, caracterizando-se então como o responsável por autorizar o fluxo das suas informações pessoais através do seu consentimento[317]. Neste ponto, assemelha-se à ideia de privacidade sob a perspectiva de Alan Westin, qual seja, a "reivindicação dos indivíduos, grupos e instituições de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros"[318]. Dentre elas, destaca-se a Lei francesa de proteção de Dados Pessoais de 1978, pois demonstra a característica diferencial das leis de primeira geração para as leis de segunda geração: as técnicas de controle centradas no cidadão[319].

O sistema normativo de proteção de dados no direito europeu tem como elemento paradigmático da terceira geração de leis a sentença sobre o Censo Alemão, que, até os dias atuais, é amplamente reconhecida como referência do campo da proteção de dados[320]. Neste cenário, em 1982, foi aprovada a *Volkszahlungsgesetz*, lei que organizava o censo e que foi motivo de grande revolta e desconfiança dentre vários setores da sociedade alemã. Essa lei estabelecia o tratamento das informações que seriam obtidas através de um questionário de 160 questões efetuado pela antiga República Federal da Alemanha (R.F.A), que serviria a finalidades estatísticas. Acontece que, alguns pontos da lei geraram grande controvérsia e os trabalhos que deveriam ser encerrados em 1983, por não serem claros quanto ao método de coleta e o destino que seria dado às informações, jamais foi concluído.

A preocupação de alguns comissários de proteção de dados pessoais e entidades da sociedade civil organizada se caracterizava pelo sentimento de insegurança diante da possibilidade de transmissão dos dados coletados pelo censo para as autoridades federais e aos *Landers*, a existência de uma multa para aqueles que não respondessem o questionário, dentre outras possíveis consequências que poderiam advir da *Volkszahlungsgeset.* Ainda, temiam a possibilidade de utilização das informações com finalidade diversa à proposta pela lei. Neste sentido, a lei federal de proteção de dados pessoais vigente à época não se demonstrou eficiente, pois não era capaz de fornecer garantias adequadas e tampouco apresentar soluções para os pontos controversos da Lei do Censo.

---

317 MAYER-SCHONEBERGER, Viktor. *Generational development of data protection in Europe. In*: AGRE, Phillip E: ROTENBERG, Marc (Org.). ***Technology and Privacy:*** The New Landscape. Cambridge: The MIT Press, 1997, p. 226-227.

318 WESTIN, Alan F. ***Privacy and Freedom.*** New York: Atheneum, 1970, p. 7.

319 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 177-178.

320 VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 28.

Portanto, os trabalhos do censo da R.F.A deram ensejo a *Bundesverfassungsricht*, sentença da Corte Constitucional Alemã. Essa sentença estabeleceu a suspensão provisória do censo, declarando a sua incompatibilidade com os art. 1.1 e 2.1 da Lei Fundamental[321]. A Corte fundamentou a sua decisão de inconstitucionalidade em diversos pontos, dentre eles, a necessidade de observação do princípio da finalidade na coleta de dados pessoais, demonstrando a essencialidade do conhecimento do uso efetivo das informações coletadas[322]. Ainda, a sentença fez referência ao direito de autodeterminação informativa dos indivíduos[323], estabelecendo a liberdade de decisão individual no que tange aos limites e condições na utilização dos seus dados[324]. Nas palavras de Stefano Rodotà, essa prerrogativa é um "poder permanente de controle sobre os seus próprios dados[325]". A doutrina de autodeterminação informativa foi fundamental para o desdobramento dos atuais sistemas de proteção de dados pessoais[326], sendo inclusive um dos fundamentos da proteção de dados previsto no art. 2º, inciso II, da LGPD[327], demonstrando como o julgado germânico foi paradigmático.

Diante da reestruturação dada ao desenvolvimento econômico e social pela tecnologia da informação e a sua relação com o processamento de dados pessoais, a Organização para a Cooperação e Desenvolvimento Econômico[328] percebeu que seria necessário a conciliação

---

[321] Que assim dispõem, respectivamente, em tradução livre: "A dignidade humana é inviolável. É dever de todo poder estatal respeitá-la e defende-la."; "Todos têm direito ao livre desenvolvimento da própria personalidade, desde que não viole os direitos alheios e não transgrida o ordenamento constitucional e a lei moral". No documento original: "Artikel 1(1) Die Wurde des Menschen ist unantastbar. Sie zu achten und zu schutzen ist Verpflichtung aller staatlichen Gewalt. … Artikel 2(1) Jeder hat das Recht auf die freie Entfaltung seiner Personichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmabige.

[322] FROSINI, Vittorio. ***Contributi ad um diritto dell'informazione.*** Napoli: Liguiro, 1991, p. 128-129.

[323] "Aquele que, com segurança suficiente, não pode vislumbrar quais informações pessoais a si relacionadas existem em áreas determinadas de seu meio social, e aquele que não pode estimar em certa medida qual o conhecimento que um possível interlocutor tenha da sua pessoa, pode ter sua liberdade consideravelmente tolhida". (MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia. **Direito, inovação e tecnologia.** Vol. 01. São Paulo: Editora Saraiva, 2015, p. 211)

[324] "Concebida como um direito fundamental, na esteira do direito geral de personalidade, o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações" (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 169)

[325] RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Editora Renovar, 2008.

[326] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 170.

[327] "Modelos de negócios são invariavelmente pautados e rentabilizados, cada vez mais, no tratamento de dados pessoais. De tal sorte, pensar que o cidadão possa ter o controle sobre seus próprios dados parece, atualmente, utopia. Porém, a autodeterminação informativa se apresenta como fundamento da LGPD, justamente nesse momento em que ainda predomina uma coleta e tratamento massivo e desenfreado de dados, como forma de devolver para o titular o pode sobre o fluxo e o uso dos seus próprios dados, mediante o estabelecimento de determinações objetivas aos agentes de tratamento" (VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 27)

[328] Trata-se de uma organização internacional que foi criada após a Segunda Guerra Mundial e que visa o bem-estar econômico e social global, estabelecendo uma relação de cooperação entre os seus países-membros. Atualmente, participam 37 países-membros. Disponível em:<http://www.oecd.org/about/membersandpartners/>.

entre o desenvolvimento econômico e a proteção da privacidade, emitindo em 1980 e 1985 o *privacy guidelines*[329] e a *declaration on transborder data flows*[330], respectivamente, que se situam entre a terceira e quarta geração de leis de proteção de dados. A ideia de participação efetiva do titular nos processos de tratamento dos seus dados pessoais está presente em metade dos oito princípios elencados nas *guidelines,* ao se referirem expressamente à participação do titular dos dados em todo o processo de tratamento de dados[331]. Acerca das *guidelines* da OCDE, que acabaram se denominando como *Fair Information Practice Principles/*FIPPS[332], Bruno Bioni explica que nelas, a "própria noção do que seja um tratamento de dados pessoais justo e lícito é vinculada ao consentimento do indivíduo". Dentre os princípios elencados, destacam-se o princípio da limitação da coleta[333] e da especificação dos propósitos[334], ao ponto em que estabelecem técnicas que devem ser utilizadas pelos agentes visando o processo informativo sobre a finalidade dos tratamentos e só assim, será validada a autorização do titular de dados. Estes princípios complementam a

---

[329] As *guidelines*, em específico, tinham como objetivo principal garantir o livre fluxo de informações entre os países-membros da OCDE, estabelecendo padrões normativos para a proteção de dados pessoais e assim, evitando disparidades regulatórias entre os países. Consequentemente, através da criação de um regulamento unitário, é garantindo o livre trânsito de informações entre os países-membros. OECD Guidelines. p.11: "Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries; (…)". Disponível em: <http//www.oecd.org/about/>.

[330] Conforme conclui-se de quatro objetivos do *declaration on transborder data flows*, trata-se de documento regulatório dos países-membros do OCDE, diante da ideia de que a ausência de disparidades regulatórias facilitaria o livre fluxo informacional: "a)achieving acceptance by Member countries of certain minimum standard of protection of privacy and individual liberties with regard to personal data; b) reducing differences between relevant domestic rules and practices of Member countries to a minimum; c) ensuring that in protecting personal data they take into consideration the interest of other Member countries; and d) eliminating, as far as possible, reasons which might induce member countries to restrict transborder flows of personal data because of the possible risks associated with such flows". (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 jul. 2020)

[331] São eles: a) Limitação de Coleta (Collection Limitation Principle); c) Especificação dos Propósitos (Purpose Especification Principle); d) Limitação do Uso (Use Limitations Principle e; g) Participação Individual (Individual Participation Principle)

[332] Cumpre observar que os FIIPS, originalmente, são um conjunto de princípios que resultaram do trabalho do Comitê de Aconselhamento sobre Sistemas de Dados Automatizados do governo dos Estados Unidos em 1973 que, posteriormente, foram transpostos pela OCDE. (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 jul. 2020)

[333] "Collection Limitation Principle: 7. There should be limits to collection of personal data and any such data should be obtained by lawful and fair means and, when appropriate, with the knowledge or consent of the data subject". (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 jul. 2020)

[334] "Purpose Specification Principle: 9 The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others are not incompatible with those purposes and as are specified on each occasion of change of purpose". (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 jul. 2020)

ideia de autodeterminação informacional, garantindo aos indivíduos a possibilidade de retificar, emendar, complementar, assim excluir as suas informações das bases de dados[335].

Percebe-se que, a terceira geração de leis, abordada acima na análise da decisão do Tribunal Constitucional Alemão e das *Guidelines* da OCDE, refletem uma preocupação que vai além da garantia de possibilitar que os indivíduos escolham entre fornecer ou não os seus dados pessoais, dando enfoque na garantia da efetividade desta liberdade. Essa ideia de efetividade se concretizou através da participação consciente e ativa dos cidadãos nas diversas fases que englobam o tratamento de dados pessoais e da inclusão de determinadas garantias, como o dever se informação e da autodeterminação informativa. Neste momento, as normas não só transferiram para o próprio titular de dados a responsabilidade de protegê-los, como também, visando o alcance da autodeterminação informativa, procuraram garantir a participação deles em todo o processo de tratamento de dados[336].

No entanto, diante de um cenário caracterizado pelo alto custo econômico e social envolvido na efetivação da autodeterminação informativa, o exercício de tal prerrogativa era a realidade de uma minoria, pois muitos não estavam dispostos a enfrentar tais consequências. Ainda, o consentimento livre, informado, inequívoco, explícito ou específico, como definido em diversas leis de proteção de dados como parâmetro definidor da i(licitude) de qualquer atividade de tratamento de dados pessoais, trata-se de um controle praticamente inefetivo das informações pessoais pelo titular daqueles dados. Neste contexto de insatisfação, diante de um sistema falho de proteção de dados pessoais baseado na tutela destas informações através de um mecanismo de escolha individual, surgem as leis da atualidade, representando as leis de quarta geração. Partindo do pressuposto de que existe um claro desequilíbrio na relação entre o titular dos dados e as entidades que coletam e processam estes dados, pode-se dizer que, de forma geral, as leis de quarta geração buscam a efetivação de técnicas que fortalecem a posição dos indivíduos[337], por meio, inclusive, de autoridades independentes para a aplicação das leis. Entende-se que, a partir do momento em que as normas não deixaram mais a escolha

---

[335] "Individual Participation Principle: 13. An individual should have the right: (…) d) to challenge data relating to him and, if the challenge is successful to have the data erases, rectified, completed or emended". (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 jul. 2020)

[336] MAYER-SCHONEBERGER, Viktor. *Generational development of data protection in Europe. In*: AGRE, Phillip E: ROTENBERG, Marc (Org.). ***Technology and Privacy:*** The New Landscape. Cambridge: The MIT Press, 1997, p. 231.

[337] RODOTÀ, Stefano. ***Repertorio di fine secolo.*** Bari: Laterza, 1999, p. 103.

de determinados tipos de processamento de dados pessoais nas mãos dos titulares, houve uma relativização da ideia do consentimento como elemento central[338].

No entanto, conforme explica Bruno R. Bioni, no que pese ter havido uma relativização do instituto ora analisado, o seu papel de protagonismo nas leis de proteção de dados não foi extinto. O autor se refere às adjetivações do consentimento (livre, informado, inequívoco, explícito ou específico) como prova de tal alegação, pois tais qualificações acabam caracterizando um "movimento refratário em torno do papel de destaque do consentimento quase como sendo sinônimo de autodeterminação informacional[339]". O processo de revisão das *guidelines* da OCDE também demonstra a caracterização de uma trajetória normativa pautada na emersão do consentimento e a sua reafirmação como vetor central das leis de proteção de dados, pois, após 30 anos, a sua base, predominantemente centrada no titular de dados como ponto focal, se manteve[340]. Ademais, a própria replicação dos princípios previstos nas *guidelines* no próprio GDPR demonstra que o protagonismo dado ao consentimento permanece presente como um dos fios condutores do tratamento e proteção dos dados pessoais. Dentre as suas disposições, destacam-se a essencialidade do consentimento via declaração ou ação afirmativa representativa[341] e um processo de tomada de decisão do titular dos dados pessoais que possua informações facilmente acessíveis, claras e de simples linguagem[342]. Neste ponto, para um melhor entendimento acerca do papel do consentimento como mecanismo de garantia da proteção de dados dos titulares na LGPD, cumpre a análise das leis infraconstitucionais que dispõem de maneira específica acerca da proteção de dados e do papel do consentimento para uma efetiva prestação de tal direito.

---

[338] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 373.

[339] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 113.

[340] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 jul. 2020.

[341] Art. 4(8): "the data subject´s consent means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed". (UNIÃO EUROPEIA. ***General Data Protection Regulation.*** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[342] Art. 7(2): "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be represented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration which constitutes an infringement of this Regulation that the data subject has given consent to shall not be binding". (UNIÃO EUROPEIA. ***General Data Protection Regulation.*** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

4.1.1 As principais leis setoriais brasileiras anteriores à LGPD

Com influência direta do padrão normativo regulado pelo *Fair Information Practice Principles*, o Código de Defesa do Consumidor disciplinou, em seu art. 43[343], a figura dos bancos de dados e cadastro de consumidores de forma ampla, visando atingir todos os tipos de dados que possuem condão de influenciar no livre desenvolvimento da personalidade do consumidor[344]. Percebe-se, diante da amplitude do dispositivo em questão, a ideia do legislador em garantir uma normatização que sustente a capacidade do indivíduo em autodeterminar as suas próprias informações. A título de exemplo, em seu §2º, o art. 43 do CDC se refere à exigência de notificação ao consumidor a respeito da abertura de um banco de dados não solicitado pelo titular de dados. Portanto, é clara a presença da transparência, permitindo que o consumidor acompanhe a circulação de suas informações pessoais[345].

Ainda, ao decorrer do art. 43, extraem-se alguns deveres do operador dos bancos de dados, quais sejam: a garantia de acesso pelo consumidor (*caput*); a restrição das informações nos bancos de dados as finalidade claras e verdadeiras; o limite temporal de 5 anos no que se refere ao armazenamento de informações negativas (§1º). Assim, é dado ao consumidor o direito de exigir a correção de informações inexatas ou que tenham superado o referido limite temporal mencionado acima (§3º). Desta forma, percebe-se que, ao incluir regras para a garantia da exatidão dos dados, bem como limitação de 5 anos para o seu armazenamento, o legislador buscou conferir, de fato, a autodeterminação informativa ao consumidor[346].

---

[343] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. (BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF. 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2020)

[344] Sobre a ameaça dos direitos da personalidade na esfera consumerista, ensina Antônio Herman de Vasconcellos e Benjamin: "De modo direto, o mau funcionamento dos arquivos de consumo ameaça, primeiramente, o direito à privacidade, por que cada indivíduo pode clamar, na esteira da elaboração mais ampla dos direitos da personalidade". (BENJAMIN, Antonio Herman de Vasconcellos. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto.** 5 ed. Rio de Janeiro: Editora Forense Universitária, 1997, p. 421)

[345] "Daí que, cada vez que o arquivo de consumo recebe dado que significa inovação, se se quer incorporá-la precisa informar o consumidor. Vale dizer, o direito à comunicação não se exaure num momento específico e inicial da vida do arquivo de consumo, mas se protrai no tempo, enquanto este permanecer" (BENJAMIN, Antonio Herman de Vasconcellos. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto.** 5 ed. Rio de Janeiro: Editora Forense Universitária, 1997, p. 476)

[346] No que se garantia da autodeterminação informativa ao consumidor, Ana Paula Gambogi ensina: "A preocupação do legislador em assegurar ao consumidor o controle da manipulação de dados seus armazenados em arquivos de consumo denota a busca pela chamada autodeterminação informacional". (GAMBOGI, Ana Paula. O Consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. *In*: MARQUES, Claúdia Lima; MIRAGEM, Bruno (Org.). **Coleção doutrinas essenciais: direito**

Já a Lei 12.414/2011 (Lei do Cadastro Positivo), se preocupa em disciplinar a formação de banco de dados nas situações em que o postulante ao crédito passar por uma análise financeira que vai além de informações relativas a dívidas não pagas, por isso o termo "cadastro positivo" e não "cadastro negativo". Como explica Leonardo R. Bessa, "qualquer dado além das informações necessárias para identificar um débito vencido e não pago pode ser classificado como informação positiva[347]". Ainda que de forma restrita ao âmbito dos históricos de crédito, a referida Lei estabelece alguns dos princípios de proteção de dados, pautando-se na ideia de gerenciamento do próprio titular de dados.

Neste sentido, em 2019, foi sancionada a Lei Complementar nº 166/2019 e com ela, a inclusão de nomes de consumidores no banco de dados que antes só ocorria mediante o consentimento do titular de dados pessoais passou a ocorrer de forma automática. No que pese tal mudança aparentar-se como um retrocesso, agora os titulares podem solicitar a retirada dos seus nomes do banco de dados. No que se refere ao compartilhamento de informações a outros bancos de dados, a referida Lei Complementar alterou a Lei 12.414/2011, passando a possibilitar ao gestor tal ato, desde que não colete informações excessivas[348] e sensíveis[349] com a finalidade de análise de crédito e desde que cumpra com a finalidade pré-estabelecida[350], qual seja, de análise creditícia. Portanto, tais limitações atuam de forma benéfica no que se refere ao controle das informações por parte do próprio titular, pautando-se na técnica legislativa da autodeterminação informacional.

Por fim, cumpre mencionar que as inovações trazidas pelo Marco Civil da Internet já foram analisadas no segundo capítulo deste trabalho sob a perspectiva da proteção de dados de

---

do consumidor – proteção da confiança e práticas comerciais. São Paulo: Editora Revista dos Tribunais, vol. 3, 2011, p. 390)

[347] BESSA, Leonardo Roscoe. **Cadastro positivo:** comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Editora Revista dos Tribunais, 2011, p. 38.

[348] Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. [...] I - objetivas: aquelas descritivas dos fatos e que não envolvam juízo de valor; (BRASIL. **Lei nº 12.414,** de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF. 09 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 10 jun. 2020)

[349] Art. 3º [...] II - claras: aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica; (BRASIL. **Lei nº 12.414,** de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF. 09 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 10 jun. 2020)

[350] Art. 5º São direitos do cadastrado: [...] VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados (BRASIL. **Lei nº 12.414,** de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF. 09 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 10 jun. 2020)

forma geral. No que se refere ao instituto do consentimento, este, em específico, pode ser observado com mais clareza no contexto do cenário "pós-Snowden", que resultou no acréscimo de três incisos no art. 7º da lei. Como resultado desta alteração, o arranjo normativo do MCI foi diretamente afetado, ao ponto em que todos os três incisos se referem à necessidade do consentimento do usuário para o tratamento de seus dados, bem como para a transferência a terceiros[351], passando a ser o usuário o protagonista na relação de proteção de seus dados pessoais. Ainda, o MCI qualifica a validade do consentimento como aquele que é livre, expresso e informado[352], estando o responsável pelas atividades de tratamento sujeitos à prestação de informações completas e de forma clara. Corroborando com a ideia de ser a autodeterminação informativa o parâmetro eleito pelo MCI para garantir a proteção de dados, em seu art. 7º, inciso X[353], é previsto a possibilidade de o usuário requerer a exclusão definitiva de seus dados pessoais quando encerrada a sua relação com determinada aplicação de Internet.

[351] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; [...] Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: [...] II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular. (BRASIL. **Lei nº 12.965,** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2020)

[352] Art. 7º [...] VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; [...] VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; (BRASIL. **Lei nº 12.965,** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2020)

[353] Art. 7º [...] X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei. (BRASIL. **Lei nº 12.965,** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2020)

4.2 A NATUREZA JURÍDICA DO CONSENTIMENTO

Apesar de aparentar-se simples e de fácil percepção relacionar o consentimento com a atuação do poder de autodeterminação informativa e, portanto, relacioná-lo com o campo da autonomia privada, a natureza jurídica do consentimento no âmbito da proteção de dados pessoais é um tema bastante polêmico na doutrina. Cumpre mencionar que, o legislador, neste ponto, demonstra a essencialidade da autodeterminação informativa como um dos fundamentos da LGPD em diversos momentos. O Capítulo III da Lei, por exemplo, claramente busca dar efetividade a tal prerrogativa do titular de dados quando dispões sobre o direito de obter do controlador a confirmação da existência do tratamento, da correção de dados incompletos, do bloqueio ou eliminação de dados desnecessários, entre diversos outros já analisados no Tópico 3.2 deste Trabalho. Assim, ao mesmo tempo em que atua como forma de viabilizar o exercício do papel da autodeterminação informativa pelo titular, o consentimento também se caracteriza como um meio de legitimação para o tratamento de dados pessoais.

