

## DIREITOS DO TITULAR DE DADOS: POTENCIALIDADES E LIMITES NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS<sup>1</sup>

### RIGHTS OF THE DATA SUBJECT: POTENTIALITIES AND LIMITS IN THE BRAZILIAN GENERAL DATA PROTECTION LAW

Maria Regina Rigolon Korkmaz<sup>2</sup>  
Mariana Sacramento<sup>3</sup>



**RESUMO:** Atualmente, múltiplos desafios são enfrentados no cenário dos progressivos avanços tecnológicos e da ostensiva coleta de dados pessoais. Considerando a integração dos dados pessoais ao corpo eletrônico da pessoa, com base na referência teórica de Stefano Rodotà, o presente artigo teve por fim, a partir de uma abordagem exploratória, analisar os chamados direitos dos titulares, dispostos na Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709 de 2018), uma vez considerado que a proteção de dados pessoais se apresenta como chave para a tutela de diversos direitos na era digital. Para compor a investigação, com um caráter eminentemente comparativo, a análise passou pelo Regulamento Europeu de Proteção de Dados (Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia), tendo em vista que modelo da União Europeia representa a grande influência exógena da normativa brasileira nesse campo. Portanto, a partir de uma interpretação sistemática do marco regulatório brasileiro, foi possível concluir que, embora sejam reconhecidas determinadas limitações, há a previsão de um importante campo de tutela da pessoa com a referência da autodeterminação informativa. Ademais, foi possível depreender da norma a existência de um significativo espaço para a atuação da Autoridade Nacional de Proteção de Dados nesse cenário, sobretudo com relação a integração, interpretação e fiscalização.

**PALAVRAS-CHAVE:** Direitos dos titulares. Proteção de dados pessoais. Privacidade. Autodeterminação informativa.

**ABSTRACT:** Currently, multiple challenges are faced within the scenario of progressive technological advances and the massive collection of personal data. Considering the integration of personal data and the person's electronic body, based on the theoretical reference of Stefano Rodotà, this article aimed, from an exploratory approach, to analyze the so-called rights of the data subject, provided by the Brazilian General Data Protection Law (Law n°. 13,709 of 2018), being data protection key to safeguard several rights in the digital age. To improve the investigation, with an eminently comparative character, the analysis considered also the General Data Protection Regulation (Regulation – EU – 2016/679 of the European Parliament and of the Council), taking into consideration that the European Union model represents the

<sup>1</sup> Agradecemos às valiosas contribuições dos Professores Carlos Affonso Souza e Danilo Doneda, bem como dos colegas, na disciplina “Lei Geral de Proteção de Dados Pessoais”, ministrada no âmbito do Programa de Pós-Graduação *Stricto Sensu* em Direito – Doutorado em Direito Civil - da Universidade do Estado do Rio de Janeiro.

<sup>2</sup> Doutoranda em Direito Civil pela Universidade do Estado do Rio de Janeiro – UERJ. Mestre em Direito e Inovação pela Universidade Federal de Juiz de Fora - UFJF. Advogada. Membro do Observatório de Legislação e Jurisprudência da Comissão de Direito Privado e Novas Tecnologias do Conselho Federal da Ordem dos Advogados do Brasil.

<sup>3</sup> Doutoranda em Direito Civil pela Universidade do Estado do Rio de Janeiro – UERJ. Mestre em Direito pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio. Professora. Advogada.

major exogenous influence of the Brazilian regulation at this field. Therefore, from a systematic interpretation of the Brazilian regulatory framework, it was possible to conclude that, despite recognized limitations, there is the provision of an important field to protect the person with the reference of informational self-determination. Furthermore, it was possible to infer from the regulation the existence of a significant space for the Brazilian National Data Protection Authority to act in this field, especially regarding integration, interpretation and oversight.

**KEYWORDS:** Rights of the data subject. Data protection. Privacy. Informational self-determination.

**SUMÁRIO:** Introdução. 1. A confirmação da existência do tratamento e o acesso aos dados. 2. A correção de dados incompletos, inexatos ou desatualizados. 3. A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD. 4. A portabilidade de dados pessoais. 5. A eliminação de dados pessoais. 6. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados. 7. Informação sobre a possibilidade de não fornecer o consentimento, as consequências da negativa e a revogação do consentimento. 8. Prerrogativas diante das decisões automatizadas. 9. Conclusão. Referências.

**SUMMARY:** Introduction. 1. The confirmation of the existence of data processing and access to personal data. 2. The rectification of incomplete, inaccurate or outdated data. 3. The anonymization, blockage or erasure of unnecessary or excessive data or data processed in non-compliance with the LGPD. 4. The right to data portability. 5. The erasure of personal data. 6. The information of public and private entities with which the controller has shared personal data. 7. The information about the possibility of not providing consent, such as the consequences of denial and the revocation of consent. 8. Prerogatives upon automated decision-making. 9. Conclusion. References.

## Introdução

Frank Pasquale, no livro *The black box society*, publicado pela *Harvard University Press*, relata o caso de Catherine Taylor, residente no estado de Arkansas, nos Estados Unidos, a qual foi incorretamente associada a uma acusação criminal de intenção de vender e manufaturar metanfetamina. O responsável pela indevida associação foi o *data broker* ChoicePoint.