Assim como Orlando Gomes[354], que defende o consentimento como um típico elemento do direito contratual, Laura Schertel se refere a tal instituto como "mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão[355]". Para a autora, existem três principais correntes acerca da natureza jurídica do consentimento no âmbito da proteção de dados pessoais. Enquanto uma parte da doutrina defende a natureza de declaração de vontade negocial, do lado oposto, há aqueles que entendem que se trata de um ato jurídico unilateral. Já a terceira corrente, afirma que a natureza do consentimento se assemelha ao negócio jurídico, mas que com ele não se confunde. Na perspectiva da Autora, a terceira corrente é a mais adequada, pois ao mesmo tempo em que é inegável a presença de características negociais no consentimento, é também um instituto personalíssimo, com natureza diferenciada[356]. Por isso, diante dessa atipicidade, há a necessidade de análise no caso concreto para afirmar quais normas são aplicáveis ao consentimento.

Já sob o ponto de vista de Danilo Doneda, no que se refere ao aspecto técnico do consentimento, não parece apropriado a sua natureza se limitar ao aspecto negocial, pois "se

---

[354] GOMES, Orlando. **Contratos.** 26 ed. 2 tir. Rio de Janeiro: Editora Forense, 2008.
[355] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 60.
[356] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 63.

assim fosse, seria legitimada a inserção desse consentimento em estruturas contratuais, dificultando a sua valoração em função dos atributos da personalidade que estão em jogo[357]". Aproximando-se da segunda corrente mencionada, o autor se refere à natureza de tal instituto como um ato unilateral, pois tem como efeito a autorização ou não de um determinado tratamento de dados, ainda assim, não estando diretamente relacionado a uma estrutura contratual[358].

Neste seguimento, relacionando-se com o que Davide Messinetti chama de "neo-dogmatismo fraco[359]", Danilo Doneda analisa criticamente a relação entre a atuação da autonomia privada nos mecanismos negociais tradicionais e dos parâmetros utilizados no consentimento para o tratamento de dados pessoais e, da problematização de uma transposição superficial do direito privado no âmbito da proteção de dados:

> Os parâmetros a serem levados em consideração para determinar o perfil desse consentimento, no entanto, não são os mesmos que embasam a atuação da autonomia priva nos mecanismos negociais tradicionais e devem levar em conta uma série de fatores que, ao fim, poderão afastar a possibilidade de se recorrer a algumas modalidades de consentimento. Uma advertência prévia, por exemplo, seria a de resistir à tentação de utilizar os mecanismos negociais em suas vestes tradicionais, até que se verifique a sua pertinência. O problema derivado de uma transposição rasa do consentimento negocial para o consentimento ao tratamento de dados pessoais está presente em toda a crítica ao "mito do consentimento". Tais problemas são, basicamente, reflexos da adaptação de uma estrutura formal e pretensamente neutra a uma realidade que apresenta apenas uma falsa semelhança com o ambiente no qual o consentimento é um real instrumento de realização da autonomia privada e pode compreender uma escolha ideológica[360].

Para Laura Schertel Mendes, a aplicação das regras adotadas no âmbito dos contratos em geral ao consentimento no tratamento de dados pessoais deve se mostrar cabível e adequada ao caso concreto. Diante das particularidades de cada caso, tal análise é essencial e neste sentido, a própria autora se refere à inaplicabilidade do instituto da capacidade civil ao consentimento, tendo em vista, principalmente, o seu caráter personalíssimo. No caso do consentimento para o tratamento de dados, não é necessária à análise acerca da capacidade

---

[357] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 302.

[358] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 378.

[359] A utilização de um instituto originalmente do direito civil, qual seja, a autonomia da vontade, há de se atentar para o que Davide Messinetti chama de 'neo-dogmatismo fraco', pois a utilização de categorias dogmáticas em outro âmbito que não o seu âmbito teórico original corre o risco de "atenuar sua relação com as rationes sistemáticas que a tradição dogmática nelas condensava, além da progressiva diminuição do grua de especificidade de problemas e remédio que tal tradição pretendia, com estas categorias, abranger". (MESSINETI, Davide. Circolazioni di dati personali e dispositivi di regolazione dei poteri individuali. ***Rivista Critica Del Diritto Privato,*** 1998, p. 341)

[360] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 301.

civil[361] do titular de dados, mas sim a sua capacidade de discernimento para autorizar a utilização de seus dados pessoais para o fim proposto pelo agente de tratamento[362]. Assim como a LGPD, o GDPR[363] não dispõe sobre normas limitando a idade mínima para consentir a tratamento de dados, cabendo posicionamento das autoridades Austríacas, que entendem como a idade mínima para o exercício de tal ato 14 anos[364].

No que se refere à adjetivação do consentimento, observa-se, das características utilizadas pelo legislador para validar o consentimento na LGPD, a sua relação com a ideia da declaração da vontade livre e consciente extraída do Código Civil no tema dos defeitos do negócio jurídico[365]. E, portanto, a partir do momento em que estes requisitos não estão presentes, configura-se o "vício de consentimento", decorrendo daí a possibilidade de anulabilidade do negócio jurídico[366]. Diante da LGPD, no §3º do art. 8º fazer menção expressa à vedação do vício de consentimento, nos exatos mesmos termos do Código Civil, sob o ponto de vista de Bruno Ricardo Bioni, "é muito provável que haja um diálogo com o Código Civil brasileiro para se interpretar toda a adjetivação do consentimento à luz dos defeitos do negócio jurídico[367]".

É inegável, no entanto, a utilização da disciplina do consentimento como um instrumento para o livre desenvolvimento da personalidade, demonstrando a relevância do direito privado na elaboração de um sistema de proteção de dados pessoais sólido. Deve, neste sentido, ser observado o perigo da "transposição rasa" analisado acima. Ambos os institutos (declaração de vontade no âmbito do negócio jurídico e consentimento visando à tutela de dados pessoais) se referem à efetivação da autodeterminação. Assim, por sintetizar a atuação da autonomia

---

[361] Art. 3 º São absolutamente incapazes de exercer pessoalmente os atos da vida civil os menores de 16 (dezesseis) anos.; Art. 4 º São incapazes, relativamente a certos atos ou à maneira de os exercer: I - os maiores de dezesseis e menores de dezoito anos; II - os ébrios habituais e os viciados em tóxico; III - aqueles que, por causa transitória ou permanente, não puderem exprimir sua vontade; IV - os pródigos. Parágrafo único. A capacidade dos indígenas será regulada por legislação especial. (BRASIL. **Lei nº 10.406,** de 10 de janeiro de 2002. Institui o Código Civil. 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 20 jun. 2020)

[362] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 63.

[363] Art. 8º (1). Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[364] LEMOS, Renato. GDPR: A nova legislação de proteção de dados da Europa. **AB21.** 20 jun. 2018. Disponível em: https://www.ab2l.org.br/gdpr-nova-legislacao-de-protecao-de-dados-pessoais-da-europa/. Acesso em: 04 jul. 2020.

[365] THEODORO JUNIOR, Humberto. **Comentários ao novo Código Civil:** dos defeitos do negócio jurídico. Rio de Janeiro: Editora Saraiva, 2013, p. 04.

[366] MONTEIRO, Washington de Barros. **Curso de Direito Civil:** parte geral. Vol. 01. São Paulo: Editora Saraiva, 2012, p. 242.

[367] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 179.

privada em determinado momento no tratamento de dados, deve ser interpretado de forma fidedigna à manifestação de escolha do titular.

4.3 A LIMITAÇÃO DA ATUAÇÃO DOS AGENTES DE TRATAMENTO PELO CONSENTIMENTO DO TITLAR DE DADOS PESSOAIS

Ao mesmo tempo em que o consentimento foi incluído no rol do art. 7º da LGPD como apenas mais uma das bases legais de tratamento, e, portanto, sem caracterizar-se como hierarquicamente superior, pode-se dizer que, não deixou de ser o ponto focal da Lei. Neste seguimento, nota-se, de uma simples observação temporal do percurso da LGPD, que se iniciou há 10 anos, que o consentimento, na primeira versão do anteprojeto da lei submetida à consulta pública, bem como na segunda consulta pública que ocorreu em 2015, era a única base legal de tratamento de dados pessoais. Apesar de tal fato demonstrar-se um retrocesso para a garantia da proteção de dados através do consentimento, uma simples análise numérica de quantas vezes o termo consentimento é citado no corpo legal demonstra não só a sua relevância para a proteção de dados como instrumento que impacta a atuação dos agentes de tratamento de diversas maneiras, mas também, a necessidade de uma interpretação deste instituto na LGPD de forma sistemática, uma vez que é mencionado 37 vezes de forma esparsa.

O legislador, além de adjetivar extensamente os requisitos que qualificam o consentimento como válido, relaciona-o diretamente como o princípio da finalidade, conforme regula o art. 5º, XII. Ainda, em casos específicos, além do consentimento livre, informado e inequívoco, deve ser também específico[368]. Observa-se aqui, que o legislador optou em adjetivar extensivamente o consentimento, característica presente na quarta geração de leis de proteção de dados já analisadas, bem como traço marcante do direito comunitário europeu.

Além do mais, seis dos nove princípios elencados no art. 6º da LGPD estão diretamente focados na atuação do titular de dados[369]. Sobre os princípios terem o seu centro gravitacional

[368] O consentimento deve também ser específico nos casos regulados pelos arts. 7º, §5º; 14, §1 º e 33, VIII, da LGPD.

[369] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas

no indivíduo e consequentemente, sendo o consentimento o instrumento legitimado pela Lei para um efetivo acompanhamento do fluxo de seus dados pessoais, Bruno R. Bioni explica que, "é uma carga principiológica que procura conformar, juntamente, a ideia de que o titular de dados pessoais deve ser empoderado com o controle de suas informações pessoais, e sobretudo, na sua autonomia da vontade"[370]. Além do mais, o regramento específico dado ao consentimento, visando a sua concretização, orientação, bem como a possibilidade do titular reforçar o controle dos seus próprios dados por meio do consentimento, seja por meio da possibilidade de revogabilidade do consentimento ou da hipótese de término do tratamento quando da comunicação do titular de dados, demonstram ser o referido instituto o elemento cardeal da LGPD e, portanto, impactando de forma direta a atuação dos agentes de tratamento.

4.3.1 O consentimento como uma base legal

De início, cumpre lembrar que, conforme conceitua a LGPD em seu art. 5º, o tratamento de dados pessoais engloba uma série de operações de titularidade dos agentes de tratamento (controlador ou operador), como a coleta, acesso, armazenamento e até mesmo a eliminação de dados pessoais, dentre outros. Portanto, o tratamento de dados pessoais está legitimado, além das hipóteses já analisadas a fundo no Capítulo 3 deste Trabalho, quando o titular de dados fornece o seu consentimento (art. 7º, I, da LGPD). Referente às adjetivações do consentimento, apesar do legislador não ter se preocupado em defini-las, uma real compreensão conceitual dos termos "livre, informado e inequívoco" é essencial para a análise da validade de tal ato.

Com base no *Article 29*[371], documento que versa de maneira específica acerca do consentimento à luz do GDPR, um consentimento livre é aquele em que o titular possui liberdade em escolher os tipos de dados que serão tratados em cada operação, sem qualquer

---

finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[370] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 128.

[371] Atual *European Data Protection Board* – EDPB.

tipo de pressão para o fornecimento do consentimento ou consequências negativas desproporcionais caso o não fornecimento de tal ato. Ao pensar na palavra livre, é comum uma associação imediata ao livre-arbítrio, sendo essa exatamente a lógica pensada pelo legislador[372]. A título de exemplo, o referido *Article* 29 menciona o caso em que um banco que solicita o consentimento dos titulares e clientes para a utilização dos dados referentes às suas movimentações bancárias para a finalidade de *marketing* da empresa. Neste caso, por óbvio, o tratamento destes dados para tal fim não é necessário para a relação contratual entre o banco e os seus clientes e, portanto, caso o cliente recuse que o tratamento de seus dados seja utilizado para *marketing* e sejam negados os serviços bancários ou qualquer outra consequência desarrazoada, como o encerramento da sua conta ou aumento de taxas, resta configurada a violação à liberdade de consentir[373].

Como sugere a Consideranda 43 do GDPR[374], para um adequado enquadramento do consentimento como livre, deve ser investigado o nível de assimetria[375] presente na relação. Portanto, deve ser levado em consideração o leque de opções disponibilizadas para o titular de dados, sendo este o elemento regulador de calibração do consentimento livre. Nas palavras de Bruno Bioni, a equalização de tal relação, que, de praxe, é orginalmente assimétrica, se dá pela análise do "poder de barganha" do titular de dados[376].

Importante também observar a característica de granularidade do consentimento livre, ideia extraída do referido *Article 29*[377], devendo o titular de dados ser possibilitado de emitir

---

[372] Tem-se como exemplo as situações nas quais para a instalação de determinado aplicativo há a obrigação do indivíduo em autorizar, sob pena de não ter acesso à aplicação, o acesso à sua geolocalização, câmara de vídeo, fotos armazenadas, dentre outros fatores de tratamento que não possuem relação com o funcionamento do aplicativo. Nestes casos, para a configuração de um consentimento livre, o titular de dados deve ter a opção livre, sem nenhum tipo de pressão para a entrega do seu ato de vontade e sem a presença de consequências negativas exageradas.

[373] EUROPEAN COMISSION. ***Article 29 Working Party.*** Disponível em: https://ec.europora.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 15 mar. 2020.

[374] Consideranda 43. "a clear imbalance between data subject and the controller". (UNIÃO EUROPEIA. ***General Data Protection Regulation.*** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[375] No que se refere à assimetria ainda mais acentuada em relações de emprego e no tratamento de dados pelo Poder Público, tendo em vista a posição superiormente hierárquica de tais agentes quando na posição de controlador de dados, o *Guideline* 259/2017 aborda de forma específica tal tema, informando a necessidade de observação de uma maior atenção pelos agentes de tratamento.

[376] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

[377] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...] § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

autorizações fragmentadas ao decorrer de todo o processo de tratamento. A este respeito, conforme entendimento de Caio César C. de Lima, o consentimento com base na lógica do tudo ou nada, característica geralmente presente nas políticas de privacidade, bem como presente na dinâmica dos contratos de adesão[378], é inválido, sendo necessário que, "nas situações em que houver coleta de dados para diferentes finalidades, o titular dos dados deve ter a possibilidade de escolher, de uma a uma, a finalidade específica com relação a qual autoriza o tratamento de dados". Corroborando com a ideia de um consentimento granular[379], a LGPD, em seu art. 9º, §3º, nos casos em que o tratamento de dados for condição para o fornecimento de produto, serviço ou para o exercício de direito se refere à necessidade do titular de dados ser informado com destaque acerca da referida condicionante, bem como dos meios pelos quais ele pode exercer os seus direitos.

O adjetivo "informado", guardando bastante relação com o princípio da transparência[380], se refere à necessidade de os titulares serem, antes da coleta de seus dados pessoais, amplamente informados acerca de todo o fluxo de tratamento. Trata-se, então, de um dever-direito de informação[381] e neste sentido, a LGPD, visando o entendimento completo por parte do titular de dados para que possa efetuar a sua tomada de decisão de forma genuína, prevê em seu art.9º que as informações sobre o tratamento de dados devem ser prestadas de forma clara, adequada e ostensiva. Ainda, em seus incisos, elenca quais informações o titular pode acessar de forma facilitada, nos seguintes termos:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
>
> I - finalidade específica do tratamento;
>
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
>
> III - identificação do controlador;
>
> IV - informações de contato do controlador;

---

[378] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 185.

[379] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 186.

[380] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[381] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 180.

> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
>
> VI - responsabilidades dos agentes que realizarão o tratamento; e
>
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Conforme se extrai do *caput* do art. 8º[382] da LGPD, a obtenção do consentimento não se restringe a uma modalidade específica, o exercício dessa transparência pode ser concretizado de diversas formas, seja por vídeo, áudio, por escrito, dentre outros, desde que, seja utilizada linguagem clara e direta, de fácil compreensão para o público alvo, bem como, para que tenha validade jurídica, deve necessariamente ser em língua portuguesa (art. 224 do Código Civil). No entanto, caso o consentimento seja fornecido por escrito, deve constar de cláusula destacada das demais[383]. Também, é dever dos agentes de tratamento informar aos titulares os possíveis riscos que podem decorrer do tratamento de seus dados e caso as informações oferecidas pelos agentes possuam conteúdo enganoso, abusivo ou não tenham sido apresentados previamente com transparência, de forma clara e inequívoca, o consentimento será considerado nulo[384].

Para que os titulares possam, em sua completude, refletir sobre o tratamento e tomar decisões com base nos seus direitos, deve ser levado em consideração pelo controlador à capacidade de assimilação dos titulares com base na ideia do homem-médio e sua a característica de vulnerabilidade. A estrita necessidade de observância da transparência pode ser observada no caso da Autoridade francesa (CNIL) contra o Google, onde a plataforma foi condenada a 50 milhões de euros diante da ausência da transparência necessária aos usuários[385]. Em um

---

[382] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[383] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[384] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...] § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[385] COMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.** 21 jan. 2019. Disponível em: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Acesso em: 20 jul. 2020.

contexto de opacidade no tratamento de dados, a presença destas informações atua como elemento legitimador do próprio consentimento (art. 9º, §1º, da LGPD) [386].

Sob o ponto de vista de Bruno Bioni, no que pese a informação ser elemento essencial para o consentimento válido, diante do risco do excesso de informação[387], há de ter cuidado com a sua sobrecarga:

> (...) a informação deve somar, deve acrescer, deve preencher o vazio da assimetria informacional, equalizando-a. É obvio, no entanto, que ao consumidor é impossível alcançar o mesmo patamar informativo do fornecedor. Até porque, para ele, é desnecessário saber todas as minúcias da atividade de tratamento de dados pessoais. Pense-se nos diversos padrões de segurança da informação, de como algoritmos são desenvolvidos e assim por diante. Ao cidadão cabe compreender os riscos e as implicações que tal atividade trará sobre a sua esfera pessoal, a fim de racionalizar alguma decisão sobre o fluxo de seus dados. Ao contrário de ser sobrecarregado com uma avalanche de informações sobre lógica dos protocolos de segurança e as formulas dos algoritmos para desvendar, respectivamente, quais seriam os tipos de vulnerabilidades de cada um dos padrões de segurança da informação e qual seria a correlação a ser descoberta por tal algoritmo[388].

Ainda, a regra adotada pela LGPD é a do consentimento inequívoco e como exceção, em situações especiais, como no caso do tratamento de dados pessoais sensíveis, de crianças e adolescentes, bem como na transferência internacional de dados pessoais, a legalidade do tratamento quando da necessidade de consentimento se relaciona ao consentimento específico. Inequivocamente significa que o titular de dados, de fato, manifestou a sua autorização para o tratamento de seus dados, mesmo que de forma implícita, uma vez que não precisa ser expressa[389]. Isso pode ocorrer de diversas formas, desde que o indivíduo concorde com algo que está claro para ele, seja por meio de vídeo, declaração escrita, em formato eletrônico ou

---

[386] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...] § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[387] "Para responder tais questões, precisamos analisar a capacidade humana de armazenar e processar informações. Para tanto, diversos autores utilizam o conceito de *bounded rationality*, que traduz a noção de racionalidade limitada e postula que os indivíduos não têm capacidade para receber, armazenar e processar grande volume de informações" (MARZAGÃO, Nelcina C. de O. Tropardi. **Da informação e dos efeitos do excesso de informação no direito do consumidor.** Tese (Doutorado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, São Paulo, 2005, p. 198)

[388] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 18.

[389] "Um usuário que resolve dispor do seu endereço de e-mail em página da internet com a seguinte mensagem 'deixe o seu e-mail aqui para receber a nosso newsletter sobre proteção de dados pessoais' está conferindo um consentimento inequívoco para esta finalidade. Assim como alguém que deixa ser fotografado como forma de permissão para a entrada em um condomínio, por motivos de segurança". (LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 120)

até mesmo oralmente[390]. Neste sentido, a Consideranda 32 do GDPR deixa claro que o silêncio, a omissão e as opções pré-validadas não são formas de consentimento[391]. Para evitar qualquer incerteza acerca da sua obtenção, o controlador deve ainda se preocupar em armazenar todas as informações que comprovem não só que o titular consentiu de forma inequívoca, mas também, especialmente nas situações em que o tratamento foi obtido de forma não presencial, que foi de fato o titular de dados que manifestou a sua vontade e não um terceiro.

Também será objeto de análise, quando da qualificação do consentimento como sendo inequívoco, a qualidade de interação do usuário, trazendo a ideia extraída do princípio da boa-fé. Ou seja, tanto no ambiente *on-line*, quanto no *off-line*, deve ser ponderado o *design* do ambiente e observado se atua como forma de manipulação das escolhas dos usuários ou se o auxilia no controle sobre os seus dados. Em pesquisa realizada pela Universidade de Bochum[392] na Alemanha em cenários pós- GDPR notou-se, através de falha no design a presença de evasão das escolhas do titular de dados.

Após a sanção do GDPR, os pesquisadores notaram que houve um aumento em cerca de 45% dos avisos de *cookies*[393] em *websites* e, portanto, passaram a analisar se tais banners de fato atuavam em benefício da transparência no tratamento de dados e na obtenção de um consentimento válido. Assim, realizaram três experimentos, dentre eles, a posição na qual os referidos avisos eram exibidos na plataforma. O resultado deste experimento demonstra

---

[390] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 119.

[391] Consideranda 32. "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido". (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[392] UTZ, Christine; DEGELING, Martin; FAHL, Sascha; SCHAUB, Florian; HOLTZ, Thorsten. (Un)informed consent: studying GDPR consent notices in the field. *In*: 2019 ACM SIGSAC **Conference on Computer and Communications Security (CC' 19)**, November 11-15, 2019, London, United Kingdom. ACM, New York, NY, USA. Disponível em: <https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentichungen/2019/09/05/uninfomed-consent_Yl7FPEh.pdf>. Acesso em: 20 jul. 2020

[393] "Aviso de cookies ou cookie notice é o banner que aparece na tela do usuário ao entrar em um site, indicando que está coletando cookies". (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 152)

claramente quanto o mero *design* pode influenciar e manipular a decisão tomada pelo titular em relação aos seus dados pessoais, ao ponto em que o aviso, além de ser posicionado no topo ou no final da página em quase 100% das vezes, era colorido com tonalidades escuras para prejudicar a visibilidade e ainda, não bloqueava o conteúdo do site, tendo, portanto, uma baixa taxa de cliques[394].

Apesar de haver a necessidade de observação dos princípios elencados no art. 18 da LGPD em todas as bases de tratamento[395], no caso do consentimento, em específico, há ainda uma maior relevância, pois, além das três adjetivações do consentimento analisadas, o consentimento é uma manifestação "pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada[396]". Corroborando com a efetividade da necessidade de observância do princípio da finalidade no consentimento, o §4º do art. 8º prevê que autorizações genéricas para o tratamento de dados pessoais serão nulas. Nos termos utilizados por Bruno Bioni para explicar o porquê de a declaração de vontade do titular como autorização do tratamento de dados ter um direcionamento específico, se refere ao consentimento genérico como uma espécie de "cheque em branco" e como consequência, o titular perderia qualquer controle sobre os seus dados.[397]

Mesmo sendo os adjetivos "informado" e "livre" mencionados antes do trecho "finalidades determinadas" na redação do art. 5º, XII, entende-se que, tais adjetivos são calibrados pelo princípio da finalidade e a partir disto, extrai-se o consentimento inequívoco do titular de dados. Assim, deve ser observado o preenchimento de todos os quatro requisitos para a adequacação do consentimento aos requisitos de validade impostos pela Lei. Neste aspecto, a Consideranda 43 do GDPR demonstra da necessidade de uma interpretação conjunta de todas

---

394 "Typical techniques include color highlighting of the button to accept privacy-unfriendly defaults, hiding advanced settings behind hard to see links, and pre-selecting checkboxes that activate data collection". (UTZ, Christine; DEGELING, Martin; FAHL, Sascha; SCHAUB, Florian; HOLTZ, Thorsten. (Un)informed consent: studying GDPR consent notices in the field. *In*: 2019 ACM SIGSAC **Conference on Computer and Communications Security (CC' 19)**, November 11-15, 2019, London, United Kingdom. ACM, New York, NY, USA. Disponível em: <https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentichungen/2019/09/05/uninfomed-consent_Yl7FPEh.pdf>. Acesso em: 20 jul. 2020)

395 "O princípio da finalidade determina que toda atividade de tratamento de dados deve se basear em um propósito 'especifico e explícito', mesmo nos casos em que a base legal seja uma das outras nove hipóteses autorizativas. Faz parte de toda a lógica do sistema da LGPD especificar a razão pela qual se faz uso de um dado". (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 186)

396 Art. 5º Para os fins desta Lei, considera-se: [...] VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

397 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 186.

as adjetivações dadas ao consentimento, ao mencionar de forma expressa a ideia de granularidade e da finalidade específica ao dispor que:

> (...)Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

Cumpre ainda, uma breve menção do Caso Cambridge Analytica, que atuou como maior incentivo para a regulamentação de dados na União Europeia, demonstrando de forma clara o porquê da menção expressa de tal princípio no art. 6º da LGPD. No referido caso, no que pese os indivíduos terem consentido com o tratamento de dados pelo aplicativo *thisismydigitallife,* jamais anuíram quanto ao repasse das suas informações pessoais a terceiros[398]. Neste ponto, o princípio da finalidade estabelece os limites da legalidade no tratamento de dados, pois delimita a realização do tratamento lícito ao motivo que fundamentou essa coleta. Ou seja, proíbe o tratamento posterior de forma incompatível com os propósitos[399] que foram previstas anteriormente[400] e os quais motivaram o consentimento do titular.

Portanto, quando o consentimento é requerido, caso haja uma mudança da finalidade do tratamento, para que este seja válido, o titular tem que consentir novamente, podendo, inclusive, revogar o consentimento caso não esteja de acordo com as alterações. Eventual uso secundário dos dados poderá ocorrer pelo controlador, desde que o tratamento seja compatível com a finalidade original, não havendo a necessidade de comprovação de outro fundamento legal para o tratamento. Caso haja a incompatibilidade entre o uso secundário e o original, deve haver o consentimento adicional do titular em relação ao novo propósito.

---

[398] HERN, Alex. Facebook agrees to pay fine over Cambridge Analytica scandal. **The Guardian.** 30 out. 2019. Disponível em: https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal. Acesso em: 04 jul. 2020.

[399] Os propósitos previstos no princípio da finalidade são os mesmos da Opinion 03/2013 e em seu art. 29 foram definidos. A legitimidade do tratamento é conceituada como um requisito amplo, que não só se estende a outras áreas do direito, mas que também deve ser interpretada caso a caso. Um tratamento específico é aquele definido de forma precisa ao titular previamente à realização do processamento, sendo possível identificar se a atuação dos controladores está dentro do propósito apresentado. Por fim, um tratamento realizado de forma explícita é necessário que o motivo seja revelado de forma clara, fornecendo um entendimento inequívoco e evitando interpretações distintas entre os envolvidos. Há, por fim, assim como o disposto no art. 9º, incisos I e IV da LGPD, a necessidade de que o titular seja informado sobre todas estas características que compõem os propósitos do princípio da finalidade.

[400] "Como não há possibilidade de tratamento posterior de forma incompatível com as finalidades previamente previstas, é de crucial relevância que os controladores avaliem, desde a concepção do projeto que envolva a coleta de dados, os propósitos específicos que almejam, pois tais propósitos servirão, ao longo do ciclo de transparência perante o usuário e também dos deveres de lealdade ao tratamento, como fronteira de legalidade para o seu uso". (VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 13)

Via de regra, este instituto pode ser visualizado nas relações diretas entre o titular e os agentes de tratamento quando o titular aceita os termos de usos e políticas de privacidade nos *sites*, por exemplo. Porém, também é possível a utilização do consentimento como uma base legal de tratamento através da relação entre o titular e o controlador que trata os dados que foram repassados a ele pelo primeiro controlador, sendo este com quem o titular teve uma relação direta. Neste sentido, desde que o primeiro controlador obtenha consentimento do específico do titular para o compartilhamento ou comunicação dos dados (o §5º do art. 7º da LGPD[401]) , não haverá a necessidade do segundo controlador fundamentar o tratamento em uma nova base legal, podendo utilizar o consentimento obtido com o primeiro controlador para tal. Para Marcel Leonardi, diante dos múltiplos cenários de compartilhamento de dados, é praticamente inviável a obtenção do consentimento para todos os tratamentos futuros pelo primeiro controlador. Sendo assim, entende ser necessário que os demais controladores avaliem a possibilidade de utilização das outras bases legais para legitimar o seu tratamento[402].

No que se refere à adjetivação do consentimento, observa-se, das características utilizadas pelo legislador para validar o consentimento na LGPD, a sua relação com a ideia da declaração da vontade livre e consciente extraída do Código Civil no tema dos defeitos do negócio jurídico[403]. E, portanto, a partir do momento em que estes requisitos não estão presentes, configura-se o "vício de consentimento", decorrendo daí a possibilidade de anulabilidade do negócio jurídico[404]. Diante da LGPD, no §3º do art. 8º fazer menção expressa à vedação do vício de consentimento, nos exatos mesmos termos do Código Civil, sob o ponto de vista de Bruno Ricardo Bioni, "é muito provável que haja um diálogo com o Código Civil brasileiro para se interpretar toda a adjetivação do consentimento à luz dos defeitos do negócio jurídico[405]".

---

[401] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] §5º: O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[402] LEONARDI, Marcel. **Principais bases legais de tratamento de dados pessoais no setor privado.** São Paulo: Editora Revista dos Tribunais, 2019, p. 76.

[403] THEODORO JUNIOR, Humberto. **Comentários ao novo Código Civil:** dos defeitos do negócio jurídico. Rio de Janeiro: Editora Saraiva, 2013, p. 04.

[404] MONTEIRO, Washington de Barros. **Curso de Direito Civil:** parte geral. Vol. 01. São Paulo: Editora Saraiva, 2012, p. 242.

[405] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 179.

Ao decorrer da análise das adjetivações do consentimento, é notório que o legislador se preocupou, diferentemente da maioria das outras bases legais[406], em criar um regramento específico ao decorrer dos artigos 7º a 9º para orientar e solidificar o controle de dados pessoais através do consentimento. Isso pode ser visto ao ponto em que menciona expressamente as hipóteses de nulidade do consentimento quando representar uma autorização genérica[407], bem como quando as informações que foram fornecidas ao titular possuam conteúdo enganoso, abusivo ou que não tenham sido apresentadas com transparência. Principalmente, diante do fato de que mesmo nas hipóteses de dispensa do consentimento, os agentes de tratamento devem observar os princípios e direitos do titular previstos na LGPD[408], e assim, garante-se ao titular de dados o direito de se opor ao tratamento de seus dados em caso de descumprimento da Lei[409]. Neste ponto, Bruno Bioni se refere à uma possível disputa interpretativa da LGPD ao questionar como, nos casos da aplicação das hipóteses de dispensa do consentimento, qual sejam, as outro nove hipóteses previstas no art. 7º da Lei, será assegurado ao titular a transparência para basear a sua vontade por meio do consentimento, mesmo que posteriormente[410].

---

406 Com exceção do legítimo interesse e do tratamento de dados pelo poder público, regulados pelos art. 10 e pelo Capítulo IV, respectivamente.

407 Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. [...] § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

408 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

409 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

410 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 129.

4.3.1.1 O consentimento específico

De forma semelhante à legislação italiana que se refere a quatro tipos consentimentos[411], o legislador brasileiro se preocupou em regulamentar de forma distinta do modelo de consentimento analisado acima, o tratamento de dados pessoais sensíveis[412], de crianças[413], na transferência internacional de dados pessoais para países com nível inferior de proteção de dados pessoais[414], bem como nos casos em que há a participação de terceiros de forma indireta no tratamento de dados[415]. Apesar das particularidades normativas de cada um destes casos, há um ponto em comum que se relaciona a uma maior carga participativa dos titulares de dados: a necessidade do consentimento específico. Trata-se, no entanto, de um requisito adicional, devendo também ser observados o consentimento livre, inequívoco e informado. Com exceção da hipótese regulada pelo Art. 7º, § 5º, da LGPD, há também a necessidade de o consentimento ser destacado.

Tais requisitos adicionais visam à obtenção de uma maior proteção, seja por conta da natureza sensível do dado coletado, da condição de vulnerabilidade dos titulares (crianças e adolescentes) ou até mesmo pela atipicidade/risco anormal da situação, como é o caso da transferência internacional de dados para país sem o mesmo nível de proteção previsto na

---

411 No direito italiano, o consentimento se divide em quatro hipóteses divergentes e por isso, a doutrina italiana se refere a "consentimentos": a) o consentimento documentado por escrito; b) o consentimento por escrito acompanhado da autorização do titular de dados para o tratamento de dados sensíveis; c) o consentimento expresso para a comunicação e a divulgação o dos dados pessoais; e d) o consentimento expresso para a transferência internacional de dados pessoais. (CARBONE, Vicenzo**.** ***Il consenso, anzi i consensi, nel tratamento informático dei dati personali. Danno e responsabilità,*** n.1, 1998, p. 23-29)

412 Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

413 Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

414 Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: [...] VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

415 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

LGPD. Entende-se como consentimento específico quando "manifestado em relação a propósitos claramente determinados pelo controlador, anteriormente ao procedimento de coleta de dados pessoais[416]" Já o consentimento destacado, se refere à necessidade do trecho relativo ao tratamento de dados ser destacado, seja pela diferença na fonte (negrito e sublinhado, por exemplo), pelo uso de caixa alta, dentre outros. O acréscimo da necessidade de um consentimento destacado consequentemente influencia na atuação dos agentes de tratamento, que devem ter ainda mais cautela ao obter o consentimento do titular de dados sensíveis.

Vale-se frisar que, diferentemente do GDPR e do próprio Marco Civil da Internet[417], a LGPD utilizou o termo "específico" ao invés de "expresso". Percebe-se, neste sentido, apesar e ambas as adjetivações dadas ao consentimento motivarem uma maior carga participativa do titular, há certa redundância no termo escolhido pelo legislador brasileiro, uma vez que o consentimento, tendo em vista o princípio da finalidade, já deve ser direcionado a propósito específico/" finalidades determinadas". Portanto, não resta claro a relação dessa adjetivação a mais com uma maior proteção ao titular de dados pessoais. Conforme entende Bruno R. Bioni, a solução para tal desafio interpretativo se refere à garantia de um processo de deliberação extremamente visível e não apenas inequívoco:

> Uma das maneiras de extrair essa carga participativa maior do titular dos dados seria adotar mecanismos que chamassem mais a sua atenção. Deve haver uma alerta que isole não só o dever-direito de informação, como, também, a declaração de vontade, colocando-a à situação na qual é exigido o consentimento específico. Isso vai muito além de cláusulas contratuais destacadas que já são mencionadas como uma forma de obter o consentimento trivial e não específico. Todo o processo de tomada de decisão é (com o perdão de ser prolixo) específico e deve ser pontual. Da informação até o aceite do titular do dado[418].

Neste seguimento, o consentimento específico demanda uma maior analise de todo o grau de interação do titular em todo o processo que o leva a consentir com o tratamento de seus dados pessoais. Além do mais, diante das particularidades dos riscos de cada uma das situações mencionadas acima que necessitam de consentimento específico, apesar do legislador não mencionar as variações de acordo com cada um dos casos, é inegável que cada uma das

---

[416] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 198.

[417] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; (BRASIL. **Lei nº 12.965,** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2020)

[418] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 189.

quatro situações mencionadas acima possui elementos bastante distintos. Como exemplo, de forma geral, há presença de um maior risco na transferência internacional para país com baixo nível de proteção de dados do que o mero compartilhamento de dados. Assim, em todas as situações, será necessária uma análise minuciosa do grau e da qualidade do ato de declaração de vontade exercido, que poderá ser considerado adequado de diversas formas, como através de uma verificação dupla do consentimento, imagens, combinação de imagens com textos, dentre outras possibilidades[419].

4.3.2 Da revogabilidade do consentimento

Demonstrando a relação intrínseca do consentimento com a proteção de dados e, portanto, da própria personalidade, conforme já analisado no decorrer do Capítulo 2 deste Trabalho, o legislador propõe a sua revogabilidade. A sua caracterização como um ato jurídico unilateral, que deve demonstrar de forma genuína a real vontade do titular de dados, consequentemente reforça a ideia de revogabilidade. Cumpre observar que, a partir da revogabilidade, há uma imediata modificação na esfera jurídica do agente de tratamento, que até então estava legitimado ao tratamento de dados pessoais. No entanto, no exercício deste direito, o titular de dados não está sujeito aos efeitos vinculantes das obrigações, não podendo o ato de revogabilidade ser associado a qualquer tipo de inadimplemento. Para Danilo Doneda, quando caracterizada a revogabilidade do consentimento nos termos do artigo 8º, §6º da LGPD, o interesse do agente de tratamento também merece ser considerado, cabendo, inclusive, em caso de eventual conduta abusiva do titular de dados, a reparação:

> A eventual conduta abusiva de quem revoga o consentimento pode ensejar um dever de reparação, uma vez que essa conduta caracterize dano a quem anteriormente teria recebido a autorização para tratar os dados pessoais dessa pessoa. (...) A verificação da abusividade dessa conduta estaria a cargo do intérprete que poderia, no caso, guiar-se por mecanismos como o do abuso de direito ou, de forma mais específica, do *venire contra factum proprium.* Em todo caso, ressalte-se a necessidade do intérprete utilizar os critérios de proporcionalidade nessa verificação, de forma a não tornar essa possibilidade de revogação uma alternativa que se revele de fato inacessível por implicar custos demasiados altos como consequência, o que afrontaria a natureza dos interesses em questão. [420]

[419] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 190.
[420] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 205.

O legislador, na intenção de privilegiar o poder de autodeterminação do titular de dados, prevê no §6º do art. 8º da LGPD, o direito do indivíduo revogar o ato pelo qual anteriormente consentiu quando houver uma alteração das informações presentes nos incisos I, II, III ou V do art. 9º da Lei e discorde de tal alteração. Portanto, não se trata de uma revogabilidade incondicional. As modificações que podem embasar o direito de revogabilidade do titular de dados se limitam à: finalidade do tratamento dos dados; à forma e duração do tratamento; à identificação do controlador ou às informações relacionadas ao uso compartilhado de dados pelo controlador. No caso da comunicação ou compartilhamento de dados tratados em conformidade com o inciso I do art. 7º, com exceção do tratamento pautado nas demais bases legais, novo consentimento será requerido (§5º do art. 7º, da LGPD).

Caso o controlador informe ao titular acerca das alterações e ele concorde com elas, não haverá a necessidade de um novo consentimento. Reiterando a ideia de transparência no processo de tratamento de dados, o legislador prevê também, neste mesmo processo, a necessidade de destacar as eventuais alterações como mecanismo para garantir a completa compreensão por parte do titular de dados. Cumpre lembrar que, ao controlador cabe o ônus da prova da regularidade do consentimento conforme os ditames da Lei e, portanto, todas as evidências capazes de comprovar a efetivação do referido procedimento devem ser armazenadas. O Art. 9º, §2º também menciona o direito de revogabilidade do consentimento na mesma lógica do art. 8º, §6º da LGPD, mas, especificamente no caso de mudança da finalidade original do tratamento[421]. Portanto, nas hipóteses em que o consentimento é requerido e o titular de dados não concorda com a nova situação proposta, a Lei garante a possibilidade de que o revogue.

4.3.3 Do encerramento do tratamento de dados pessoais

A Seção IV do Capítulo II da LGPD se preocupa em definir, de forma específica e taxativa, as hipóteses nas quais ocorrerá o término do tratamento de dados. Neste aspecto, cumpre lembrar

[421] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...] § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

que, a proteção da LGPD engloba todo o ciclo de vida do dado pessoal, que se encerra com o descarte. Neste aspecto, o término do tratamento enseja a eliminação do dado pessoal da base do agente de tratamento e, portanto, quando configurada alguma das hipóteses previstas nos incisos do art. 15 da Lei, a eliminação deve ocorrer de forma automática, não havendo a necessidade de qualquer pedido por parte do titular de dados. No entanto, cumpre observar que, logo em seguida, em seu art. 16, a LGPD prevê as exceções ao término do tratamento.

Assim, quatro hipóteses taxativas configuram o término do tratamento de dados pessoais: quando a finalidade do tratamento de dados foi alcançada ou quando os dados não são mais necessários/pertinentes para o alcance de tal finalidade; nos casos em que foi especificado o período de guarda dos dados e este foi alcançado e por determinação da ANPD em caso de violação da LGPD. Percebe-se que, o inciso IV do art. 15 acaba se relacionando de forma direta com o fortalecimento do instituto do consentimento, pois, caso o agente de tratamento não aja em conformidade com tudo que foi mencionado no decorrer dos tópicos 4.3.1 e 4.3.2, a Autoridade Nacional de Proteção de Dados poderá determinar que o agente de tratamento elimine os dados da sua base, sendo, inclusive, uma das sanções administrativas previstas na Lei[422]. Vale-se ressaltar que, ao agente de tratamento é dada a oportunidade de comprovar a licitude no referido tratamento de dados.