A circulação dessa informação repercutiu na imediata rejeição de todas as submissões de Catherine em seleções profissionais. Uma vez notificada a ChoicePoint, a informação foi suprimida. No entanto, tal supressão não ocorreu para os agentes com os quais o *data broker* havia compartilhado os dados, vários dos quais Catherine teve que pedir a remoção da equívoca acusação criminal, tendo, inclusive, recorrido à via judicial. Mesmo após as correções que puderam ser identificadas e realizadas, ela levou quatro anos para conseguir um emprego e foi rejeitada para a compra de um apartamento, o que a levou a ter que morar

com a irmã, além de ter exacerbados seus problemas cardiológicos.<sup>4</sup>

O diagnóstico de Pasquale do cenário contemporâneo é o de que os controladores de dados elaboram e estimulam um sistema não de respeito aos direitos das pessoas, mas orientado pela maximização de lucro e pela elevação da inovação acima de qualquer valor.<sup>5</sup>

Emerge, assim, a imprescindibilidade da agenda de proteção de dados pessoais para a proteção de diversos direitos, bem como, em específico, o significativo papel que a sistemática dos direitos dos titulares de dados pode representar nesse campo. Stefano Rodotà já advertia que a proteção de dados pessoais pode ser lida como o direito fundamental mais expressivo da condição humana contemporânea,<sup>6</sup> na medida em que se apresenta como chave para que diversos direitos e garantias sejam assegurados na era da informação.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709 de 2018) – primeiro marco regulatório geral brasileiro sobre o tema – apresenta, entre seus fundamentos, a promoção dos direitos fundamentais da pessoa natural, sobretudo a liberdade, a privacidade e o livre desenvolvimento da personalidade. Os paradigmas de que os dados pessoais integram o corpo eletrônico da pessoa, na síntese de Rodotà,<sup>7</sup> ou, como esclarece Danilo Doneda, constituem o espelho representativo da personalidade<sup>8</sup> e viabilizam compreender as bases sobre as quais é estruturada a regulação brasileira.

A intrínseca associação que se estabelece entre a pessoa humana e seus dados demanda mecanismos disponíveis para garantir essa proteção. Isso porque, em atenção às demandas contemporâneas, a clássica sequência “pessoa-informação-sigilo” é superada para alcançar a noção de “pessoa-informação-circulação-controle”, na qual o imperativo é a circulação controlada de dados.<sup>9</sup> Para além da privacidade, a proteção de dados se lança em bases de proteção mais objetivas, dinâmicas e também coletivas.<sup>10</sup>

Apesar de o paradigma do controle individual ser insuficiente, razão pela qual este

---

<sup>4</sup> PASQUALE, Frank. *The black box society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015, p. 33-34.

<sup>5</sup> PASQUALE, Frank. *The black box society*, cit., p. 146.

<sup>6</sup> RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008. Tradução: Danilo Doneda e Luciana Cabral Doneda, p. 21.

<sup>7</sup> RODOTÀ, Stefano. Transformações do corpo. *Revista Trimestral de Direito Civil*, v. 19, p. 91-107, 2004.

<sup>8</sup> DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

<sup>9</sup> RODOTÀ, Stefano. *A vida na sociedade da vigilância*, cit., p. 93.

<sup>10</sup> Como define Rodotà, a partir da experiência europeia, a privacidade como direito complexo insere no seu conteúdo a autodeterminação informativa, entendida como o “direito de manter controle sobre as suas informações e de determinar a maneira de construir sua esfera particular”. Por esfera privada entende-se “aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo” (RODOTA, Stefano. *A vida na sociedade da vigilância*, cit., p. 15, 92).

deve ser coordenado com o controle na esfera coletiva,<sup>11</sup> a atribuição de prerrogativas ao titular dos dados representa um importante vetor no sentido de se entrelaçar o propósito de tutela da pessoa a partir dos seus dados com o exercício de sua autodeterminação informativa. É nessa direção que a LGPD sistematiza, sobretudo em seu capítulo III, as disposições referentes aos “Direitos do titular”,<sup>12</sup> embora o tratamento normativo desses direitos esteja disperso pela LGPD, orientando-se, especialmente, pela principiologia da norma.<sup>13</sup>

Tanto a importância que a temática dos direitos dos titulares ganha no cenário da proteção de dados quanto suas potencialidades podem ser ilustradas, por exemplo, com a extensão pela Itália, no *Codice in materia di protezione dei dati personali*, de direitos dos titulares previstos no *General Data Protection Regulation (GDPR)* – ou Regulamento Europeu de Proteção de Dados (Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia) – a um rol de legitimados para a proteção póstuma do titular.<sup>14</sup>

Vale dizer, o imperativo de controle da pessoa sobre suas informações, enquanto um dos fundamentos da LGPD – a autodeterminação informativa (art. 2º, II) –, ganha elementos com maior densidade para proteger a pessoa humana, embora a tutela dos dados pessoais já pudesse, antes desse marco regulatório, ser extraída da ordem jurídica brasileira.