Por último e mais importante na análise do arcabouço legal do consentimento, o inciso III do art. 15 define como hipótese que configura o término de tratamento quando houver a expressa solicitação do titular de dados neste sentido. Assim, o agente de tratamento estará obrigado por lei a atender tal pedido do titular de dados, ressalvando os casos de manutenção previstos no art. 16 da Lei. Relacionando este direito de exclusão dos seus dados de determinada base de tratamento ao direito da revogabilidade, o legislador menciona expressamente o §5º do art. 8º da LGPD: “comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no §5º do art. 8º desta Lei, resguardado o interesse público”. A utilização do termo “inclusive” para fazer referência à revogabilidade do consentimento demonstra que o legislador apenas exemplificou uma das hipóteses, não sendo, portanto, a configuração do término de tratamento por comunicação do titular decorrente da revogação do consentimento. Este, inclusive, é o entendimento de Caio César C. Lima:

[422] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...] VI - eliminação dos dados pessoais a que se refere a infração; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

> Nesse ponto, expomos o nosso entendimento de que a mera revogação do consentimento, se não for seguida de expressa solicitação de exclusão dos dados, autorizará a manutenção desses dados pessoais, ratificados ao tratamento até então realizados, conforme disposto no §5º do artigo 8º. Assim, nos casos de revogação do consentimento, a eliminação dos dados pessoais somente será processada, quando houver pedido direto para tanto, não se tratando de consequência direta e imediata do exercício do direito de revogação[423].

As hipóteses de autorização da conservação previstas no art. 16 da Lei atuam como limite ao direito do titular previsto no inciso III do art. 15, bem como de todos os outros três incisos. O caput do art. 16 reitera o fato de que os dados pessoais serão automaticamente eliminados quando configurada alguma das situações presentes nos incisos do art. 15, ou seja, após o término do seu tratamento. Em seguida, se refere à conservação dos dados pessoais, mesmo a situação se enquadrando nas situações de término do tratamento, para as seguintes finalidades: cumprimento de qualquer obrigação legal (estadual, municipal ou federal) ou regulatória pelo controlador; estudo por órgão de pesquisa; quando subsistir motivação para a retenção dos dados para posterior transferência a terceiros ou por uso exclusivo do controlador, desde que os dados passem pelo processo de anonimização nos termos do art. 12 da Lei.

No que se refere ao disposto no inciso I do art 16, qual seja, o cumprimento de obrigação legal ou regulatória pelo controlador, entende-se que, mesmo o legislador apenas se referindo ao controlador na redação de tal inciso, quando o operador se encontrar em situação semelhante a do controlador, ele poderá se utilizar deste inciso para manter os dados com objetivo de cumprimento de obrigações legais. Cumpre também observar que, deve o controlador, nos casos de retenção dos dados com base em determinações previstas em legislação internacional, analisar os riscos que podem advir do não cumprimento de tais previsões[424]. Diferentemente da retenção de dados para o estudo de órgãos de pesquisa, que é recomendada a anonimização dos dados pessoais (inciso II), na situação de uso exclusivo do controlador, além de ser vedado o acesso por terceiro, o controlador apenas pode socorrer a este inciso desde que submeta os dados pessoais ao processo de anonimização. Neste ponto, pode o controlador, com base no fato de que os dados anonimizados não estão originariamente sob o escopo de proteção da LGPD, sustentar acerca da possibilidade de acesso por terceiros, desde que sejam respeitados os requisitos dispostos na Lei, especialmente o previsto no *caput* do art. 12[425]. Portanto, de forma resumida, conclui-se que

---

[423] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 212.
[424] LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 213.
[425] 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

os agentes de tratamento mencionados em cada inciso poderão manter os dados, desde que com o objetivo específico de atender as referidas obrigações.

4.4 O TRATAMENTO IRREGULAR E A CARACTERIZAÇÃO DA RESPONSABILIDADE DOS AGENTES DE TRATAMENTO

Da própria natureza do instituto da responsabilidade, tanto civil, quanto administrativa, é notório o seu papel limitador da atividade dos agentes de tratamento, seja pelo impacto causado no setor financeiro das empresas, os altos custos de remediação ou até mesmo o impacto negativo na sua reputação, tendo em vista o valor da proteção de dados na atualidade. Assim, mesmo não estando a sua configuração limitada às infrações legais relacionadas ao consentimento do titular de dados, acaba sendo uma fonte auxiliar no fortalecimento do titular de dados por meio de uma maior rigidez ao cumprimento do regime jurídico dado consentimento na LGPD. A título de exemplo, qualquer utilização de dados com finalidade diversa daquela a qual o titular autorizou, bem como a ausência de comprovação efetiva do consentimento inequívoco, podem resultar na responsabilização administrativa dos agentes de tratamento, nos termos do art. 52 a 54 da Lei e, na presença da configuração de dano decorrente deste tratamento irregular ao titular de dados, estarão os agentes passíveis a receberem as sanções civis.

Corroborando com tal ideia, cumpre, logo de início, a análise da emblemática sanção de €50 milhões aplicada pela Autoria Nacional de Proteção de Dados Francesa (CNIL) à plataforma do Google, diante da inobservância da garantia das previsões legais relacionadas ao consentimento (adjetivações). Em tal caso, o consentimento foi considerado nulo por diversos motivos, dentre eles: a ausência da transparência necessária aos usuários; a diluição do processo de personalização de anúncios em diversos documentos, dificultando a compreensão por parte do titular; pluralidade de serviços que impossibilitavam o usuário de exercer o seu direito a um consentimento específico e inequívoco e incompatibilidade do princípio da finalidade com a necessidade de marcação de caixas de “eu concordo” genéricas, onde o

---

quando, com esforços razoáveis, puder ser revertido. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

titular consente de forma integral para todos os tipos de tratamento efetuados pela referida plataforma[426].

Percebe-se, das considerações feitas pela CNIL, a existência de uma intrínseca relação entre a responsabilidade, que no caso foi administrativa e a regulação do instituto do consentimento.

No contexto brasileiro, a inobservância da legislação, caracterizada, por exemplo, pelo não cumprimento das garantias que devem ser dadas ao referido instituto nos termos do art. 7º ao 9º da LGPD, bem como todas as obrigações dos agentes de tratamento que foram analisadas ao decorrer do Capítulo 3 deste Trabalho, configura o tratamento irregular de dados. Este tema é abordado pelo art. 44 da LGPD, que em seus incisos introduz quais circunstâncias serão levadas em consideração para analisar a regularidade da atividade de tratamento de dados pessoais, estando todas as três circunstâncias relacionadas ao avanço tecnológico de determinada época[427]. Neste sentido, sempre que o controlador ou o operador, em razão do exercício da atividade de tratamento de dados pessoais causarem dano ao titular destes dados, em violação à LGPD[428] ou decorrentes da violação da segurança dos dados[429], responderá pelos danos. A presença do instituto da responsabilidade civil, portanto, está diretamente relacionada ao tratamento irregular de dados, sob os temos do art. 44 da Lei.

Destarte, o legislador utiliza-se de técnicas cíveis e administrativas para garantir quando resta configurado o dano decorrente do tratamento de dados. Ou seja, tanto em descumprimento dos procedimentos para a proteção de dados ou das bases legais, os agentes de tratamento estarão sujeitos à indenização civil e às sanções administrativas. Diferentemente do instituto

---

[426] COMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.** 21 jan. 2019. Disponível em: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Acesso em: 20 jul. 2020.

[427] 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: 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[428] 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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[429] 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. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

da responsabilidade civil, que se preocupa com a reparação, as sanções administrativas objetivam a inibição do comportamento vedado através da fiscalização pela Autoridade Nacional de Proteção de Dados Pessoais, sendo este o tema abordado na Seção I do Capítulo VIII da LGPD ("Da Fiscalização - Das sanções Administrativas"). O exercício do poder fiscalizatório, por exemplo, é configurado por meio da aplicação de diversas penalidades administrativas, dentre elas, destacam-se as advertências[430] e multas, essas de até 2% da receita anual da empresa, limitando-se ao valor de 50 milhões por infração[431].

4.4.1 Da responsabilidade civil

O legislador, indo de encontro com a necessidade de equilibrar a relação entre os agentes de tratamento e os titulares de dados pessoais, não só estabeleceu diversas regras para ordenar o tratamento, mas também se preocupou em relacionar à violação destas regras à responsabilidade civil quando a atividade de tratamento importar em danos aos titulares[432]. Desta forma, o art. 42 da LGPD prevê a responsabilidade quando da violação à legislação, tanto dos controladores, quanto dos operadores e indica, de forma clara, a possibilidade de reparação do dano patrimonial, moral, individual ou coletivo. A fim de assegurar a efetiva indenização ao titular de dados, a LGPD aponta a aplicação da responsabilidade solidária[433] (art. 42, §1º), nos seguintes termos:

> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:

---

[430] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[431] Art. 52. [...] II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[432] "A responsabilidade civil em matéria de dados pessoais é primordial para o equilíbrio das relações dessa natureza, sobretudo quando envolvida a tecnologia. A título exemplificativo, uma rápida busca por um tema específico na Internet poderá rapidamente retornar uma enorme base de dados. Mais do que isso, essa pesquisa, ou o acesso a um site, poderá iniciar ou alimentar um infindável perfil sobre as preferências e interesses daquele usuário da rede, alimentando algoritmos e outras tecnologias preditivas a respeito do comportamento do usuário, com massivo tratamento de dados pessoais envolvido. (BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019, p. 319)

[433] A solidariedade é regulada pelo Código Civil em seu art.264, fazendo menção à relação entre credor e devedor: Há solidariedade, quando na mesma obrigação concorre mais de um credor, ou mais de um devedor, cada um com direito, ou obrigado, à dívida toda.

> 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;
>
> 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.

Percebe-se, da leitura destes incisos, que o legislador relaciona a responsabilização solidária do operador ao descumprimento da lei e das ordens lícitas do controlador. Ou seja, demonstra que mesmo que a atuação do operador esteja subordinada a tais ordens dadas pelo controlador, não deve o operador apenas e cumprir com essas instruções, sendo também seu dever conhecer as normas relacionadas à proteção de dados pessoais. Ainda, diante da possibilidade de envolvimento de mais de um controlador no processo de tratamento de dados, o inciso II do §1º do art. 42 facilita o controle por parte do titular de dados, pois não seria razoável determinar que o titular descobrisse quem, dentro de uma organização empresarial, deu causa ao dano sofrido.

Mario Toews[434] traz à tona situação que exemplifica perfeitamente o instituto da responsabilidade solidária e o direito de regresso àquele que reparou o dano (controlador ou operador) previsto no §4º do art. 42 da LGPD. Se refere ao recente caso de vazamento de dados de diversos sócios torcedores de um grande clube de futebol através de falha no sistema do *FutubolCard,* site que realiza as vendas de ingressos do programa de fidelidade aos sócios torcedores[435]. Neste caso, conforme definição dada pela LGPD, na relação de tratamento de dados, o time se configura como o controlador e o site vendas como o operador. Sob a aplicação do inciso I do §1º deste mesmo artigo, ambos os agentes de tratamento seriam responsáveis pela reparação de dados aos titulares, mesmo diante do vazamento de dados ter se dado por falha no site do *FutebolCard.* Nas palavras de Marcos G. da Silva Bruno, tal inciso "pode ser importante mitigador de responsabilidade ao controlador, no caso de culpa do operador[436]".

---

[434] TOEWS, Mario. LGPD, responsabilidade solidária e ações regressivas. **IT Forum 365 – a voz da TI.** 02 abr. 2020. Disponível em: https://itforum365.com.br/colunas/lgpd-responsabilidade-solidaria-e-acoes-regressivas/#:~:text=Esse%20%C3%A9%20um%20caso%20de,Prote%C3%A7%C3%A3o%20de%20Dados%20(LGPD).&text=No%20par%C3%A1grafo%204%C2%BA%2C%20estabelece%20o,%C3%A0%20responsabiliza%C3%A7%C3%A3o%20e%20%C3%A0%20indeniza%C3%A7%C3%A3o.. Acesso em: 24 jun. 2020.

[435] GLOBO ESPORTE. **Palmeiras admite vazamento de dados de sócios e aponta falha da FutebolCard**. 05 fev. 2020. Disponível em: https://globoesporte.globo.com/futebol/times/palmeiras/noticia/palmeiras-admite-vazamento-de-dados-de-socios-e-aponta-falha-da-futebolcard.ghtml. Acesso em: 24 jun. 2020.

[436] BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019, p. 323.

No decorrer do processo civil, poderá o juiz inverter o ônus da prova em favor do titular de dados. Cumpre lembrar que, a distribuição do ônus da prova nos termos do Código de Processo Civil é realizada do seguinte modo: "ao autor, quanto ao fato constitutivo de seu direito" e "ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor[437]". Contudo, o próprio §2º do art. 42, que prevê tal possibilidade, estabelece também as suas hipóteses de aplicação, limitando-se à verossimilhança da alegação, hipossuficiência para fins de produção de prova, bem como a onerosidade excessiva da produção de provas. Ainda, no caso de dano coletivo resultado de violação da referida legislação, é possível que tal reparação seja cobrada coletivamente em juízo (art. 42, §3º).

4.4.1.1 As excludentes de responsabilidade

O art. 43 da LGPD, de forma bastante objetiva, como pode se concluir da linguagem utilizada e das hipóteses aplicáveis, traz quando os agentes de tratamento não serão responsabilizados. A sua estrutura é caracterizada por apenas três incisos, todos eles estando sujeitos à prova por parte dos agentes de tratamento. O primeiro deles diz respeito à inexistência do nexo de causalidade entre a conduta e o dano, ou seja, a não realização do o tratamento de dados pessoais que lhes é atribuído. Apesar desta hipótese de excludente de responsabilidade parecer óbvia, é muito comum o titular, diante da complexidade da atividade de tratamento de dados pessoais, demande a empresa incorreta[438]. Neste sentido, o legislador, já prevendo este ser um problema recorrente diante de tal complexidade, dispõe em seu art. 42 sobre a responsabilidade solidária dos agentes.

De forma completamente oposta, o legislador prevê no inciso II do art. 43 que, mesmo na existência do nexo de causalidade entre a conduta e o dano, se o agente de tratamento provar que agiu em conformidade com as obrigações impostas pela lei, não será responsabilizado. No entanto, ao ponto em que afasta a ilicitude do ato, consequentemente afasta o dever de indenizar. Trata-se, ainda, de uma comprovação ampla, devendo tal agente demonstrar que

---

[437] Art. 373. O ônus da prova incumbe: I - ao autor, quanto ao fato constitutivo de seu direito; II - ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor. (BRASIL. **Lei nº 13.105,** de 16 de março de 2015. Código de Processo Civil. Brasília, DF. 16 mar. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 maio. 2020)

[438] O Inquérito Civil Público 08190.052296/18-50 ilustra perfeitamente a situação relatada ao fundamentar o seu arquivamento no fato de que "os dados pessoais supostamente obtidos durante o ataque são oriundos de outra fonte.

tomou as medidas de segurança recomendadas, cumpriu com as normas estabelecidas internamente, procedimentos, padrões técnicos, dentre outros[439].

O terceiro e último inciso do art. 43, assim como o inciso I deste mesmo artigo, afasta o nexo causal entre a conduta do agente e o dano, ao ponto em que se refere à culpa exclusiva do titular dos dados ou de terceiros. Portanto, ao ponto em que a conduta da vítima ou de terceiro "anula" todo a atuação do agente de tratamento, pode-se dizer que, a operação realizada por tal agente caracterizará apenas como ferramenta na produção do evento danoso[440].A respeito da aplicabilidade deste inciso, Marcos G. da Silva Bruno[441] traz interessante discussão acerca da culpa de terceiro nos casos em que resta configurado determinada invasão de um sistema por agente não autorizado. Nas palavras do autor, "nunca se pode esperar uma absoluta segurança em sistemas informáticos". No entanto, espera-se do agente de tratamento que adote as melhores técnicas para garantir a segurança dos dados pessoais que se encontram em sua base. Neste caso, sendo até este o fundamento utilizado pelo TJSP em decisão[442], se a invasão se concretizou porque o terceiro utilizou táticas inovadoras, as quais o agente de tratamento, mesmo com a utilização de sistemas efetivamente seguros, não tinha como garantir a proteção de dados, é admitida a excludente de responsabilidade por fato de terceiro.

4.4.1.2 A natureza da responsabilidade civil na LGPD

Por não prever de forma clara a respeito da natureza da responsabilidade aplicável ao tema, o legislador abriu espaço para uma série de controvérsias acerca da aplicabilidade da responsabilidade subjetiva ou da responsabilidade objetiva aos agentes de tratamento. Autores reconhecidos no campo do Direito Digital, como Danilo Doneda e Leonardo Henrique de Carvalho, defendem, com base em analogias com o Código de Defesa do Consumidor, que a

---

[439] GUEDES, Gisela Sampaio da Cruz. **Regime de Responsabilidade adotado pela lei de proteção de dados brasileira.** São Paulo: Editora Revista dos Tribunais, 2019, p. 179.

[440] "A expressão 'culpa exclusiva da vítima' é imprópria, sobretudo, porque confunde dois elementos da responsabilidade civil absolutamente distintos: culpa e nexo causal. Quando ocorre 'culpa exclusiva da vítima', a responsabilidade do agente é afastada por falta de nexo causal entre a sua conduta e o dano". (LLAMBÍAS, Jorge Joaquín. **Tratado de derecho civil.** Tomo III. Buenos Aires: Editorial Perrot, 1973, p. 718)

[441] BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019, p. 325.

[442] "Não se pode fechar os olhos a uma dura e triste realidade: os sistemas computacionais não são 100% indevassáveis. Aí estão os hackers para demonstrar que a muralha digital, inclusive aquela erguida nos grandes centros tecnológicos mundiais, ostenta um certo grau de vulnerabilidade." (BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível nº 108339-32.2015.8.26.0100. Relator: Desembargador Antonio Nasciento. Data de julgamento: 25 ago. 2016)

LGPD adotou o modelo de responsabilidade objetiva. O CDC, ao decorrer de seus artigos 12 a 14[443], se refere claramente à possibilidade de responsabilização objetiva de forma ampla, ou seja, de toda a cadeia de consumo de consumo e de serviço. Neste sentido, dentre os artigos da LGPD que foram inspirados no CDC[444], destaca-se a semelhança do art. 43 da LGPD com o art. 12, §3º do CDC[445], tornando-se extremamente compreensível a referida analogia utilizada para sustentar a aplicação da responsabilidade objetiva aos agentes de tratamento de dados pessoais.

Essa parte da doutrina também sustenta que o risco é elemento intrínseco da atividade de tratamento de dados[446], corroborando com a ideia da teoria do risco extraída das relações

---

[443] Art. 12: O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. (BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção ao consumidor e dá outras providências. Brasília, DF. 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2020)
Art. 13: O comerciante é igualmente responsável, nos termos do artigo anterior, quando: I - o fabricante, o construtor, o produtor ou o importador não puderem ser identificados; II - o produto for fornecido sem identificação clara do seu fabricante, produtor, construtor ou importador; III - não conservar adequadamente os produtos perecíveis. Parágrafo único. Aquele que efetivar o pagamento ao prejudicado poderá exercer o direito de regresso contra os demais responsáveis, segundo sua participação na causação do evento danoso. (BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção ao consumidor e dá outras providências. Brasília, DF. 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2020)
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. (BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção ao consumidor e dá outras providências. Brasília, DF. 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2020)

[444] 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. [...] § 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. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

[445] Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. [...] § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: (BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção ao consumidor e dá outras providências. Brasília, DF. 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2020)

[446] "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 àqueles que sejam, 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

consumeristas. Com base em tal teoria, a configuração da responsabilidade objetiva do agente de tratamento se dá em razão do próprio risco da atividade exercida. Vale ressaltar a existência de diversas extensões de tal teoria, como exemplo da teoria do risco integral, administrativo, proveito e criado. Dentre elas, destaca-se a teoria do risco integral, na qual é aplicada a responsabilidade independentemente de ter sido a vítima quem deu causa dano. Diante das excludentes de responsabilidade expressas na LGPD, não seria razoável sustentar a aplicação de tal teoria. No caso do tratamento de dados pessoais, a doutrina se referre à aplicação da teoria do risco do negócio ou da atividade, extraída do CDC. No entanto, não se pode admitir como risco todo tipo de atividade de tratamento de dados pessoais, sob o risco de banalização do instituto[447].

Importante salientar que, no âmbito das relações de consumo, o legislador positivou, de forma bastante clara no art. 45 da LGPD, a aplicação do microssistema consumerista às violações do direito do titular. Ou seja, sempre que o titular de dados pessoais tiver adquirido ou utilizado produto ou serviço como destinatário final, e, portanto, caracterizando-se como consumidor nos termos do art. 2º do CDC[448], tal relação estará sujeita às regras de responsabilidade do próprio CDC (objetiva). Ademais, em seu art. 17, a LGPD garante o direito de equiparação a aqueles que, apesar de não se enquadrarem no conceito de consumidor pelo CDC, sofreram danos em razão do produto ou serviço viciado. Desta forma, possibilita que todas as vítimas do evento, embora não tenham consumido diretamente o produto ou serviço que deu causa ao dano, possam invocar as mesmas garantias do consumidor de fato.