Com efeito, em atenção à ontologia existencial dos dados pessoais e à necessidade de garantir sua tutela, o presente artigo tem por fim explorar determinadas potencialidades e limites do regime jurídico dos direitos dos titulares de dados na LGPD. Para tanto, o GDPR será oportunamente utilizado como referência para a análise, uma vez considerado que a União Europeia é a grande referência exógena do Brasil em termos de proteção de dados.

Enquanto opção metodológica para desenvolver a análise das disposições legais, considerando suas interfaces, algumas das prerrogativas foram investigadas de maneira conjunta. Assim, após a presente introdução, no capítulo primeiro foi abordado o direito de

---

<sup>11</sup> RODOTÀ, Stefano. *A vida na sociedade da vigilância*, cit., p. 37.

<sup>12</sup> No que se refere ao debate sobre a natureza de direitos e de remédios, a partir do art. 18 da LGPD, Eduardo Nunes de Souza e Rodrigo da Guia Silva consideram que: “a ancoragem das medidas e procedimentos previstas no rol do art. 18 ao direito de privacidade (vale dizer, sua instrumentalização a esse direito) mostra-se imprescindível, pois é o direito que, traduzindo valores e interesses, é passível de um juízo de merecimento de tutela. Em outros termos, é possível funcionalizar direitos à axiologia do sistema, mas não remédios legais isoladamente considerados” (SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. *Direitos do titular de dados pessoais na Lei 13.709/2018: uma abordagem sistemática*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 243-286, p. 265, 279).

<sup>13</sup> Cf. FRAZÃO, Ana. *Direitos básicos dos titulares de dados pessoais*. In: *Lei Geral de Proteção de Dados Pessoais. Revista do Advogado*, v. 144, nov. 2019.

<sup>14</sup> Sobre o tema, cf. NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Autonomia privada, portabilidade de dados pessoais e planejamento sucessório*. In: TEIXEIRA, Daniele Chaves (Coord.). *Arquitetura do Planejamento Sucessório*. Belo Horizonte: Fórum, 2021, p. 659-674. Tomo II.

demandar a confirmação da existência do tratamento e o acesso aos dados. O capítulo segundo tratou da correção de dados incompletos, inexatos ou desatualizados. O capítulo terceiro teve por centralidade a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD. Em seguida, o capítulo quarto se dedicou ao debate sobre a portabilidade de dados, ao passo que o capítulo quinto desenvolveu o tema da eliminação dos dados pessoais. O capítulo sexto abordou a prerrogativa de demandar informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados, seguido do capítulo sétimo, direcionado ao requerimento de informação sobre a possibilidade de não fornecer o consentimento, as consequências da negativa, bem como sobre a possibilidade de revogá-lo. O capítulo oitavo endereçou prerrogativas atinentes às decisões automatizadas, seguido da conclusão.

## **1. A configuração da existência do tratamento e o acesso aos dados**

Enquanto referência central das prerrogativas dos titulares na LGPD, o art. 18 dispõe que “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”, assegurando, de plano, o (I) direito à confirmação da existência do tratamento<sup>15</sup> e o (II) acesso aos dados.

Como gradações da materialização da autodeterminação informativa, a confirmação da existência do tratamento de dados se apresenta como um primeiro passo para que diversas prerrogativas do titular sejam efetivamente exercidas, como o próprio direito de acesso, porque confere ao titular a possibilidade de saber que aquele determinado tratamento existe.

A rigor, a confirmação da existência do tratamento e o acesso aos dados podem ser interpretados como densificações do princípio da transparência, o qual estabelece a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”. Em direção complementar, o princípio do livre acesso determina a “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”.

---

<sup>15</sup> Por tratamento de dados se compreende “toda operação realizada com dados pessoais”, conforme estabelecido, através de um rol exemplificativo, no inciso X, do art. 5º, da LGPD.

Como um passo adiante da confirmação da existência do tratamento, o direito de acesso abrange, em uma leitura sistematizada da LGPD, as informações sobre a origem dos dados, a (in)existência de registros, os critérios utilizados e a finalidade do tratamento, seus destinatários, a existência de decisões automatizadas, entre outros, ressalvado o segredo de empresa. Ou seja, para além do acesso aos dados pessoais propriamente ditos, as informações que circundam o tratamento também deverão ser disponibilizadas ao titular, como dispõe o art. 9º, da LGPD, ratificando a principiologia citada.<sup>16</sup> Viviane Nóbrega Maldonado sustenta a possibilidade de se extrair do art. 9º que, independentemente de qualquer requisição, o titular deverá ser informado sobre o início do tratamento dos dados pessoais, concomitantemente ao momento da coleta.<sup>17</sup> O GDPR normatiza expressamente a obrigatoriedade de apresentar informações quando os dados são recolhidos junto ao titular (art. 13), bem como quando não são diretamente coletados junto à pessoa à qual se referem (art. 14).

A propósito, embora a normativa do *caput* do art. 18, da LGPD, possa sugerir, a princípio, a obrigatoriedade do atendimento das requisições formuladas pelo titular em face do controlador, a impossibilidade técnica, operacional ou mesmo jurídica, como o exemplo da proteção do segredo de empresa, pode vir a fundamentar a negativa. Nesse sentido é que se extrai do parágrafo 4º, do art. 18. Todavia, enquanto passo inicial para o princípio da transparência e com recurso interpretativo ao GDPR, não seria admissível a recusa para a confirmação da existência do tratamento de dados. Em adição, o art. 19 apresenta certa procedimentalização para a confirmação da existência de tratamento e para o acesso aos dados, nos seguintes termos:

A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

---

<sup>16</sup> “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; 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”.