Do outro lado, há os defensores da responsabilidade subjetiva. Assim como aqueles que defendem a ausência da necessidade da culpa como fundamento do regime estabelecido pela LGPD, há diversos autores com destaque na área do Direito Digital que entendem de forma oposta, como Marcos Gomes da Silva Bruno[449], Márcio Cots[450] e Leonardo Corrêa[451],

---

do risco, levando-se em conta que o tratamento de dados apresenta risco intrínseco aos seus titulares". (MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados.** São Paulo: Editora Revista dos Tribunais, 2019, p. 473)

[447] BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019, p. 320-321.

[448] Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. (BRASIL. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção ao consumidor e dá outras providências. Brasília, DF. 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2020)

[449] "É possível sustentar que a regra geral da Lei é a da responsabilidade civil subjetiva, no qual o elemento da culpa deverá ser demonstrado". (BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019, p. 323)

demonstrando que, de fato, tal tema gera uma divisão de entendimentos na doutrina brasileira. Solidificando tal posicionamento, a doutrina traz o que, para eles, são diversas pistas na LGPD que lidam para o caminho da responsabilidade subjetiva. De início, sustentam que toda a organização do Capítulo VI, que é dedicado exclusivamente para tratar sobre o tema segurança e boas práticas no processo de tratamento de dados, resulta na criação de um verdadeiro *standard* de conduta a ser seguido pelos agentes de tratamento de dados[452].

Seguindo essa linha de pensamento, Gisela Sampaio da Cruz faz referência à referida criação de um padrão de conduta socialmente esperado pelos agentes de tratamento na LGPD e a sua relação com o instituto da responsabilidade subjetiva:

> Ao criar um verdadeiro *standard* de conduta, a LGPD se aproximou mais do regime de responsabilidade fundado na culpa. Afinal, a noção atual de "culpa" envolve mesmo a análise dos *standards* de conduta socialmente aceitos. Nos últimos tempos, a noção clássica de culpa cedeu lugar para um conceito mais objetivado, que tem sido designado de culpa normativa. A culpa passou a ser analisada a partir da ideia de desvio de conduta, que leva em conta apenas o comportamento exigível diante das especiais circunstâncias do caso concreto. Por outras palavras: significa dizer que não se investiga mais o direcionamento da vontade do agente para o descumprimento da ordem jurídica em termos abstratos, mas sim, a sua adequação (ou não) ao padrão de comportamento esperado naquelas circunstâncias concretas[453].

Fica evidente, ao decorrer deste Trabalho, que o legislador impôs uma de deveres a serem seguidos pelos agentes de tratamento, sob pena de serem responsabilizados. Portanto, essa parte da doutrina entende que, não faria sentido a criação de uma série de deveres se não para a implementação da responsabilidade subjetiva, uma vez que a responsabilização independentemente de culpa retira toda lógica da imposição de deveres a serem seguidos pelos agentes de tratamento. Tendo em vista, principalmente, o "novo" conceito de culpa analisado no trecho acima (culpa normativa[454]), na ocorrência de algum incidente de

---

[450] "A responsabilidade civil dos agentes de tratamento segue a regra geral estabelecida pelos artigos 186, 187 e 927 do Código Civil". (COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** São Paulo: Editora Revista dos Tribunais, 2018, p. 175)

[451] "Com a necessidade de prova técnica sobre o vazamento de dados e suas causas, a boa exegese legal deverá afastar o automatismo da responsabilização objetiva pura, nesse caso. Pois, (...), a verificação da conduta ilícita imporá conhecimento técnico. Sem isso, a diligência pode ser mal compreendida, gerando insegurança jurídica profunda. O anseio da lei é buscar mais segurança aos usuários, mas isso tem de ser balanceado com a realidade do mundo digital. Espera-se, desta feita, que esse tipo de questão seja tratado *cum grano salis.* Caso contrário, a lei criará uma situação de profunda injustiça". (CORRÊA, Leonardo. É importante não perder o foco da segurança jurídica no âmbito da LGPD. **Revista Consultor Jurídico.** 03 mar. 2019. Disponível em: www.conjur.com.br/2019-mar-03/Leonardo-correa-segurança-jurídica-ambito-lgpd. Acesso em: 23 jun. 2020)

[452] GUEDES, Gisela Sampaio da Cruz. **Regime de Responsabilidade adotado pela lei de proteção de dados brasileira.** São Paulo: Editora Revista dos Tribunais, 2019, p. 175.

[453] GUEDES, Gisela Sampaio da Cruz. **Regime de Responsabilidade adotado pela lei de proteção de dados brasileira.** São Paulo: Editora Revista dos Tribunais, 2019, p. 177.

[454] "O conceito de culpa também se encontra em estado de indefinição no atual direito da responsabilidade civil. Originalmente, culpa era apenas a situação contrária ao direito, porque negligente, imprudente, imperita ou dolosa, que acarretava danos aos direitos de outrem. Modernamente, todavia, diversos autores abandonaram esta conceituação, preferindo considerar a culpa o descumprimento de um standard de diligência razoável,

segurança ou irregularidade no tratamento de dados, será analisada a conduta do agente de tratamento no caso concreto e não apenas no plano abstrato. Neste sentido, será objeto de exame não só o dano causado ao titular, mas o posicionamento do agente perante tal incidente, como exemplo, as ações que tomou para evitar ou conter os efeitos dos danos ou até mesmo, quando possível, remediá-los.

A outra pista presente na Lei que, ao entendimento desta parte da doutrina, aponta para o regime da responsabilidade subjetiva, se associa com o inciso II do art. 43. Este dispositivo regula uma das hipóteses de não responsabilização dos agentes de tratamento, e essa, em específico, faz relação direta à ideia da culpa como fundamento da responsabilidade do agente de tratamento ao prever que serão responsabilizados quando provarem "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados". O foco estaria neste inciso, pois, as excludentes reguladas pelos incisos I e III do art. 43 poderiam existir ainda que a LGPD consagrasse a responsabilidade objetiva. Ambas as hipóteses, diferentemente do inciso II, possuem relação com a ideia do nexo de causalidade. Percebe-se que, nos termos do referido inciso, mesmo com a presença do nexo causal entre a conduta do agente e o dano, se o agente provar que em nenhum momento agiu em desconformidade com as normas previstas na LGPD, observando os *standards* de conduta esperados, não será responsabilizado.

Por fim, conclui-se que, ao mesmo tempo em que tais pistas não autorizam, por si só, a conclusão de que o tratamento de dados pessoais estaria sujeito a um regime caracterizado pela responsabilidade subjetiva, a semelhança normativa do tema com o previsto no CDC e a aplicabilidade da teoria do risco também não são suficientes para afirmar que o regime adotado como regra foi o da responsabilidade objetiva. Neste sentido, como também ensina a doutrina, independentemente do regime adotado pela LGPD, é inquestionável que a efetiva demonstração do dano é indispensável para a efetivação de qualquer indenização. É cediço que, sem a presença do dano, o pedido indenizatório do titular não possui fundamento, devendo ainda levar-se em consideração a possibilidade do dano presumido, como exemplo da ocorrência de incidentes de segurança. Importante lembrar que, as situações em que o dano

---

diferenciando esta noção, dita 'normativa' ou 'objetiva', da outra, dita 'psicológica'". (MORAES, Maria C. Bodin de. **Risco, solidariedade e responsabilidade objetiva.** São Paulo: Editora Revista dos Tribunais, 2006, p. 21)

pode ser presumido dever ser analisadas com bastante cautela, para que se possa evitar a banalização de tal instituto[455].

4.4.2 Da responsabilidade administrativa

Diferentemente do instituto da responsabilidade civil, que se preocupa com a reparação, as sanções administrativas objetivam a fiscalização pela Autoridade Nacional de Proteção de Dados Pessoais. Neste ponto, o legislador estabelece a intervenção da atividade estatal de fiscalização em razão das infrações cometidas às normas previstas em lei, após procedimento administrativo que garanta a oportunidade da ampla defesa, devendo ainda ser considerados alguns critérios, como a gravidade da infração, o grau do dano, a boa-fé do infrator, dentre outras[456]. Estes critérios atenuantes e agravantes da atividade sancionatória demonstram que o seu proposito não é ser punitivo e sim pedagógico. Busca-se, com isso, a implementação de instrumentos que possam garantir e proteger a dignidade humana. O exercício do poder fiscalizatório é regido pelo art. 52 da LGPD, se concretizando através da aplicação de diversas penalidades administrativas, nos seguintes termos:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

---

[455] BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019, p. 324.

[456] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...] As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. (BRASIL. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020)

> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Dentre todas as sanções administrativas aplicáveis quando do cometimento de infrações às normas previstas na Lei pelos agentes de tratamento de dados, necessitam ser abordadas de forma mais específica às penalidades pecuniárias, o bloqueio e a eliminação dos dados pessoais objetos da infração. Ambos os incisos II e III se referem à aplicação da penalidade pecuniária de multa. A multa simples, no entanto, deve ser aplicada seguindo alguns parâmetros: o valor de até 2%, limitando-se ao à R$ 50 milhões (por infração[457]); o faturamento no último exercício como base de cálculo (excluídos os tributos) e a limitação do destinatário à pessoa jurídica de direito privado, grupo ou conglomerado no Brasil. Este último parâmetro, sob o olhar de Fabricio da Mota Alves[458], deve ter a sua amplitude protetiva ampliada, abarcando também as pessoas naturais que desenvolvem atividades sujeitas ao escopo da LGPD, pois resta evidente, da distinção projetada no §3º do art. 52 às entidades e órgãos públicos, que o objetivo do legislador é a aplicação da multa pecuniária a todos os destinatários da LGPD, nos termos do seu art. 3º.

No que se refere ao subteto sancionatório de até R$50 milhões, percebe-se que, os únicos que se beneficiam de tal limitação no valor da penalidade pecuniária são os agentes de tratamento com faturamento anual superior a R$ 2,5 bilhões. Ao analisar a extensão do valor das penas pecuniárias em outras leis, a exemplo da Lei 12.529/11 e da Lei 12.965/14, que, respectivamente, limitam as multas aplicáveis às empresas em até 20% do faturamento bruto e em até 10% do faturamento, resta claro que o teto de R$50 milhões previsto na LGPD acaba

---

[457] Referente a incidência da multa simples por infração, Fabricio da Mota Alves faz importante observação: "(....) muito se tem sustentado tratar-se de um risco à atividade econômica dos agentes de tratamento de dados. Isso porque haveria espaço hermenêutico para que a ANPD compreendesse a infração tendo por parâmetro: o número de titulares afetados; o número de incidentes de violação a direitos de proteção de dados; ou o número de disposições e normas violadas na LGPD. Pelo critério da razoabilidade declaradamente previsto no inciso XI do §1º do artigos ora em análise, de se supor que a penalidade não compreenderá uma avaliação singular dos eventos violadores de direitos e obrigações de proteção de dados, mas um conjunto de fatores, tais como ocorrências infratoras, abrangência de titulares de dados afetados, natureza e categoria dos dados pessoais, etc". (ALVES, Fabricio da Mota. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 367)

[458] ALVES, Fabricio da Mota. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 365.

por fragilizar o poder de polícia da ANPD. No entanto, apesar da imposição pecuniária causar grande impacto no setor financeiro de determinada instituição que efetua o tratamento de dados pessoais de forma inadequada, diante do valor que possuí a proteção de dados pessoais para os consumidores na atualidade, estas empresas estarão ainda sujeitas a danos muitos maiores às suas reputações. Além do mais, deve ser levado em consideração os altos custos para a implementação de medidas de remediação.

Com natureza distinta da multa simples, a multa diária atua como instrumento coercitivo para o cumprimento da obrigação imposta. Mesmo com tal divergência, ao ponto em que a multa regulada pelo inciso II do art. 52 é aplicada em razão do cometimento de uma infração, a LGPD optou erroneamente por limitar o valor da multa diária ao mesmo teto estabelecido para a multa simples. Como já reiterado pela jurisprudência pátria em diversos casos, a aplicação de multa que importa em ônus excessivo ao infrator e como consequência, o enriquecimento ilícito ao Estado é caracterizada como ilegal e inconstitucional. Portanto, por não ter a multa diária caráter indenizatório ou ressarcitório, demonstra-se completamente descomedida a aplicação indistinta do mesmo teto estabelecida para a multa simples, cabendo a ANPD realizar uma leitura interpretativa do inciso III com base nos princípios constitucionais nos casos de aplicação excessiva do referido instrumento.

O bloqueio dos dados pessoais objeto da infração até a sua regularização, a despeito de apresenta-se como uma solução razoável, traz algumas questões a serem enfrentadas. Ao ponto em que limita temporariamente o tratamento de dados pelo agente de tratamento que cometeu infrações às normas previstas na LGPD, quando bloqueados, permanecerão sobre custódia desta mesma empresa ou haverá a transferência para a ANPD custodiar tais dados? Acontece que, o armazenamento é uma forma de tratamento e a Lei sequer define essa questão, trazendo uma enorme insegurança jurídica, pois caso os dados sejam mantidos pelo agente de tratamento que deveria suspender o tratamento, o inciso V é ineficaz.

Já a eliminação de dados pessoais, a qual se refere o inciso VI, trata-se do apagamento definitivo, não abrindo espaço para a questão analisada acima. A única preocupação da Autoridade Nacional de Proteção de Dados, diante dos diversos métodos que existem na atualidade para a recuperação de dados excluídos, deve ser assegurar que a eliminação seja realizada por completo. Neste sentido, O GDPR, em seu art. 58, (2), (f) e (g)[459] estabelece

[459] Art. 58 (2). Cada autoridade de controlo dispõe dos seguintes poderes de correção: f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição; g) Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16.o, 17.o e 18.o, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do

algumas medidas corretivas a serem adotadas pela ANPD para assegurar a plenitude da eliminação de dados.

Em respeito aos critérios de hierarquia, cronologia e especialidade previstos na Lei de Introdução às normas do Direito Brasileiro (LINDB), o §2º do art. 52 remete à ideia de que as leis devem dialogar entre si. Sendo assim, a aplicação de multa pela ANPD em vista de infração no tratamento de dados pessoais não configura *bis in idem* às sanções aplicadas a uma agente de tratamento submetido ao regime regulatório do CDC. Diferentemente seria se a LGPD indicasse a aplicação de multas pela ANPD e por um órgão de defesa do consumidor. O que a LGPD pretende com o disposto no art. 52 é garantir que eventual penalidade imposta por violação as suas normas não substituem a aplicação de outras sanções administrativas, cíveis ou penais, quando a conduta do agente infrator também violar outros instrumentos legais.

Ainda, objetivando a transparência no processo regulamentador para a edição de normas complementares para a fixação e multas, o legislador prevê o instituto da consulta pública e alguns critérios a serem observados, como a necessidade de publicação previa e a demonstração objetiva das formas e dosimetrias para o cálculo do valor-base das multas (art. 53). A aplicação da pena de multas, como já relatado acima, é tema que tem a sua aplicabilidade bastante questionada ao longo de todo o processo legislativo da LGPD[460] e percebe-se, ao ponto em que o art. 54 discorre acerca da dosimetria e da necessidade de motivação administrativa da multa diária, a existência de uma fragmentação normativa desde o §4º do art. 52. Por fim, conclui-se que, apesar de alguns pontos no regime sancionatório da

---

artigo 17.o, n.o 2, e do artigo 19.o. (UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020)

[460] Principalmente no que se refere aos questionamentos contrários à criação de, nas palavras do Relator na Câmara dos Deputados, Deputado Orlando Gomes, "indústria da multa", caracterizada pela proposta de destinação de recursos provenientes de multas para o fomento das atividades da Autoridade Nacional de Proteção de Dados. Tal posicionado foi dado pelo deputado em 2012 no seu relatório perante a Comissão Especial do PL 4060: "Como dito anteriormente, um órgão somente poderá fiscalizar efetivamente um determinado setor da economia com verbas suficientes e perenes. Por outro lado, o ente regulador não pode se tornar simplesmente um novo elemento arrecadador. Por esses motivos, ao mesmo tempo em que prescrevemos claramente a separação de receitas orçamentarias próprias para o futuro órgão designado, determinamos oito fontes adicionais de recursos. Em tempo, esclarecemos que os oito incisos previstos nada mais são do que aqueles normalmente destinados a órgãos da administração direta ou indireta, tais como receitas com dívida ativa, doações, mercado financeiro, cobrança de emolumentos, acordos, convênios ou contratos e venda de publicações. É importante observar que não se quer criar uma indústria da multa. Apenas se garantir a independência administrativa da Autoridade, e, comisso, assegurar o poder fiscalizatório do órgão.

LGPD que devem ser sanados, “as penalidades trazidas na LGPD são suficientes à exequibilidade de um bom regime regulatório[461]”.

4.5 AS LIMITAÇÕES DO CONSENTIMENTO

Baseando-se na caracterização do titular de dados como parte vulnerável na relação de tratamento, é notória a preocupação da LGPD em evitar ao máximo qualquer hipótese de violação de dados pessoais[462]. Para Bruno R. Bioni, há uma discrepância ainda maior na relação de tratamento de dados e por isso, trata-se então de uma hiper-vulnerabilide do titular de dados[463]. Neste sentido, apesar da Lei se preocupar em criar um sistema normativo próprio para o consentimento como base legal, as limitações do referido instituto vão muito além das lacunas jurídicas, iniciam-se na própria complexidade do fluxo informacional. Portanto, mesmo com o fortalecimento de tal instituto na LGPD, estes obstáculos sociais e legais acabam impedindo um verdadeiro processo de tomada de decisões acerca dos dados pessoais.

4.5.1 A complexidade do fluxo informacional para o titular de dados pessoais

Sob uma perspectiva normativa e, consequentemente, superficial, tendo em vista a imensidão que pode se extrair das limitações cognitivas do ser humano, pode-se dizer que, diante do complexo ambiente de compartilhamento de dados, atividade essencial na indústria publicitária[464], por exemplo, torna o fluxo informacional extremamente frágil, uma vez que o

---

[461] ALVES, Fabricio da Mota. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019, p. 385.

[462] “A LGPD é uma norma que visa modificar a cultura no tratamento de dados pessoais para que riscos sejam mitigados desde antes do tratamento, evitando-se ao máximo qualquer hipótese, sempre presente, de violação de dados pessoais. No decorrer da lei há uma motivação nítida nesse sentido, impondo que os agentes de tratamento, desde a concepção da iniciativa que visa tratar dados pessoais e durante todo o seu ciclo de vida, que termina com o seu descarte, reflitam, analisem e adotem medidas efetivas para garantir a legalidade dos procedimentos e a proteção desse insumo tão valioso, mas, ao mesmo tempo, tão perigoso, se tratado de forma irregular”. (VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 158)

[463] “A diretriz normativa da autodeterminação informacional se perdeu em meio às assimetrias do mercado informacional, concluindo-se que o cidadão-consumidor está exposto a uma hiper vulnerabilidade que mistifiica a sua prometida capacidade de controle dos seus dados pessoais”. (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 191)

[464] The selective targeting of ads based on past behaviors, and, possibly, other personal information, raises concerns over an insidious form of discrimination that Oscar Gandy has called the ‘panoptic sort’. Aggregating information drawn from diverse sources and different contexts, individuals are profiled and assigned to

titular de dados não tem como ter consciência de todos os atores que fazem parte de todo o processo de mineração de seus dados pessoais[465]. Neste sentido, conforme comprovado em diversas pesquisas de universidade extremamente renomadas[466], as habilidades cognitivas dos seres humanos, por natureza, já são limitadas, fator que se acentua na memorização e entendimento acerca de todas as informações relevantes para a tomada de decisões relacionadas à proteção de dados pessoais[467].

Assim, a complexidade em volta de todo fluxo informacional em adição ao tratamento massivo e desenfreado de dados pessoais resulta em uma verdadeira evasão ao consentimento.

Neste seguimento, pesquisadores das Universidades de Stanford e Carnegie Mellon realizaram analise empírica da reação dos usuários aos modelos de publicidade *online.* Com base em entrevistas[468] pautadas na questão da compreensão dos titulares de dados em relação ao fluxo das suas informações pessoais, foi constado que: apenas 17% dos usuários deletam os *cookies*, enquanto 60% não deletam e 23% sequer sabiam dizer apagavam ou não tal ferramenta de coleta de dados pessoais. Ainda, em relação ao modo de navegação privada que consequentemente bloqueia a coleta de dados pessoais, 23% dos usuários utilizavam este mecanismo, 50% dos usuários não utilizavam e 27% não tinha certeza. Além destas

---

categories of treatment". (BAROCAS, Solon; NISSENBAUM, Helen. **The Trouble with Notice and Consent.** p.3. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409. Acesso em: 10 jul. 2020)

[465] "After investigating the subject of behavioral targeting intensively and extensively, our own ongoing uncertainty over what really is happening with information about our online activities suggests that notice, as yet, may not be sufficient to meaningful consent. Users who are subject to OBA confront not only significant hurdles but full-on barriers to achieving meaningful understanding of the practice and uses to which they are expected to be able to consent. This stems from various types of complexity and volatility in the ecology and dynamics of the industry, its policies and its information flows". (BAROCAS, Solon; NISSENBAUM, Helen. **The Trouble with Notice and Consent.** p.3. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409. Acesso em: 10 jul. 2020)

[466] Como exemplo de pesquisas que os seus resultados confirmaram a evasão ao consentimento: Privacy and modern advertising: most US internet users want 'do not track' to stop collection of data about their online activities (Universidade de Berkely); Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising (Universidades de Stanford e Carnegie Mellon) e The tradeoff fallacy: how marketers are misrepresenting and opening them um to exploitation (Universidade da Pensilvania).