<sup>17</sup> MALDONADO, Viviane Nóbrega. Dos direitos do titular. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). *LGPD: lei geral de proteção de dados comentada*. 2. ed. rev. ampl. atual. São Paulo: Thomson Reuters Brasil, 2019. cap. 3. p. 215-245, p. 222.

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

A princípio, verifica-se que a confirmação da existência de tratamento ou o acesso aos dados pessoais deverá ser providenciado imediatamente e em formato simplificado, quando assim for possível. Contudo, em específico para o acesso, quando tal demandar uma declaração clara e completa com as informações apontadas na norma, será admitido um prazo de 15 (quinze) dias, a ser computado a partir do requerimento. Ainda, a norma estabelece o imperativo de armazenamento dos dados em formato que favoreça o exercício do direito de acesso, bem como da possibilidade de as informações poderem ser prestadas por meio eletrônico, se idôneo para a finalidade, ou na forma impressa.

O parágrafo 3º, do art. 19, estabelece o que vem sendo referido como *acesso qualificado*, na medida em que, para além do simples acesso aos dados, quando o tratamento tiver por base o consentimento ou um contrato, o titular poderá solicitar a cópia eletrônica integral de seus dados em formato que permita sua utilização subsequente, desde que respeitado o segredo de empresa. A regulamentação pela Autoridade Nacional de Proteção de Dados (ANPD), nesse ponto, ainda está em aberto.

No âmbito do GDPR, a portabilidade de dados pessoais, desde que atendidos os pressupostos legais, como será endereçado, autoriza a solicitação pelo titular dos dados para que estes sejam transmitidos de um controlador a outro, bem como permite que o próprio titular receba os dados que lhe dizem respeito. Na LGPD, por sua vez, identifica-se uma normatização diversa, na qual a portabilidade, prevista no inciso V, do art. 18, sugere um fluxo informacional entre controladores ao passo que o recebimento dos dados pelo titular foi inserido no dispositivo que trata da confirmação da existência de tratamento e do acesso aos dados.

Nesse campo, a proteção dos segredos comercial e industrial pode representar uma dificuldade jurídica mais sensível para que o exercício do direito de acesso qualificado se dê de forma plena. Isso porque, para além dos dados fornecidos pelo titular, o agente de tratamento poderá ter gerado os chamados dados inferidos<sup>18</sup> a partir das próprias atividades de tratamento,

---

<sup>18</sup> A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) apresenta uma taxonomia dos dados pessoais. Os dados derivados são definidos como aqueles gerados a partir de outros dados, com base em formas significativamente mecânicas, utilizando raciocínios simples e matemática básica para detectar padrões. Apesar da possibilidade de os dados derivados serem utilizados para fins preditivos, não são propriamente baseados em

dos quais a divulgação pode representar algum risco à tutela do segredo de empresa. Esse debate, que será melhor delineado no âmbito do direito à portabilidade, não pode pressupor abstratamente o risco ao sigilo, o qual deverá ser razoavelmente demonstrado para fundamentar a negativa à disponibilização desses dados, sob pena de mitigação desse direito.

Daniela Copetti Cravo sustenta que, a depender da leitura que se faça do art. 19, parágrafo 3º, a configuração do uso desses dados em caráter meramente doméstico poderia autorizar uma ampliação da abrangência dessa prerrogativa para os dados inferidos. Isso porque, em atenção às contingências do ordenamento jurídico brasileiro, para legitimar a tutela do segredo de empresa, a concorrência desleal apenas poderia se configurar diante de um prejuízo concorrencial, o que não poderia ser lido como uma implicação lógica e automática da disponibilização desses dados a qualquer titular, pressupondo-se, irrestritamente, o risco da descoberta da fórmula protegida pelo sigilo através do mero acesso aos dados inferidos.<sup>19</sup> Além de representar uma materialização da autodeterminação informativa, e desde que equilibrados os interesses em questão, a prerrogativa prevista no parágrafo 3º, do art. 19, pode ser de grande valia para o titular, sobretudo em áreas sensíveis, como diante dos dados inferidos referentes à saúde.

## **2. A correção de dados incompletos, inexatos ou desatualizados**

A intrínseca associação entre a pessoa humana e os dados pessoais que lhe dizem respeito, enquanto representação da sua personalidade, justificam a prerrogativa de corrigir, junto ao controlador, os dados incompletos, inexatos ou desatualizados. As prerrogativas anteriormente exploradas, quais sejam, a de ter conhecimento sobre a existência do tratamento dos dados e a de acessá-los, se apresentam como um importante passo para o pleno exercício da correção.

A rigor, a atribuição ao titular da possibilidade de requerer a correção de seus dados

---

raciocínios probabilísticos. Os dados inferidos, por seu turno, seriam o produto de uma análise probabilística, como resultado de correlações utilizadas para criar previsões de comportamentos (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Working Party on Security and Privacy in the Digital Economy*. 2014. Disponível em: <[https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg\(2014\)3&doclanguage=en](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en)>. Acesso em: 01 dez. 2020, p. 5).

<sup>19</sup> FORTALECENDO o debate sobre portabilidade de dados no Brasil | Simpósio ITS. [S. l.]: Instituto de Tecnologia e Sociedade, 2020. (175 min.), son., color. Disponível em: <<https://www.youtube.com/watch?v=iNvr9ZStqEM>>. Acesso em: 15 nov. 2020.



pode ser lida como uma das expressões da autodeterminação informativa que se faz presente durante todo o ciclo do fluxo informacional. Nesse sentido, a complementação, a correção e a atualização dos dados pessoais se apresentam como importantes mecanismos para garantir que a pessoa seja representada de forma fidedigna, de modo a impedir que ela sofra os reflexos de um tratamento de dados, como no campo das decisões automatizadas, em desacordo com sua real situação. Ao mesmo tempo, pode figurar como um direito da pessoa natural de manter sua história atualizada, correta e completa.

Além disso, a título de exemplo, um mero endereço desatualizado poderia resultar em uma correspondência importante não recebida, na indevida atribuição de dívida a uma pessoa, no não recebimento de determinados valores devidos,<sup>20</sup> entre outros.

A prerrogativa da correção pode ser lida como uma expressão do princípio da qualidade dos dados, previsto no art. 6º, inciso V, da LGPD,<sup>21</sup> que determina que os dados coletados devem ser precisos, completos e atualizados, na medida em que é necessário garantir ao titular a exatidão, a clareza, a relevância e a atualização de seus dados coletados, em atenção à necessidade e à finalidade daquele determinado tratamento.

Com efeito, destaque-se que pode ser relevante que o responsável pelo tratamento dos dados guarde um registro do histórico das modificações e das atualizações realizadas pelo titular, de forma a garantir um maior acesso à informação. Além disso, diante do pedido de correção dos dados, o agente de tratamento ao qual o titular se reportou deve informar aos demais agentes com os quais tenha compartilhado aqueles dados sobre o ato de correção.

A vantagem em manter o registro está na garantia da veracidade do resultado gerado a partir do processamento daquelas informações, inclusive no que diz respeito a tratamentos de dados pretéritos. Do mesmo modo, caso o titular de dados queira excluir aquela informação, é facultado a ele solicitar sua eliminação, e não apenas a correção. Como desvantagem, é possível observar que as empresas deverão manter um banco de dados cada vez maior para garantir a preservação de toda linha histórica de informações, além de que é possível apontar certo conflito com o princípio da necessidade.<sup>22</sup>

Questiona-se, por fim, se um pedido de correção, por parte do titular, acarretaria,

---

<sup>20</sup> Cf. SILVA, Priscilla Regina. Os direitos dos titulares de dados. In: MULHOLLAND, Caitlin (Org.) *LGPD e o Novo Marco Normativo no Brasil*. Porto Alegre: Arquipélago, 2020, p. 200.

<sup>21</sup> “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”.

<sup>22</sup> Tal como previsto no art. 6º, inciso III, da LGPD, o princípio da necessidade estabelece a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”.

na realidade, uma retirada do consentimento em relação ao tratamento dos dados anteriores. Todavia, a retirada do consentimento apresenta-se como uma prerrogativa autônoma do titular elencada no rol do art. 18 da LGPD, como a seguir será endereçado.

O GDPR, por seu turno, estabelece previsão análoga, como a de retificação dos dados pessoais incorretos e incompletos, levando em consideração a finalidade do tratamento.<sup>23</sup>

### **3. A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD**

A LGPD garante aos titulares dos dados a possibilidade de bloquear, ou mesmo eliminar os dados pessoais que foram colhidos em desconformidade com suas disposições, ou mesmo aquelas informações desnecessárias ou excessivas. Além disso, ao titular dos dados ainda é garantida a possibilidade de requerer que suas informações pessoais sejam anonimizadas<sup>24</sup> diante desse contexto de desconformidade, de forma que tais dados não possam mais ser associados à sua pessoa.

A rigor, o dado anonimizado, não se enquadrando como dado pessoal – porque não relacionado a uma pessoa identificada ou identificável, de maneira permanente –, estaria, a princípio, afastado do escopo da norma, salvo em situações como a prevista no parágrafo 2º, art. 12. O marco regulatório define dados anonimizados como “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. A própria nomenclatura “anonimizado” já indica que a informação era um dado pessoal que “passou por um procedimento para que os vínculos com o seu titular fossem apagados, tornando o mesmo anonimizado”.<sup>25</sup> Com efeito:

Não se pode apenas reduzir a noção de dado anônimo ou anonimizado a dado não associado ao nome de alguém. Ainda que não haja a certa identificação do titular das informações pelo nome, a distinção (*singling out*) mediante outros identificadores

---

<sup>23</sup> Conforme teor do artigo 16, do GDPR: “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”.