[467] "Especially in the presence of complex, ramified consequences associated with the protection or release of personal information, our innate bounder rationality limits our ability to acquire, memorize and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics. (…) Even if individuals have access to complete information about their privacy risks and modes of protection, they might not be able to process vast amounts of data to formulate a rational privacy-sensitive decision. Human beings' rationality is bounded, which limits our ability to acquire and then apply information". (ACQUISTI, Alesssandro; GROSSKLAGS, Jens. Privacy and rationality in individual decision making.. ***IEEE Securty & Privacy Review***, jan./fev. 2005, p. 27-30. Disponível em: https://ieeexplore.ieee.org/abstract/document/1392696. Acesso em: 10 jul. 2020)

[468] 14 entrevistados na primeira fase e 314 na segunda fase das entrevistas. (CRANOR, Lorrie Faith; MCDONALD. Aleecia M. ***Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising.*** P. 04-05. Disponível em: < https://www.researchgate.net/publication/228237033_Beliefs_and_Behaviors_Internet_Users'_Understanding_of_Behavioral_Advertising. Acesso em: 10 jul. 2020)

constatações, também foi analisado o porquê uma porcentagem tão baixa dos usuários deletavam os *cookies,* dentre outros aspectos relevantes para a conclusão de que indivíduos não possuem conhecimento técnico suficiente para exercer uma plena autodeterminação dos seus dados pessoais no processo de tratamento.

Ainda, na última etapa das pesquisas, os usuários foram submetidos à seguinte pergunta: se preferiam receber US $1,00 como desconto no produto/serviço pela utilização dos seus dados pessoais pelos provedores de Internet ou se pagariam este mesmo valor para que os provedores não coletassem os seus dados pessoais. Confirmando as limitações cognitivas dos titulares de dados no processo de tomada de decisões acerca da proteção dos seus dados pessoais, 69% dos usuários submetidos a essa etapa da pesquisa concordariam com o desconto em troca das suas informações pessoais. Assim, conclui-se que, além da falta de conhecimento relacionado ao processo de tratamento de dados e a sua relação com a publicidade *online*, a própria estrutura dos modelos de negócios travados na Internet agrava ainda mais a vulnerabilidade dos titulares de dados[469]. O resultado desta pesquisa demonstra a de forma clara à configuração do fenômeno das dissonâncias cognitivas[470], onde as pessoas dizem valorizar a proteção de seus dados pessoais, mas atuam de forma completamente contrária.

No que se referem às referidas barreiras psicológicas que impedem o indivíduo de controlar as suas informações pessoais por completo, há também como exemplo a ideia de "benefícios imediatos", característica da teoria da utilidade subjetiva que pode ser visualizada na possível ocorrência de dano com relação aos dados pessoais após o acesso do titular a um produto ou serviço *online.* Aqui, o titular de dados, de forma natural, tende a valorizar os benefícios imediatos em prol da perda do controle de seus dados pessoais e assim, raramente o sujeito irá voltar atrás através da utilização do seu direito de revogar o consentimento.

---

[469] "First and foremost, consumers cannot protect themselves from risks they do not understand. We find a gap between the knowlesge users currently have and the knowledge they would need to possess in order to make effective decisions about their online privacy. (…) Ideally, users could choose for themselves but at present they lack the knowledge to be able to make informed decisions". (CRANOR, Lorrie Faith; MCDONALD. Aleecia M. ***Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising.*** P. 04-05. Disponível em: < https://www.researchgate.net/publication/228237033_Beliefs_and_Behaviors_Internet_Users'_Understanding_of_Behavioral_Advertising. Acesso em: 10 jul. 2020)

[470] "Nesse jogo de ganhos e perdas, o ser humano tende a procurar uma 'zona de conforto' para não se culpar em torno do prejuízo por ele suportado. Trata-se das chamadas dissonâncias cognitivas em que o sujeito procura um alívio para simetricamente compensar um desconforto. É nesse contexto que se insere o denominado 'paradoxo da privacidade'. Em que pese as pessoas valorarem a proteção de seus dados pessoais, elas empreendem ações dissonantes a tal apreço. As suas condutas contradizem o que elas estimam, surgindo-se uma relação de incoerência entre o que elas praticam e o que elas enxergam como ideal". (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 141)

Ainda, mesmo com o fornecimento de informações completas e coerentes acerca dos riscos da atividade de tratamento, bem como das técnicas que vão ser utilizadas pelos agentes para a mitigação destes riscos, a assimetria informacional e a vulnerabilidade do cidadão são elementos próprios do mercado informacional. Assim, configura-se nada mais que uma falsa proposta de participação do titular no processo de tratamento dos seus dados ao fazê-lo "concordar" com o compartilhamento dos seus dados pessoais com apenas um 'click'. Assim, para Bruno Bioni o consentimento acaba por fazendo parte desta verdadeira assimetria informacional:

> Muito embora se dedique um diploma próprio para tratar dessa situação específica de vulnerabilidade, apostam-se todas as fichas normativas como se a parte mais fraca desse arranjo regulatório fosse um sujeito racional, livre e capaz para fazer valer a proteção de seus dados pessoais. O protagonismo do consentimento encerra, portanto, uma contradição (intrínseca) desse ambiente ou estratégia regulatória. (...) O consentimento tem sido visto como o pilar dessa estratégia regulatória, mais como um meio para legitimar os modelos de negócios da economia digital, do que como um meio eficiente para desempenhar a proteção de dados pessoais. Ele tem sido encarado como uma verdadeira ficção legal deformadora e voraz do teorizado regime legal de proteção de dados pessoais e da sua aplicação na prática. Não seria mais do que uma mistificação, na medida em que não é confrontado com o anotado contexto socioeconômico que estrangula a prometida liberdade da autodeterminação informacional[471].

Cumpre aqui, a análise de exemplo prático do dia-a-dia de praticamente todos os indivíduos que possuem ou não acesso à internet e que se caracteriza como uma verdadeira evasão do consentimento, qual seja: as políticas de privacidade. Essa espécie de contrato de adesão[472], onde é necessário o consentimento do titular para legitimar qualquer tipo de operação de dados pessoais, é nada mais do que resultado direto da insuficiência normativa acerca das formas de operação do consentimento. Como é de conhecimento comum, nas políticas de privacidade, não é dada a oportunidade de alteração contratual ao usuário do serviço ou produto, impossibilitando-o de que exerça o controle sobre as suas informações pessoais e assim, reforçando ainda mais a existente assimetria das relações travadas no mercado informacional. Cumpre mencionar que, a caracterização das políticas de privacidade como um contrato de adesão é objeto de divergência na doutrina[473], havendo aqueles que entendam tal mecanismo como condições gerais de contratação[474].

---

[471] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 160.

[472] Para uma melhor compreensão acerca dos contratos eletrônicos de adesão, ver: LIMA, Cíntia Rosa Pereira de. Validade e obrigatoriedade dos contratos de adesão eletrônicos (Shrek-wrap e click-wrap) e dos termos e condições de uso (browse-wrap): um estudo comparado entra Brasil e Canadà. Tese Doutorado – Faculdade de Direito da Universidade de São Paulo, 2009.

[473] "Isto porque os termos de uso acabam por disciplinar um número indeterminado de relações contratuais do consumidor, na medida em que, por exemplo, seria capaz de regulamentar o fluxo dos dados pessoais dos consumidores com outras aplicações e com os famigerados 'parceiros comerciais'. Por esse viés, as políticas de

Apesar de caracterizar-se como um mecanismo de controle de dados pessoais por parte do titular, demonstra-se extremamente falho por diversos motivos, principalmente pelo acesso ao indivíduo estar condicionado pela sua aceitação aos termos de privacidade, bem como da fixação do programa contratual pela parte mais forte, ou seja, cabe ao fornecedor determinar o rumo do referido fluxo informacional. Tal dinâmica contratual, própria dos contratos de adesão[475], retira o poder de barganha do titular de dados no que diz respeito à sua própria privacidade, fazendo do consentimento uma mera condicionante à utilização do serviço/produto, característica nomeada pelos doutrinadores anglo-americanos de "*take-it-or-leave-it*", ou seja, pela tradução direta para a língua portuguesa: a lógica do tudo ou nada[476].

As constatações extraídas de estudo empírico realizado pela *Global Privacy Enforcement Network*/GPEN em 2014 revelaram dados extremamente relevantes, comprovando que tal ferramenta contratual está longe de ser considerada uma forma de autocontrole de dados pessoais. Das políticas de privacidade de aplicativos móveis analisadas, 85% não prestavam informações adequadas acerca da coleta, uso e compartilhamento de dados pessoais aos usuários; 1/3 coletavam dados pessoais de maneira excessiva e desnecessária para a finalidade do tratamento; 59% utilizavam vocabulário de difícil compreensão em relação às informações básicas de privacidade e 43% tinham um design inadequado, seja pelas letras muito pequenas ou textos demasiadamente grandes[477].

Essa última constatação, qual seja, a presença de textos longos e de difícil compreensão e a sua relação com a dificuldade de o titular de dados racionalizar um processo de tomada de decisões deu, inclusive, ensejo a um estudo realizado na *Carnegio Mellon University*. As pesquisadoras chegaram à conclusão que usuários precisariam de pelo menos 201 horas, equivalente a U$3,354 por ano, para que conseguissem ler apenas os termos de uso dos sites

---

privacidade enquadrar-se-iam nessa última espécie do fenômeno da massificação contratual. A nossa indecisão é decorrente do próprio impasse na doutrina no que diz respeito à utilidade de tal diferenciação entre contratos de adesão e condições gerais de contratação". (BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 162)

474 GOMES, Orlando. **Contratos de adesão:** condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972, p. 05-09.

475 "A expressão contrato de adesão resulta inicialmente do fato de que o que impressiona nessa figura, em relação à estrutura normal de um contrato, é a posição do aderente que não tem a possibilidade de discutir as cláusulas, até mesmo as que lhe sejam desfavoráveis, quer sejam ilegais, quer não, sob pena de ser excluído o círculo dos possíveis contratantes". (MIRANDA, Custódio da Piedade Ubaldino. **Contratos de Adesão.** São Paulo: Atlas, 2002, p. 20)

476 MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor:** o novo regime das relações contratuais. São Paulo: Editora Revista dos Tribunais, 2011, p. 79.

477 INFORMATIONAL COMISSIONER'S OFFICE. ***Global survey finds 85% of mobile apps fail to provide basic privacy information.*** Disponível em https://www.wired-gov.net/wg/news.nsf/articles/Global+survey+finds+85+of+mobile+apps+fail+to+provide+basic+privacy+information+10092014151000?open. Acesso em: 13 jul. 2020.

acessados, na média, por ano por um usuário americano. Cumpre ressaltar que essa contabilização anual sequer incluía as políticas de privacidade[478]. Soma-se, ainda, ao fato de uma constante atualização dos termos de uso/privacidade, que, muitas das vezes, a versão posterior se caracteriza como mais evasiva do que a anterior. A diminuição da esfera de controle sobre os dados pessoais através das alterações nos termos de uso como pode ser vista em estudo feito pela *Eletronic Frontier Foundation*/EFF[479], que analisou a evolução das políticas de privacidade do *facebook* no período de 5 anos (2005-2010), constatando diversas alterações que possibilitavam um maior controle de dados pessoais por parte dos usuários.

Aqui entra em jogo o dever de os agentes de tratamento facilitarem o processo cognitivo dos titulares de dados em relação ao tratamento de dados e à sua privacidade. Neste sentido, Rony Vainzof sugere a utilização de políticas de privacidade segmentadas:

> No ambiente digital, o uso de uma política de privacidade segmentada permitirá que um usuário navegue até a seção específica, em vez de ser obrigado a percorrer grandes quantidades de texto pesquisando essas informações relevantes acerca da sua privacidade. As informações obrigatórias prestadas ao titular expressamente previstas na LGPD, perante o princípio da transparência, são requisitos legais mínimos. O controlador deve avaliar o caso em concreto regularmente para eventuais adaptações considerando o conceito de 'homem médio' do seu público alvo e o nível de compreensão dos seus titulares para utilização de uma comunicação inteligível[480].

Cumpre também a análise de dois casos envolvendo os termos de uso do *Facebook Messenger* e da Samsung *Smart TV*, nos anos de 2014 e 2015, respectivamente, que tiveram uma reação social extremamente negativa[481]. Para ampliar a base de dados da plataforma, o modelo de troca de mensagens de forma privada foi retirado da rede social e caso os usuários pretendessem continuar com tal ferramenta teriam que baixar um novo aplicativo *(Facebook Messenger)*. Acontece que, o acesso a este novo serviço estava condicionado a um novo termo de uso, que, de forma estratégia, era bem mais permissivo que a termo de uso do *Facebook.* Dentre outras disposições, o referido aplicativo poderia gravar áudios, fazer ligações, tirar fotos e até mesmo editar mensagens de texto sem a necessidade de um novo

---

[478] MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. *The cost of Reading Privacy Policies.* ***Journal of law and Policy for information society,*** v. 4, 2008, p. 544-565.

[479] OPSAHL, Kurt. Facebook's Eroding Privacy Policy: a timeline. **Eletronic Frontier Foundation.** Disponível em: https://www.eff.org/deeplinks/2010/04/facebook-timeline. Acesso em: 13 jul. 2020.

[480] VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019, p. 151.

[481] FIORELLA, Sam. ***The insidiousness of Facebook Messenger's android mobile app permissions.*** Disponível em: https://pt.slideshare.net/plantquack3480/the-insidiousness-of-facebook-messengers-android-mobile-app-permissions-updatedsam-fiorella. Acesso em: 13, jul., 2020.

consentimento dos usuários para determinadas finalidades[482]. Já a abusividade da política de privacidade da Samsung *Smart TV*, que por sinal, foi alterada logo em seguida, se caracterizava pela inclusão de cláusula que se referia à possibilidade de armazenamento e transmissão a terceiros das palavras e outras informações sensíveis captadas pelo sensor do televisor[483].

Percebe-se, da análise da abusividade dos termos de uso em geral, um direito à autodeterminação que se limita ao consentimento não é capaz de solucionar a desproteção dos dados pessoais dos usuários. Assim, a validade do termo de uso/privacidade não deve se limitar à obtenção do consentimento do usuário, devendo também ser considerada a integridade do fluxo informacional em questão, o que não foi observado nos dois casos analisados acima. Para Bruno Bioni, há a necessidade de observação de todo o contexto em que o consentimento foi obtido, ideia presente no conceito de privacidade/consentimento contextual[484]:

> Nesse arranjo ambivalente, devem-se esgotar os elementos contextuais da relação sob análise, verificando-se, dentre outros aspectos: i) quais são os propósitos do tratamento dos dados pessoais, levando-se em consideração o contexto da relação subjacente ao fluxo informacional; ii) como terceiros podem estar inseridos no fluxo informacional e sob quais condições; iii) quais são as implicações do tratamento de dados sobre seu titular; iii.a) no que diz respeito ao desenvolvimento da sua personalidade; iii.b) para que ele se relacione livremente em outras e nas diversas esferas sociais. Deve-se reunir, pois, todo um conjunto de informações necessárias – fatores contextuais – para verificar a integridade do fluxo informacional, observando-se o valor social da privacidade informacional e a negociabilidade limitada dos direitos da personalidade[485].

---

[482] HAYASHI, Eduardo Issao. 10 termos de uso do Facebook Messenger que vão deixar você boquiaberto. **Tecmundo.** 08 ago. 2014. Disponível: https://www.tecmundo.com.br/facebook/60271-10-termos-uso-facebook-messenger-deixar-voce-boquiaberto.htm. Acesso em: 13 jul. 2020.

[483] HERN, Alex. *Samsung rejects concern over 'Orwellian' privacy policy*. Fev. 2015. **The Guardian.** Disponível em: **https://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy#:~:text=Users%20of%20Samsung's%20Smart%20TV,the%20television%20is%20plugged%20in.** Acesso em: 13 jun. 2020.

[484] Para uma melhor compreensão acerca da privacidade e consentimento contextual, ver Capítulo 5.4 da obriga Proteção de Dados Pessoais: a Função e os Limites do Consentimento de Bruno Ricardo Bioni (BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020)

[485] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 221.

4.5.2 Limitações jurídicas

Além das demais bases legais já analisadas no tópico 3.3 deste Trabalho, reguladas nos incisos II ao X do art. 7º da LGPD, que acabam, inevitavelmente, diminuindo a esfera protetiva do titular de dados por meio do consentimento, o legislador optou por adotar "exceções" ao pleno exercício do consentimento que por si só limitam tal instituto. No que se refere à ressalva de resguarda do interesse público expresso no art. 8º, §5º, por exemplo, apesar deste conceito ser amplamente utilizado como uma norma de superioridade em relação ao interesse privado, conforme analisa o Professor Juliano Heinen, há uma plurissignificação do referido termo no ordenamento jurídico brasileiro[486]. Ao ponto em que a LGPD não define o seu conceito, tampouco os seus limites, esta lacuna jurídica acaba, por lógica, enfraquecendo o direito do titular de dados de exercer livremente os seus atos de vontade em relação ao tratamento de seus dados pessoais.

Neste mesmo sentido, a exceção do segredo comercial e industrial, utilizada nove vezes no texto legal da LGPD, atua como um direito do agente de tratamento e consequentemente, se configura como uma limitação ao direito concedido pela Lei ao titular de dados. Tal relação é clara da simples leitura do inciso II do art. 9º, o qual prevê o direito ao acesso facilitado às informações acerca da forma e duração do tratamento, "observados os segredos comercial e industrial". Também, em seu §3º, o art. 19, ao se refere à possibilidade de solicitação por parte do titular de dados de cópia eletrônica integral de seus dados pessoais nas hipóteses de tratamento originadas no consentimento. Ao fim, o legislador condicionou a observação dos segredos comerciais aos termos de regulamentação da ANPD. Ou seja, de antemão, transferiu o papel de definição do que ao certo é considerado segredo comercial e industrial, e, portanto, apesar de tratar-se exceção ao fortalecimento do campo de atuação do titular de dados e direito dos agentes de tratamento, evita que a sua utilização se dê de forma arbitrária.

De forma expressa, a LGPD dispensa a exigência do consentimento previsto nos termos do art. 7º, I da Lei nas situações em que o próprio titular dos dados tornou-os manifestamente públicos, conforme prevê o §4º do art. 7º. Nas palavras de André de Oliveira Schenini Moreira**,** o legislador se manifesta acerca de tal exceção ao regime jurídico dado ao consentimento pela LGPD de "forma tímida em um parágrafo, mas cujo papel pode ser estratégico na atividade de quem está sujeito a essa legislação". De acordo com esse

[486] HEINEN, Juliano. **Interesse público:** premissas teórico-dogmáticas e proposta de fixação de cânones interpretativas. 1 ed. Salvador: Editora JusPodivm, 2018.

mesmo autor, a menção expressa à dispensa apenas da base legal do consentimento é totalmente duvidosa, pois, sob a sua perspectiva, tal exceção devia ser aplicável a todas as outras hipóteses autorizadoras do tratamento de dados pessoais do art. 7º[487].

Neste aspecto, é importante considerar a diferença entre dados de acesso público e aqueles manifestamente públicos, ao ponto em que, no §3º deste mesmo artigo, o legislador se referiu à expressão de "dados cujo acesso é público". A dispensa da exigência do consentimento se configura quando o usuário, por iniciativa própria, tornar público os seus dados pessoais, diferentemente dos dados pessoais, que caracteriza pela presença de terceiros no processo de publicização dos dados pessoais. Conforme entendimento de Marcel Leonardi ao comentar o projeto de lei 5.276/16, entende-se por dados pessoais de acesso público aqueles "cuja divulgação pública é obrigatória por lei – o fato de alguém ser proprietário de um imóvel, ou sócio de uma empresa, por exemplo, ou os dados acerca das atividades de órgãos públicos, nos termos da Lei de Acesso a Informações". Em ambos os casos, o legislador não autorizou o uso indiscriminado de tais informações, quebrando com a ideia de não associação destes tipos de dados como passíveis de proteção diante da sua não confidencialidade, racionalidade própria do pensamento dicotômico entre público e privado[488].

Aqui, cumpre mencionar julgamento de ação civil pública pelo Tribunal de Justiça do Rio Grande do Sul (TJRS) enquanto já vigente o Marco Civil da Internet. O Tribunal, ao reformar a decisão de primeira instância, mudou também a racionalidade do que seriam considerados "dados cadastrais" e que, portanto, a sua comercialização, para fins de marketing, por exemplo, poderia ser realizado mesmo sem o consentimento/autorização do titular destes dados justamente por serem dados de "domínio público". No entanto, os dados considerados cadastrais eram dados como nome, endereço, idade, profissão, estado civil e filiação, pois foi de entendimento do referido Tribunal que, "quase todos os cidadãos comuns, quase que diariamente, são compelidos a fornecer ao praticar atos da vida civil (...), não sendo, portanto, sigilosos"[489]. Portanto, a lógica utilizada pelo TJRS não permite que seja feita uma análise como base na finalidade da publicidade de tais dados, o porquê destes dados estarem em circulação e consequentemente, a justificativa da sua disponibilização.