<sup>24</sup> “Muito embora a anonimização esteja capitulada na lei brasileira como um direito do titular, deve ser levado em consideração que o exercício de tal direito não se dá de forma irrestrita, haja vista que a própria lei, nas hipóteses em que menciona a conveniência do processo de anonimização, faz a ressalva do sempre que possível, tal como se extrai dos artigos 7º, inciso IV, 11, inciso II, c, 13, caput e 16, inciso II.” (MALDONADO, Viviane Nóbrega. *Dos direitos do titular*, cit., p. 225).

<sup>25</sup> SOUZA, Carlos Affonso. *Eles sabem quem é você?* Entenda o monitoramento de celulares na quarentena. Disponível em: <<https://tecfront.blogosfera.uol.com.br/2020/04/17/eles-sabem-quem-e-voce-entenda-o-monitoramento-de-celulares-na-quarentena/>>. Acesso em: 14 fev. 2021.

é possível, inclusive para a formação de perfil de comportamento do indivíduo. Para ser anônimo, o dado não pode ter associação com pessoa identificada ou identificável de forma permanente e irreversível, raciocínio este apenas derivado do conceito amplo de dado pessoal. Se assim caracterizado, o estatuto de proteção dos dados pessoais não se aplica, ou, eventualmente, aplica-se de maneira particularizada à atividade de tratamento das informações em questão.<sup>26</sup>

Deve ser implementada uma espécie de ampla ocultação da identidade do titular, não bastando a retirada do nome, a fim de que aquelas informações possam ser utilizadas de uma forma com que não seja possível identificar quem é a pessoa natural por trás delas. A exemplo da utilização da informação não-individualizada, mas em caráter estatístico, confira-se:

Para proteger a privacidade dos indivíduos, as bases de dados anonimizadas podem se valer de vários expedientes, como ocultar algumas informações, generalizar outras e assim por diante. Então ao invés de saber quem exatamente visitou o meu estabelecimento eu sei que essa pessoa é homem ou mulher e que tem uma idade entre 40-50 anos, só para continuar com o exemplo. Somando todas as entradas na base de dados eu consigo gerar uma visualização de quantos % do meu público é de cada faixa etária, gênero e assim por diante.<sup>27</sup>

No entanto, Carlos Affonso Souza adverte para o fato de que “quanto mais informações eu jogo nessa base, mais fácil fica reidentificar a pessoa cujo dado foi anonimizado”. Assim, uma forma de, efetivamente, anonimizar o dado é não restringir a ação apenas a esconder o nome, o endereço e o número de telefone do titular. Além disso, deve-se considerar que “o estado de anonimização é sempre temporal, já que a tecnologia avança e algo que hoje exige muito esforço para ser quebrado amanhã pode ser simplificado”.<sup>28</sup>

O titular pode, portanto, requerer a anonimização<sup>29</sup> daquele dado que passará por um processo de tratamento de forma a perder a associação entre informação e titular, eliminando a possibilidade de identificá-lo. Todavia, o pedido de anonimização feito pelo titular não garante a total quebra do vínculo entre informação e pessoa natural<sup>30</sup> caso uma ferramenta mais sofisticada possa reverter o processo de anonimização, quando, então, a natureza de dados

---

<sup>26</sup> MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. vol. 998. Caderno Especial. p. 99-128. São Paulo: Ed. RT, dezembro 2018, p. 108-109.

<sup>27</sup> SOUZA, Carlos Affonso. *Eles sabem quem é você?*, cit., n. p.

<sup>28</sup> SOUZA, Carlos Affonso. *Eles sabem quem é você?*, cit., n. p.

<sup>29</sup> Em alguns Estados-Membros da União Europeia, a anonimização corresponde ao anonimato computacional, em que se torna muito difícil identificar os titulares dos dados usando os meios de informática disponíveis. Para outros Estados, a anonimização somente ocorre a partir do anonimato perfeito, no qual não seria possível identificar o titular, até mesmo para o controlador (SILVA, Priscilla Regina. *Os direitos dos titulares de dados*, cit., p. 203).

<sup>30</sup> “A grande questão diz respeito a saber o grau de segurança e a confiança na irreversibilidade da anonimização, sem o que a técnica perde por completo a sua finalidade de proteção. Assim, observa-se que a questão do direito à anonimização depende da avaliação das alternativas técnicas e da implementação de padrões aceitáveis de segurança, sem o que o direito respectivo não tem como ser eficaz.” (FRAZÃO, Ana. *Direitos básicos dos titulares de dados pessoais*, cit., p. 39).

anonimizados estará em jogo.<sup>31</sup> A reversibilidade do processo de anonimização deve levar em conta, de acordo com a LGPD, “fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios”, segundo o parágrafo 1º, do art. 12.

Em outro plano, o bloqueio dos dados, prerrogativa também atribuída ao titular, consiste na “suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados”, conforme consta no art. 5º, inciso XIII, da LGPD, e, para o exercício desse direito, o titular deverá requerê-lo expressamente.<sup>32</sup>

A eliminação dos dados desnecessários, excessivos, ou tratados em desconformidade com a LGPD merece destaque e deve ser assegurada, em atenção à significativa facilidade de coleta na contemporaneidade, que se pode fazer presente de maneiras muito opacas, como através da simples utilização de nosso celular ou da navegação *online*.<sup>33</sup>

#### **4. A portabilidade de dados pessoais**

A portabilidade, para além de sua previsão na LGPD, já era normatizada em outras esferas do ordenamento jurídico brasileiro, com seus contornos próprios, como no mercado financeiro, na telefonia e como um remédio concorrencial.<sup>34</sup> A rigor, a portabilidade de dados pessoais prevista na regulação de proteção de dados brasileira apresenta uma clara influência do modelo da União Europeia, embora a LGPD a tenha normatizado de forma bem mais simplificada, a abrir campo para diversas discussões e para regulamentação, sobretudo pela ANPD.