---

[487] MOREIRA, André de Oliveira Schenini. A exceção dos dados pessoais tornados manifestamente públicos pelo titular na LGPD. **Migalhas.** 07 jan. 2019. Disponível em: **https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd**. Acesso em: 16 jul. 2020.

[488] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 256.

[489] Resumo do Processo nº CNJ 0152244-45.2016.8.21.7000 feito pelo site do Migalhas. Disponível em: https://www.migalhas.com.br/arquivos/2016/11/art20161104-10.pdf. Acesso em: 16 jul. 2020.

Demonstrando o rompimento dessa cultura jurídico-legal de associação da proteção de dados pessoais ao direito à privacidade, ao final da redação do §4º do art. 7º, o legislador se refere à: "resguardados os direitos do titular e os princípios previstos nesta Lei", Ainda, a LGPD garante que devem ser observados no processo de tratamento a finalidade, a boa-fé e o interesse público que justificaram a disponibilização dos dados pessoais de acesso público.. Sob o ponto de vista de Bruno Bioni, o princípio mais relevante ao tratamento de dados tornados manifestamente públicos pelo titular é o princípio da finalidade[490]. No entanto, é garantido ao titular tanto os seus direitos previstos nos artigos 9º e 18, da LGPD, principalmente, quanto os princípios previstos nos art. 6º da Lei.

Em especial, os direitos previstos nos incisos IV e VI do art. 18, de certa forma, conflitam com a exceção trazida pelo art. 7º, §4º. Tais incisos se referem ao direito do titular de dados requerer a eliminação de determinados dados em posse do controlador, bem como impedir o seu uso, o que não se aplicaria aos dados tornados manifestamente públicos pela simples interpretação dos mencionados artigos. Assim, o legislador já antevê tal ponto de atrito ao prever no §2º do art. 18, deixando claro que: "o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei". Ou seja, ao mesmo em que é garantido ao titular de dados os direitos dos incisos IV e VI do art. 18 quando restar configurado o desrespeito à LGPD, o uso de dados em conformidade com a LGPD nos casos de dispensa do consentimento não está sujeito à oposição do titular.

Conclui-se que, apesar da dispensa do consentimento em relação aos dados tornados público pelos seus titulares, deve ser levado em consideração pelos agentes de tratamento o contexto em que tais informações foram disponibilizadas[491]. A ausência de clareza pelo legislador quanto aos limites da referida exceção à necessidade do consentimento demanda, neste momento, uma interpretação da doutrina. Em relação a essa análise contextual[492], cumpre

---

[490] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 257.

[491] Neste mesmo sentido se posicionou o Parlamento Scocês em documento de diretrizes para a adoção do GDPR: "There is no definition of 'manifestly made public' under GDPR, however, simply because personal data is in the public domain (for example, in a newspaper article),or has been provided directly to a Member, does not necessarily mean it has been manifestly made public by the person. This exemption can only be relied upon in circumstances where it is clear that the data subject has themselves put their personal data into the public domain, for example, on their own social media account or on a charity fundraising page that they have set up themselves)". Disponível em: https://www.parliament.scot/S5ChamberOffice/2018_06_01_Motions_Guidance_FINAL.pdf

[492] "Imaginemos, contudo, a situação em que um usuário, ao preencher e publicar seus dados em um perfil de uma rede social, não sabia que aqueles seriam acessíveis ao público em geral por falta de ou precária informação. O fato de que tais dados foram lançados ao ubíquo mundo da internet pelo próprio titular,

mencionar exemplos de casos concretos explicados por Bruno Bioni que traduzem perfeitamente essa ideia:

> Por exemplo, a principio, terceiros não poderiam usar dados de uma rede social, mesmo que de perfis públicos, para fins de *marketing.* As circunstâncias pelas quais os dados foram tornados públicos pelo seu próprio titular deram-se pra uma outra finalidade, que é a de se relacionar com quem integra o seu círculo social. Por outro lado, a princípio, seria compatível o uso de dados de perfis públicos de uma rede social (e.g LinkedIn) por terceiros, como *headhunters*, para aproximar seus usuários às vagas profissionais de seu eventual interesse. Esse uso é compatível com a finalidade não só da plataforma em si, como, principalmente, a razão pela qual tais dados são públicos[493].

Referente às limitações jurídicas, além dos riscos de uma transposição rasa dos elementos do Código Civil para regulamentar os institutos da LGPD e sanar as suas lacunas, tema já abordado no Tópico 4.2 deste Trabalho, cumpre também observar o que muitos autores chamam de um "paradoxo da privacidade". Este termo se refere à limitação da obtenção de tutela nos casos em que o consentimento centraliza a disciplina de proteção de dados, pois somente é possível a obtenção da tutela esperada depois do indivíduo ter concordado em revelar os seus dados pessoais, para que então possa arguir a presença de algum defeito[494]. Por isso, diante dessas limitações que decorrem tanto da própria natureza da LGPD, quanto das próprias exceções previstas, a preocupação da sociedade em geral e da autoridade reguladora devem se pautar no impedimento de que instrumentos sejam utilizados como artifícios para "maquiar" a atuação dos agentes de tratamento que vão além dos limites intencionados de fato pela Lei.

---

tornando-se manifestamente públicos, mas sem os devidos cuidados que a própria LGPD exige, permitiria que terceiros utilizassem tais dados sob a exceção do §4º do art. 7º? Considerando o teor da LGPD, penso que a ciência do titular sobre a publicização de seus dados também é condição indispensável para que o tratamento daqueles, sem prévio consentimento, seja autorizado. No entanto, não podemos esquecer do mundo prático e do ambiente digital para o qual a lei é especialmente direcionada - nesse sentido, exigir dos controladores a investigação pretérita da intenção de usuários quanto aos dados já tornados públicos por estes parece, ao meu ver, uma exigência inviável". (MOREIRA, André de Oliveira Schenini. A exceção dos dados pessoais tornados manifestamente públicos pelo titular na LGPD. **Migalhas.** 07 jan. 2019. Disponível em: https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd**.** Acesso em: 16 jul. 2020.)

[493] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020, p. 258.

[494] CARBONE, Vicenzo***. Il consenso, anzi i consensi, nel tratamento informático dei dati personali. Danno e responsabilità,*** n.1, 1998, p. 26.

5 CONCLUSÃO

Diante da capacidade do processamento dos dados disponibilizados nas redes sociais revelarem verdadeiramente uma parcela da personalidade dos indivíduos, em conjunto com um sistema de tratamento de dados pautado na maximização de lucros, se consolida ainda mais a necessidade de uma legislação de proteção de dados pessoais no Brasil. A complexidade dos efeitos que a má utilização de dados pessoais pode causar na vida do titular faz com que a tutela jurídica dos dados pessoais não possa ser entendida como uma mera evolução do direito à privacidade. Assim, o direito à proteção de dados pessoais passa a ser pressuposto para que a pessoa não seja controlada pelos agentes de tratamento, que não tenha a sua autonomia privada cerceada e em última análise, a inibição do livre desenvolvimento da sua personalidade. Neste sentido, a LGPD demonstra logo de início, em seu art. 1º, que objetiva a proteção dos diretos fundamentais da liberdade e da privacidade, possibilitando o livre desenvolvimento da personalidade da pessoa natural identificada ou identificável.

Conforme restou demonstrado no desenvolvimento do segundo capítulo da presente monografia, apesar do direito a proteção de dados pessoais não ser considerado formalmente um direito fundamental à luz d CF/88, sendo inclusive tema que motivou a instituição da PEC 17/2019, em recente decisão (maio, 2020) do STF relatada pela Ministra Rosa Weber, foi reconhecido o direito à proteção de dados pessoais como um direito fundamental autônomo. É inegável, neste ponto, que o referido julgamento se caracteriza como um grande avanço jurisprudencial na esfera de proteção de dados pessoais no ordenamento jurídico brasileiro. No entanto, há de ser observada a necessidade de definição de critérios para definir a aplicação, os limites do próprio direito, bem como os da sua violação.

Corroborando com o caráter fundamental da proteção de dados pessoais, a interpretação sistemática da LGPD, pautada no protagonismo do titular, demonstra que o seu arranjo normativo se fundamenta na mitigação dos riscos desde antes da operação e que, portanto, intende a modificação da cultura de tratamento de dados pessoais. Consequentemente, as empresas devem adequar todos os seus setores às novas regras estabelecidas pela LGPD, adotando práticas de *compliance.* Em um contexto internacional, apesar do livre arbítrio de cada estado para regular os atos que foram praticados dentro do seu território de forma independente, a criação de legislações semelhantes se demonstra extremamente benéfica para a desburocratização do fluxo internacional de dados. Assim, a promulgação da LGPD coloca o Brasil no cenário da economia digital mundial, possibilitando, por exemplo, a transferência

internacional de dados entre países da União Europeia, uma vez que a regulamentação europeia, mencionada inúmeras vezes ao decorrer deste Trabalho, principalmente diante das suas semelhanças com o regramento de proteção de dados brasileiro, prevê a possibilidade de transferência dos dados pessoais para um país terceiro desde que a regulamentação deste país seja avaliada e considerada com nível de proteção adequada pela Comissão Europeia.

Da análise do terceiro capítulo deste trabalho, conclui-se que a LGPD, na intenção de reduzir a assimetria do mercado informacional, prevê um sistema protetivo sólido ao titular de dados, definindo de forma clara os seus direitos, bem como os deveres dos agentes de tratamento (controlador e operador), que quando desrespeitados estão sujeitos às sanções cíveis e administrativas, a depender do caso concreto. Além de estender o seu campo protetivo com uma extensa definição dos processos considerados tratamento de dados pessoais em seu art. 5º, X, a Lei define de forma taxativa as hipóteses que legitimam o tratamento de dados pessoais, bem como a necessidade de adequação aos princípios e da boa-fé independentemente do tratamento estar fundamentado em alguma base legal, deixando claro que os dados pessoais não são meros bens de cunho patrimonial.

O consentimento, neste sentido, atua como instrumento que viabiliza uma maior carga participativa do titular no processo de tratamento de seus dados pessoais. Assim, ao mesmo tempo em que possibilita a autodeterminação informativa, é um mecanismo de legitimação do tratamento de dados pessoais. Apesar de ser apenas mais uma das dez hipóteses que legitimam o tratamento de dados na LGPD, não deixa de ser o ponto focal da Lei. Corroborando com tal ideia, uma simples análise numérica de quantas vezes o termo consentimento é citado no corpo legal demonstra não só a sua relevância para a proteção de dados como instrumento que impacta a atuação dos agentes de tratamento de diversas maneiras, mas também, a necessidade de uma interpretação deste instituto de forma sistemática, uma vez que é mencionado 37 vezes de forma esparsa na LGPD.

Ao decorrer da análise das adjetivações do consentimento (livre, inequívoco e informado), é notório que o legislador se preocupou, diferentemente da maioria das outras bases legais, em criar um regramento específico ao decorrer dos artigos 7º a 9º da Lei para orientar e solidificar o controle de dados pessoais através do consentimento. Isso pode ser visto ao ponto em que menciona expressamente as hipóteses de nulidade do consentimento quando representar uma autorização genérica, bem como quando as informações que foram fornecidas ao titular possuam conteúdo enganoso, abusivo ou que não tenham sido apresentadas com transparência. Principalmente, diante do fato de que mesmo nas hipóteses de dispensa do

consentimento, os agentes de tratamento devem observar os princípios e direitos do titular previstos na LGPD, e assim, garante-se ao titular de dados o direito de se opor ao tratamento de seus dados em caso de descumprimento da Lei. Os instrumentos de reforço do controle de dados por meio do consentimento, a exemplo da possibilidade de revogabilidade do consentimento ou da hipótese de término do tratamento quando da comunicação do titular de dados, demonstram de forma clara que o referido instituto é o elemento cardeal da LGPD e que, portanto, impacta de forma direta a atuação dos agentes de tratamento.

Ainda, em relação à adjetivação do consentimento, observa-se, das características utilizadas pelo legislador para validar o consentimento na LGPD, a sua relação com a ideia da declaração da vontade livre e consciente extraída do Código Civil no tema dos defeitos do negócio jurídico, onde a ausência deste requisito configura o vício do consentimento, vedação mencionada na Lei de proteção de dados nos mesmos termos do Código Civil. Não obstante o impacto do direito civil na elaboração de uma dogmática de proteção de dados pessoais, o consentimento, como um dos pontos mais sensíveis da referida matéria, merece não só ser analisado no caso concreto de acordo com as suas próprias peculiaridades normativas, como também, deve o intérprete ter em mente que a sua natureza está intrinsicamente ligada a atributos da personalidade, ainda que de forma tangencial.

Ao mesmo tempo em que o legislador garante um regramento específico ao consentimento, as falhas presentes no texto legal, como exemplo da não definição dos adjetivos que balizam a validade de tal instituto, acabam por enfraquecer a esfera protetiva dos titulares de dados por meio de tal mecanismo. Neste ponto, além das demais bases legais que legitimam o tratamento de dados pessoais, que acabam, inevitavelmente, ampliando o campo de atuação dos agentes de tratamento, o legislador optou por adotar “exceções” ao pleno exercício do consentimento que por si só o limita. A ressalva de resguarda do interesse público expresso no art. 8º, §5º, por exemplo, apesar de ser amplamente utilizado como uma norma de superioridade em relação ao interesse privado, sequer foi definida ou limitada pela Lei. Neste mesmo sentido, a exceção do segredo comercial e industrial, utilizada nove vezes no texto legal, atua como um direito do agente de tratamento e consequentemente, se configura como uma limitação ao direito concedido ao titular de dados.

Em relação às lacunas jurídicas, caberá à Autoridade Nacional de Proteção de Dados, quando instituída, diante da sua competência para deliberar sobre a interpretação da LGPD, sanar as referidas falhas normativas. Neste ponto, a própria Lei condiciona a observação dos segredos comerciais aos termos de regulamentação da ANPD. Ou seja, de antemão, transferiu o papel

de definição do que ao certo é considerado segredo comercial e industrial, e, portanto, apesar de tratar-se exceção ao fortalecimento do campo de atuação do titular de dados e direito dos agentes de tratamento, evita que a sua utilização se dê de forma arbitrária.

Ainda, há de ser considerada na análise da efetividade do instituto do consentimento frente à proteção de dados à luz da LGPD, a complexidade em volta de todo fluxo informacional, que em conjunto com o tratamento massivo e desenfreado de dados pessoais resulta em uma verdadeira evasão ao consentimento. Ainda, mesmo com o fornecimento de informações completas e coerentes acerca dos riscos da atividade de tratamento, bem como das técnicas que vão ser utilizadas pelos agentes para a mitigação destes riscos, a assimetria informacional e a vulnerabilidade do cidadão são elementos próprios do mercado informacional. Destarte, o mencionado descaso normativo em relação às formas pelas quais o consentimento deveria ser operacionalizado (adjetivações) pode ser visto de forma clara nos contratos de adesão.

Neste segmento, os termos de uso e políticas de privacidade dos sites configuram-se nada mais do que uma falsa proposta de participação do titular no processo de tratamento dos seus dados ao fazê-lo "concordar" com o compartilhamento dos seus dados pessoais com apenas um 'click'. A presença de textos longos e de difícil compreensão agrava ainda mais a dificuldade de o titular de dados racionalizar um processo de tomada de decisões. Percebe-se, da análise da abusividade dos termos de uso em geral, que um direito à autodeterminação que se limita ao consentimento não é capaz de solucionar a desproteção dos dados pessoais dos usuários. Aqui entra em jogo o dever de os agentes de tratamento facilitarem o processo cognitivo dos titulares de dados em relação ao tratamento de dados e à sua privacidade.

Por fim, conclui-se que, no que pese a instituição de um regramento específico para o instituto do consentimento na LGPD, visando o empoderamento dos indivíduos no processo de tomada de decisões a respeito do tratamento de seus dados pessoais, fazendo com que eles exerçam certo domínio de seus dados inclusive nas hipóteses em que o consentimento não seria a base legal para o tratamento, há de ser considerada, principalmente, a posição de vulnerabilidade do titular de dados na referida relação. Portanto, uma análise da regularidade do tratamento de dados quando da necessidade do consentimento não deve se pautar somente no fornecimento da declaração de vontade em favor da operação pelo titular de dados, mas também, se o fluxo informacional em questão é integro. No que se refere à autodeterminação informativa como um dos fundamentos previstos no art. 1º, II, da Lei, a garantia de tal direito focado exclusivamente no consentimento, diante das assimetrias do mercado informacional, gera uma mistificação de um adequado controle pelo titular de seus dados pessoais.

Uma carga principiológica pautada na atuação do titular de dados, o que pode ser visto na menção expressa do titular em seis dos nove princípios da Lei, e a necessidade de observação destes princípios independentemente da base legal utilizada pelo agente de tratamento demonstra o papel de protagonismo do titular de dados na LGPD, sendo o consentimento o mecanismo mais relevante para a tutela dos seus dados. Neste ponto, o legislador se preocupou em criar um regramento jurídico liberal, posição que, por lógica, não condiz com a dinâmica de poder existente entre os agentes de tratamento e o titular de dados. No entanto, diante da vulnerabilidade do titular de dados, uma maior intervenção por parte da ANPD no ponto de vista normativo, ou até mesmo através da criação de políticas públicas, será essencial na equalização da referida assimetria do mercado informacional e na garantia de uma verdadeira autonomia ao titular de dados, garantindo uma maior efetividade à utilização do instituto do consentimento como um mecanismo para a proteção de dados pessoais. Assim, ao mesmo tempo em que haveria um empoderamento do titular de dados pessoais, a maior intervenção garantiria que a proteção de dados pessoais não fique sobre cargo do titular de forma desarrazoada.

REFERÊNCIAS

ACQUAVIVA, Marcus Claudio. **Dicionário jurídico brasileiro Acquaviva.** 9 ed. Rev., atual. e ampl. São Paulo: Editora Jurídica Brasileira, 1998.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and rationality in individual decision making. ***IEEE Securty & Privacy Review***, jan./fev. 2005. Disponível em: https://ieeexplore.ieee.org/abstract/document/1392696. Acesso em: 10 jul. 2020.

ALVES, Fabricio da Mota. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019.

BANDEIRA DE MELLO, Celso Antonio. **Curso de Direito Administrativo.** 33 ed. São Paulo: Editora Malheiros, 2016.

BAROCAS, Solon; NISSENBAUM, Helen. **The Trouble with Notice and Consent.** p.3. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409. Acesso em: 10 jul. 2020.

BASTOS, Celso Ribeiro. **Curso de Direito Constitucional.** 15 ed. São Paulo: Editora Saraiva, 2020.

BATISTA, Adonis. Você sabe o que são cookies? Conheça os 3 tipos. **Blog Hariken.co,** 2019. Disponível em: https://blog.hariken.co/voce-sabe-o-que-sao-cookies-na-internet-conheca-os-3-tipos/. Acesso em: 20 jul. 2020.

BELLAVISTA, Alessandro. *Quale legge sulle banche datti?* **Rivista Critica del Diritto Privato,** n. 03, 1991.

BENJAMIN, Antonio Herman de Vasconcellos. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto.** 5 ed. Rio de Janeiro: Editora Forense Universitária, 1997.

BENNET, Colin. ***Regulating privacy, data protection and public policy in Europe and the United States.*** Ithaca: Cornell University Press, 1992.

BENNETT, Colin. ***Regulating Privacy.*** Ithaca: Cornell University Press, 1992.

BESSA, Leonardo Roscoe. **Cadastro positivo:** comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Editora Revista dos Tribunais, 2011.

BIONI, Bruno Ricardo. Projeto de Lei 215/2015, infanticídio aos recém-nascidos direitos digitais no Brasil. ***Digital Rights***, n. 28, out. 2015. Disponível em: https://www.digitalrightslac.net/pt/proyecto-de-ley-2152015-infanticidio-contra-los-recien-nacidos-derechos-digitales-en-brasil/. Acesso em: 17 mar. 2020.

_____. **Proteção de dados pessoais:** a função e os limites do consentimento. 2 ed. Rio de Janeiro: Editora Forense, 2020.

_____. Dados “anônimos” como antítese de dados pessoais: o filtro da razoabilidade. **Revista GENJurídico,** 2019. Disponível em: http://genjuridico.com.br/2019/10/11/dados-anonimos-antitese-dados-pessoais/. Acesso em: 15 abr. 2020.

_____. **Xeque-mate:** o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: Editora Saraiva, 2015.

BRANCO, Sérgio. **Memória e esquecimento na internet.** Porto Alegre: Editora Arquipélago, 2017.

BRASIL MARKENSINIS (Org.). **Protecting privacy.** Oxford: Oxford University Press, 1999.

BRASIL. Câmara dos Deputados. Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei nº 4060, de 2012 [Tratamento de Dados Pessoais]. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=. Acesso em: 10 jun. 2020.