---

<sup>31</sup> Nesse sentido, vários estudos recentes têm demonstrado como é fácil, mesmo a partir de dados públicos, identificar pessoas a partir de alguns atributos. Hoje já se fala nos “quase-identificadores” – *quasi-identifiers* –, que seriam variáveis que, embora não identifiquem pessoas diretamente, têm alta correlação com identificadores únicos e ainda podem ser usadas para identificações indiretas (FRAZÃO, Ana. *Nova LGPD: direito de anonimização, bloqueio ou eliminação de dados*. Jota. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-de-anonimizacao-bloqueio-ou-eliminacao-de-dados-31102018>>. Acesso em: 01 out. 2020).

<sup>32</sup> Para além de se configurarem como direito do titular, o bloqueio ou a eliminação de dados são também possíveis sanções passíveis de aplicação pela ANPD, conforme o art. 52, incisos V e VI, da LGPD.

<sup>33</sup> “Assim como ocorre com o direito à anonimização, a efetividade do direito ao bloqueio e também do direito à eliminação dos dados depende da utilização de técnicas que possibilitem que o resultado seja assegurado e não seja revertido. Por essa razão, também em relação a tais direitos, é fundamental a discussão sobre idoneidade das alternativas, metodologias e medidas de segurança.” (FRAZÃO, Ana. *Direitos básicos dos titulares de dados pessoais*, cit., p. 40).

<sup>34</sup> CRAVO, Daniela Copetti. O direito à portabilidade na Lei de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 347-365, p. 347-348.

No contexto do GDPR, a portabilidade pode ser lida como um objetivo operacional com o propósito maior de fomentar o controle dos dados pessoais pelo titular e a confiança no ambiente digital. Laura Somaini enfatiza que o escopo do instituto seria o de promover um reequilíbrio entre os agentes de tratamento e os titulares de dados, relação não raro comprometida pela assimetria informativa e de poder.<sup>35</sup> Assim, embora a portabilidade de dados possa ter implicações em outras esferas do direito, como no âmbito concorrencial, a finalidade central do instituto é apontada como sendo a de fortalecer a autodeterminação informativa. Com efeito, evidencia-se o objetivo de mitigar o aprisionamento tecnológico do titular dos dados a um determinado agente de tratamento, apesar da existência de outros que ofereçam uma prestação mais vantajosa e/ou satisfatória (*lock-in*).

Como um avanço diante do direito de acesso,<sup>36</sup> em comparação com a precedente Diretiva 95/46/CE, o GDPR normatizou no seu art. 20<sup>37</sup> a portabilidade como a prerrogativa de o titular “receber os dados pessoais que tenham fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e transmitir esses dados a outro responsável pelo tratamento sem impedimentos”.<sup>38</sup> Por sua vez, a LGPD consagrou, no art. 18, inciso V, o direito de o titular obter do controlador, a qualquer momento e mediante requisição, a “portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os

---

<sup>35</sup> SOMAINI, Laura. The right to data portability and user control: ambitions and limitations. *Rivista di Diritto Dei Media*, Milano, v. 2018, n. 3, p.1-27, out. 2018. Disponível em: <<http://www.medialaws.eu/rivista/the-right-to-data-portability-and-user-control-ambitions-and-limitations/>>. Acesso em: 02 fev. 2020, p. 9-11.

<sup>36</sup> “Se dunque il diritto all'accesso ha una dimensione essenzialmente statica, rispondendo all'esigenza di garantire all'interessato la sola conoscenza dei dati su cui si sta esplicando il trattamento, il diritto alla portabilità si preoccupa di regolare la dimensione dinamica del controllo dell'interessato sui dati oggetto del trattamento, proiettando la protezione nella sfera della disponibilità dei dati da parte dello stesso interessato. In altre parole, il diritto alla portabilità rende, o perlomeno dovrebbe rendere, il suo titolare pieno ed effettivo dominus dei dati che lo riguardano, dandogli la possibilità non solo di riappropriarsene ma anche di farne l'utilizzo che meglio ritiene, anche mediante trasferimento a terzi.” (TROIANO, Stefano. Il diritto alla portabilità dei dati personali. In: GALGANO, Nadia Zorzi (Org.). *Persona e mercato dei dati. Riflessioni sul GDPR*. Milano: Cedam, 2019. cap. 7. p. 195-218. E-book. n. p.).

<sup>37</sup> “Artigo 20º Direito de portabilidade dos dados. 1. “O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) O tratamento se basear no consentimento dado nos termos do artigo 6º, n.º 1, alínea a), ou do artigo 9º, n.º 2, alínea a), ou num contrato referido no artigo 6º, n.º 1, alínea b); e b) O tratamento for realizado por meios automatizados. (...)”.