_____. Conselho da Justiça Federal. **Enunciado 531.** Disponível em: https://www.cjf.jus.br/cjf/noticias/2013/abril/enunciado-trata-do-direito-ao-esquecimento-na-sociedade-da-informacao#:~:text=O%20Enunciado%20531%20diz%20que,%C3%A0%20dignidade%20da%20pessoa%20humana. Acesso em: 10 jun. 2020.

_____. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 jun. 2020.

_____. **Guia de boas práticas da Lei Geral de Proteção de Dados.** Brasília, DF. 2020. P. 41. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 10 jun. 2020.

_____. **Lei Federal nº 12.527,** de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 maio. 2020.

_____. **Lei nº 10.406,** de 10 de janeiro de 2002. Institui o Código Civil. 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 20 jun. 2020.

_____. **Lei nº 12.965,** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF. 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 abr. 2020.

_____. **Lei nº 13.105,** de 16 de março de 2015. Código de Processo Civil. Brasília, DF. 16 mar. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 maio. 2020.

_____. **Lei nº 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jun. 2020.

_____. **Lei nº 3.071,** de 1º de janeiro de 1916. Código Civil dos Estados Unidos do Brasil. Rio de Janeiro, RJ. 01 jan. 1916. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L3071.htm. Acesso em: 10 abr. 2020.

_____. **Lei nº 5.172,** de 25 de outubro de 1966. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília, DF. 25 out. 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em: 10 abr. 2020.

_____. **Lei nº 8.069,** de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF. 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 08 jun. 2020.

_____. **Lei nº 8.078,** de 11 de setembro de 1990. Dispõe sobre a proteção ao consumidor e dá outras providências. Brasília, DF. 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2020.

_____. **Medida Provisória nº 869,** de 28 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2008, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF. 28 dez. 2018. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 20 jun. 2020.

_____. Ministério da Justiça. **Decolar.com é multada por prática de *geopricing* e *geoblocking*:** decisão inédita do Departamento de Proteção e Defesa do Consumidor (DPDC) obriga empresa a pagar R$ 7,5 milhões. 18 jun. 2018. Disponível em: http://www.Justiça.gov.br/News/collective-nitf-content-51. Acesso em: 06 jun. 2020.

_____. **Projeto de Lei nº 5276,** de 13 de maio de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília, DF. 13 maio. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 20 jun. 2020.

_____. **Projeto de Lei nº 53,** de 01 de junho de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF. 01 jun. 2018. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 20 jun. 2020.

_____. **Projeto de Lei nº 5762, de** 30 de dezembro de 2019. Altera a Lei nº 13.709, de 2018, prorrogando a data de entrada em vigor de dispositivos da Lei Geral de Proteção de

Dados Pessoais – LGPD – para 15 de agosto de 2022. Brasília, DF. 30 dez. 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704. Acesso em: 20 jun. 2020.

_____. Superior Tribunal de Justiça. Recurso Especial nº 22.337/RS. Relator: Ministro Ruy Rosado de Aguiar. Data de julgamento: 20 mar. 1995.

_____. Supremo Tribunal Federal. Recurso Extraordinário nº 1.010.606/RJ. Relator: Ministro Dias Toffoli. Recorrente: Nelson Curi. Recorrido: Globo Comunicação e Participações S/A. Disponível em: http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786. Acesso em: 10 jan. 2020.

_____. Supremo Tribunal Federal. Referendo na medida cautelar na Ação Direta de Inconstitucionalidade nº 6.389/DF. Requerente: Partido Socialista Brasileiro. Intimado: Presidente da República. Relatora: Ministra Rosa Weber. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em: 18 jul. 2020.

_____. Tribunal de Justiça de São Paulo. Apelação Cível nº 108339-32.2015.8.26.0100. Relator: Desembargador Antonio Nasciento. Data de julgamento: 25 ago. 2016.

_____. Tribunal de Justiça de São Paulo. Mandado de Segurança nº 2073993-57.2014.8.26.0000. Relator: Desembargador Edison Brandão. Data de julgamento: 16 dez. 2014.

_____. Tribunal de Justiça do Rio Grande do Sul. Apelação cível nº 70079524351. Relator: Gelson Rolim Stocker. 17ª Câmara Cível. Data de julgamento: 28 mar. 2019. Data de publicação: 02 abr. 2019.

BRITO CRUZ, Franscisco. **Direito, democracia e cultura digital:** a experiência de elaboração legislativa do marco civil da internet. Dissertação (Mestrado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, São Paulo, 2009.

BRUNO, Marcos G. da Silva, **LGPD:** Lei Geral de Proteção de Dados comentada. MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. (Coord.). São Paulo: Editora Thomson Reuters, 2019.

CARBONE, Vicenzo***. Il consenso, anzi i consensi, nel tratamento informático dei dati personali. Danno e responsabilità,*** n.1, 1998.

CASTRO, Catarina Sarmento. **Direito da informática, privacidade e dados pessoais.** Coimbra: Editora Almedina, 2005.

COMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.** 21 jan. 2019. Disponível em: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Acesso em: 20 jul. 2020.

CORRÊA, Leonardo. É importante não perder o foco da segurança jurídica no âmbito da LGPD. **Revista Consultor Jurídico.** 03 mar. 2019. Disponível em: www.conjur.com.br/2019-mar-03/Leonardo-correa-segurança-jurídica-ambito-lgpd. Acesso em: 23 jun. 2020.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** São Paulo: Editora Revista dos Tribunais, 2018.

CRANOR, Lorrie Faith; MCDONALD. Aleecia M. ***Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising.*** Disponível em: < https://www.researchgate.net/publication/228237033_Beliefs_and_Behaviors_Internet_Users'_Understanding_of_Behavioral_Advertising. Acesso em: 10 jul. 2020.

DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. **Revista de la Faculdad de derecho de la Pontifícia Universidad Católica Del Peru**, n. 51, 1997.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo.** Rio de Janeiro: Editora Forense, 2018.

DONEDA, Danilo. **A autonomia do direito fundamental de proteção de dados.** São Paulo: Editora Revista dos Tribunais, 2019.

_____. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Editora Thomson Reuters Brasil, 2019.

_____. Princípios de proteção de dados pessoais. *In:* LUCCA, Newton de; SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e Internet III:** Marco civil de internet. São Paulo: Editora Quartier Latin, 2015.

EUROPEAN COMISSION. ***Article 29 Working Party.*** Disponível em: https://ec.europora.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 15 mar. 2020.

FEDERAL TRADE COMISSION. **Do not call registry.** Disponível em: https://www.donotcall.gov/report.html. Acesso em: 18 abr. 2020.

FERRAZ JR, Tércio S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, vol. 88, 1993.

FIORELLA, Sam. ***The insidiousness of Facebook Messenger's android mobile app permissions.*** Disponível em: https://pt.slideshare.net/plantquack3480/the-insidiousness-of-facebook-messengers-android-mobile-app-permissions-updatedsam-fiorella. Acesso em: 13, jul., 2020.

FRAZÃO, Ana. Lei Geral de Proteção de Dados Pessoais: direitos básicos dos titulares de dados pessoais. **Revista do Advogado nº 144,** AASP, 2019.

_____. O direito a explicação e à oposição diante de decisões totalmente automatizadas. **Revista JOTA.** 05 dez. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018#_ftn2>. Acesso em: 20 jun. 2020.

FROSINI, Vittorio. ***Contributi ad um diritto dell'informazione.*** Napoli: Liguiro, 1991.

G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA.** Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 19 abr. 2020.

GAMBOGI CARVALHO, Ana Paula. O consumidor e o direito à autodeterminação informacional. **Revista de Direito do Consumidor,** n. 46, 2003.

GAMBOGI, Ana Paula. O Consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. *In*: MARQUES, Claúdia Lima; MIRAGEM, Bruno (Org.). **Coleção doutrinas essenciais: direito do consumidor –** proteção da confiança e práticas comerciais. São Paulo: Editora Revista dos Tribunais, vol. 3, 2011.

GEORGITON, Peter V. The FBI's Carvnivore: how federal agents may be viewing your personal e-mail and why there is nothing you can do about it. ***Ohio State Law Journal,*** vol. 62, n. 06, 2001.

GOMES, Orlando. **Contratos de adesão:** condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972.

_____. **Contratos.** 26 ed. 2 tir. Rio de Janeiro: Editora Forense, 2008.

GUEDES, Gisela Sampaio da Cruz. **Regime de Responsabilidade adotado pela lei de proteção de dados brasileira.** São Paulo: Editora Revista dos Tribunais, 2019.

HEINEN, Juliano. **Interesse público:** premissas teórico-dogmáticas e proposta de fixação de cânones interpretativas. 1 ed. Salvador: Editora JusPodivm, 2018.

HERN, Alex. *Samsung rejects concern over 'Orwellian' privacy policy*. Fev. 2015. **The Guardian.** Disponível em: **https://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy#:~:text=Users%20of%20Samsung's%20Smart%20TV,the%20television%20is%20plugged%20in.** Acesso em: 13 jun. 2020.

INFORMATIONAL COMISSIONER'S OFFICE. **Global survey finds 85% of mobile apps fail to provide basic privacy information.** Disponível em https://www.wired-gov.net/wg/news.nsf/articles/Global+survey+finds+85+of+mobile+apps+fail+to+provide+basic+privacy+information+10092014151000?open. Acesso em: 13 jul. 2020.

INGLATERRA. Information Comissioner's Office. **Informe.** Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#5. Acesso em: 18 abr. 2020.

JIMENE, Camila do Valle. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

JUNQUEIRA, Thiago; CHALFIN, Ricardo. Covid-19 e a postergação da LGPD: histeria ou sabedoria? **Revista Consultor Jurídico.** 21 abr. 2020. Disponível em: https://www.conjur.com.br/2020-abr-21/opiniao-covid-19-postergacao-lgpd-histeria-ou-sabedoria#sdfootnote4sym. Acesso em: 27 jun. 2020.

KOSINSKI, Michael. *Private traits and attributes are predictable from digital records of human behavior*. ***Proceedings of the National Academy of Sciences,*** vol. 110, n. 15, 2013.

LEMOS, Renato. GDPR: A nova legislação de proteção de dados da Europa. **AB21.** 20 jun. 2018. Disponível em: https://www.ab2l.org.br/gdpr-nova-legislacao-de-protecao-de-dados-pessoais-da-europa/. Acesso em: 04 jul. 2020.

LEMOS, Ronaldo. **Debater a Lei Geral de Proteção de Dados é refletir sobre o futuro, afirma Ministro Salomão.** 26 ago. 2019. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Debater-a-Lei-Geral-de-Protecao-de-Dados-e-refletir-sobre-o-futuro--afirma-ministro-Salomao.aspx. Acesso em: 29 jun. 2020

LEONARDI, Marcel. **Principais bases legais de tratamento de dados pessoais no setor privado.** São Paulo: Editora Revista dos Tribunais, 2019.

_____. **Tutela e privacidade na internet.** São Paulo: Editora Saraiva, 2012.

LIMA, Adriano. **Gestão da segurança e infraestrutura de tecnologia da informação.** São Paulo: Editora Senac, 2018.

LIMA, Caio. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019.

LIMA, Cíntia Rosa Pereira. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. **Revista dos Tribunais,** vol. 946, 2014.

LLAMBÍAS, Jorge Joaquín. **Tratado de derecho civil.** Tomo III. Buenos Aires: Editorial Perrot, 1973, p. 718.

LUCCA, Newton de. Marco Civil da Internet: uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. *In:* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.) **Direito & Internet III:** Marco Civil da Internet. São Paulo: Editora Quartier Latin, 2015.

MALDONADO, Viviane Nóbrega. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019.

MAÑAS, José Luis Piñar. *El derecho fundamental a la protección de datos personales (LOPD). In:* MAÑAS, José Luis Piñar (Org.). ***Protección de datos de carácter personal en Iberoamérica.*** Valencia: Tirant Lo Blanch, 2005.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor:** o novo regime das relações contratuais. São Paulo: Editora Revista dos Tribunais, 2011.

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

MARZAGÃO, Nelcina C. de O. Tropardi. **Da informação e dos efeitos do excesso de informação no direito do consumidor.** Tese (Doutorado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, São Paulo, 2005.

MAYER-SCHONEBERGER, Viktor. *Generational development of data protection in Europe. In*: AGRE, Phillip E,: ROTENBERG, Marc (Org.). ***Technology and Privacy:*** The New Landscape. Cambridge: The MIT Press, 1997.

_____; CUKIER, Kenneth. ***Big data:*** *a revolution will transform how we live, work and think.* New York: Hougton Miffin Publishing, 2013, p. 176.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. *The cost of Reading Privacy Policies.* ***Journal of law and Policy for information society,*** v. 4, 2008.

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia. **Direito, inovação e tecnologia.** Vol. 01. São Paulo: Editora Saraiva, 2015.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça,** 2018.

_____. **A Lei Geral de Proteção de Dados Pessoais:** um modelo de aplicação em três níveis. São Paulo: Editora Revista dos Tribunais, 2019.

_____. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais: novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. **Portal JOTA**. 10 maio. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020#_ftnref8. Acesso em: 18 jul. 2020.

_____. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.

_____. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de Brasília, Brasília, Distrito Federal, 2008. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf. Acesso em: 10 abr. 2020.

_____; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados.** São Paulo: Editora Revista dos Tribunais, 2019.

MESSINETI, Davide. Circolazioni di dati personali e dispositivi di regolazione dei poteri individuali. ***Rivista Critica Del Diritto Privato,*** 1998.

MIRAGEM, Bruno. **Curso de direito do consumidor.** 6 ed. Rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2006.
MIRANDA, Custódio da Piedade Ubaldino. **Contratos de Adesão.** São Paulo: Atlas, 2002.

MONCAU, Luiz Fernando Marrey. Direito ao esquecimento. São Paulo: Editora Thomson Reuters, 2018.

MONTEIRO, Washington de Barros. **Curso de Direito Civil:** parte geral. Vol. 01. São Paulo: Editora Saraiva, 2012.

MORAES, Maria C. Bodin de. **Risco, solidariedade e responsabilidade objetiva.** São Paulo: Editora Revista dos Tribunais, 2006.

MOREIRA, André de Oliveira Schenini. A exceção dos dados pessoais tornados manifestamente públicos pelo titular na LGPD. **Migalhas.** 07 jan. 2019. Disponível em: https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd**.** Acesso em: 16 jul. 2020.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust. ***De-anonymization of large sparse datasets.*** 2007. Disponível em: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf. Acesso em: 14 jun. 2020.

ODLYZKO, Andrew. *Privacy, economics, and price discrimination on the internet.* ***Fifth International Conference on Eletronic Commerce.*** *2003.* Disponível em: http://ssrn.com/abstract=429762. Acesso em: 14 jun. 2020.

OLIVEIRA, Caio César de. **A Lei Geral de Proteção de Dados Pessoais e um 'direito ao esquecimento' no Brasil.** São Paulo: Editora Revista dos Tribunais, 2019.

OPSAHL, Kurt. Facebook's Eroding Privacy Policy: a timeline. **Eletronic Frontier Foundation.** Disponível em: https://www.eff.org/deeplinks/2010/04/facebook-timeline. Acesso em: 13 jul. 2020.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 jul. 2020.

PANEBIANCO, Mario. *Bundesverfassungsgerich, dignitá umana e diritti fondamentali*. ***Diritto e Societá,*** n. 02, 2000.

PASQUALE, Frank. ***The black box society:*** *the secret algorithm's that control money and information.* Cambridge: Harvard University Press, 2015.

RESTA, Giordio. *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali.* ***Rivista Critica del Diritto Privato***, 2000.

RODATÁ, Stefano. **A vida na sociedade da vigilância.** DONEDA, Danilo; DONEDA, Luciana Cabral (Trad.). Rio de Janeiro: Editora Renovar, 2008.

_____. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Editora Renovar, 2008.

_____. ***Repertorio di fine secolo.*** Bari: Laterza, 1999.

ROSEN, Jeffrey. ***The unawanted gaze.*** New York: Random House, 2000.

ROSSO, Angela Maria. LGPD e setor público: aspectos gerais e desafios. **Revista Migalhas.** Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios. Acesso em: 17 jun. 2020.

SIQUEIRA JR., Paulo Hamilton. **Teoria do Direito.** São Paulo: Editora Saraiva, 2009, p.218.

SOLOVE, Daniel J. ***The digital person****: technology and privacy in the information age*. New York: New York University Press, 2004, p.46.

SOUSA, Carlos Affonso Pereira de. Mau uso do direito ao esquecimento deve ficar no radar. **Revista Migalhas.** 10 maio. 2019. Disponível em: https://www.migalhas.com.br/quentes/300036/mau-uso-do-direito-ao-esquecimento-deve-ficar-no-radar-alerta-professor-carlos-affonso. Acesso em: 10 jun. 2020.

SOUZA, Carlos Affonso; PADRÃO, Vinicius. **Incidentes de segurança e dever de notificação à luz da Lei Geral de Proteção de Dados Pessoais.** São Paulo: Editora Revista dos Tribunais, 2019.

SWIRE, Peter; LITAN, Robert. ***None of your business.*** Washington: Brookings Institution Press, 2010.

TASSO, Fernando Antonio. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Editora Thomson Reuters Brasil, 2019.

TAVERES, Monica. Após espionagem, Dilma pede urgência de votação do Marco Civil da Internet. **Jornal O Globo.** 11 set. 2013. Disponível em: http://oglobo.globo.com/sociedade/tecnologia/apos-espionagem-dilma-pede-urgencia-de-votação-do-marco-civil-da-internet-9912712. Acesso em: 19 abr. 2020.

TEFFÉ, Chiara Spadaccini de. **Tratamento de dados pessoais de crianças e adolescentes: proteção e consentimento.** São Paulo: Editora Revista dos Tribunais, 2019.

TEICH, Nelson. ***COVID-19*****: histeria ou sabedoria?** Disponível em: https://www.linkedin.com/pulse/covid-19-histeria-ou-sabedoria-nelson-teich/. Acesso em: 27 jun. 2020.

TEPEDINO, Gustavo. **Temas de Direito Civil.** Rio de Janeiro: Editora Renovar, 1999.

THEODORO JUNIOR, Humberto. **Comentários ao novo Código Civil:** dos defeitos do negócio jurídico. Rio de Janeiro: Editora Saraiva, 2013.

TOEWS, Mario. LGPD, responsabilidade solidária e ações regressivas. **IT Forum 365 – a voz da TI.** 02 abr. 2020. Disponível em: https://itforum365.com.br/colunas/lgpd-responsabilidade-solidaria-e-acoes-regressivas/#:~:text=Esse%20%C3%A9%20um%20caso%20de,Prote%C3%A7%C3%A3o%20de%20Dados%20(LGPD).&text=No%20par%C3%A1grafo%204%C2%BA%2C%20estabelece%20o,%C3%A0%20responsabiliza%C3%A7%C3%A3o%20e%20%C3%A0%20indeniza%C3%A7%C3%A3o.. Acesso em: 24 jun. 2020.

UNIÃO EUROPEIA. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho,** de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações eletrônicas (Directiva relacionada à privacidade e às comunicações electrónicas). 12 jul. 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058. Acesso em: 20 jul. 2020.

_____. **Directiva 95/46/CE do Parlamento Europeu e do Conselho,** de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20 maio. 2020.

_____. ***General Data Protection Regulation.*** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020

_____. **Regulamento Geral de Proteção de Dados.** Disponível em: https://gdpr.algolia.com/pt/gdpr-article-3. Acesso em: 10 jun. 2020.

UNITED STATES OF AMERICA. **47 U.S. CODE § 521.** Purposes. Disponível em: https://www.law.cornell.edu/uscode/text/47/521. Acesso em: 10 maio. 2020.

_____. **5 U.S CODE § 552.** Public information; agency rules, opinions, orders, records, and proceedings. Disponível em: https://www.law.cornell.edu/uscode/text/5/552. Acesso em: 10 maio. 2020.

UTZ, Christine; DEGELING, Martin; FAHL, Sascha; SCHAUB, Florian; HOLTZ, Thorsten. (Un)informed consent: studying GDPR consent notices in the field. *In*: 2019 ACM SIGSAC **Conference on Computer and Communications Security (CC' 19)**, November 11-15, 2019, London, United Kingdom. ACM, New York, NY, USA. Disponível em: <https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentichungen/2019/09/05/uninfomed-consent_Yl7FPEh.pdf>. Acesso em: 20 jul. 2020.

VAINZOF, Rony. LGPD: **Lei Geral de Proteção de Dados comentada.** São Paulo: Editora Thomson Reuters Brasil, 2019.

VIEIRA, Débora. O que você precisa saber sobre a lei geral de proteção de dados. **Migalhas,** 01 ago. 2018. Disponível em: https://www.migalhas.com.br/depeso/284723/o-que-voce-precisa-saber-sobre-a-lei-geral-de-protecao-de-dados. Acesso em: 29 jun. 2020.

VITAL, Alan. **Práticas de Compliance e a LGPD.** 2019. Disponível em: https://vitaladvocacia.com.br/praticas-de-compliance-e-a-lgpd/. Acesso em: 28 jun. 2020.
WESTIN, Alan F. ***Privacy and Freedom.*** New York: Atheneum, 1970.

ZANATTA, Rafael A. F. **Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor.** São Paulo: Editora Revista dos Tribunais, 2019.