<sup>38</sup> GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Orientações sobre o direito à portabilidade dos dados*. [s.l.], 2017. Disponível em: <[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611233](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233)>. Acesso em: 17 mar. 2020, p. 3-4.

segredos comercial e industrial”.<sup>39-40</sup>

A portabilidade também poderá ser exercida, segundo a redação do parágrafo 3º, do art. 18, da LGPD, por um representante legal, além do titular, diante do agente de tratamento, sem quaisquer custos (parágrafo 5º), como, de regra, aplica-se aos demais direitos do titular.

Em específico, a utilização pelo legislador da expressão “fornecedor de serviço ou produto” para normatizar a portabilidade na LGPD tem gerado controvérsias sobre esse direito estar ou não restrito ao âmbito consumerista. Todavia, em uma leitura sistematizada da norma, parece mais razoável compreender essa redação como fruto de um equívoco por parte do legislador em razão da originária associação do instituto da portabilidade à esfera do consumo, o que não se consolidou, seja no Brasil, seja na União Europeia. Nessa direção, Daniela Copetti Cravo sustenta uma leitura ampliada da expressão, de forma a não restringir a portabilidade de dados às relações de consumo, visto que o *caput* do art. 18 se refere expressamente à figura do “controlador”, e não à de um “fornecedor de serviço ou produto”.<sup>41</sup>

Uma questão que deve ser endereçada diz respeito à normatização aberta e simplificada da portabilidade na LGPD. Ao traçarmos um paralelo com o GDPR, é possível identificar que a regulação europeia limitou a portabilidade dos dados fornecidos pela pessoa quando o tratamento tiver por base legal o contrato ou o consentimento, além de restringir sua incidência apenas àquelas situações nas quais o tratamento dos dados se der de forma automatizada.<sup>42</sup> Adicionalmente, a proteção de interesses de terceiros<sup>43</sup> é expressamente

---

<sup>39</sup> A atual redação do direito à portabilidade na LGPD resulta de alteração promovida pela Lei 13.853, de 2019, uma vez que a redação original dispunha o direito de “portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador”. Na leitura de Viviane Nóbrega Maldonado, a alteração foi importante para sugerir que a ANPD deveria regulamentar a portabilidade e a sua requisição, e não questões relacionadas ao segredo de empresa (MALDONADO, Viviane Nóbrega. *Dos direitos do titular*, cit., p. 231).

<sup>40</sup> O §7º, do art. 18, da LGPD, estabelece que a portabilidade não abrangerá os dados anônimos. Como dados que se referem a pessoas identificáveis, os dados pseudonimizados estão na abrangência da portabilidade, o que se depreende do próprio art. 11, do GDPR, apesar de a LGPD não disciplinar expressamente a questão. A propósito: “O processo de anonimização é frequentemente confundido com a pseudoanonimização. Enquanto o primeiro busca eliminar a possibilidade de identificação sem que se pretenda a reversão do procedimento, a pseudoanonimização torna indisponíveis os dados que permitiriam a identificação por meio de técnicas como a encriptação. A pseudoanonimização protege os dados da publicização, e sobre tais dados incide a aplicação da LGPD” (SILVA, Priscilla Regina. *Os direitos dos titulares de dados*, cit., p. 201).

<sup>41</sup> FORTALECENDO o debate sobre portabilidade de dados no Brasil | Simpósio ITS, cit., n. p.

<sup>42</sup> O Considerando 73 do GDPR indica a possibilidade de restrições adicionais a direitos dos titulares.

<sup>43</sup> Apesar de não mencionada expressamente como um limite à portabilidade na LGPD, a proteção de interesses de terceiros pode condicionar o seu exercício, o que poderá demandar uma análise casuística, em atenção à razoabilidade, para equilibrar a proteção do titular e de outros envolvidos. Segundo Hert *et al.*, seria demandado um *case-by-case approach* para a delimitação da portabilidade (HERT, Paul de; PPAKONSTANTINO, Vagelis; MALGIERI, Gianclaudio; BESLAY, Laurent; SANCHEZ, Ignacio. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, [s. l.], v. 34, n. 2, p.193-203, abr. 2018. Elsevier BV, p. 198).

assinalada no GDPR, ao passo que a LGPD apenas se refere aos segredos comercial e industrial. Cravo pondera que, a princípio, o alcance da portabilidade de dados estaria contido na mesma abrangência da LGPD, considerados os limites dos artigos 3º e 4º da norma, o que poderia tornar esse direito muito oneroso e pouco factível.<sup>44</sup>

Ainda que o GDPR apresente uma regulação mais densificada sobre quais dados pessoais são portáveis, a utilização da expressão “dados fornecidos” tem gerado divergências sobre sua abrangência no modelo europeu. Segundo uma interpretação restrita, apenas seriam compreendidos nesse conceito os dados fornecidos explicitamente pelo titular, como através do preenchimento de formulários. Por uma leitura ampla da expressão, o Grupo do Artigo 29 sustenta:

Os dados "fornecidos" pelo titular devem igualmente incluir os dados pessoais que sejam observados a partir das atividades dos utilizadores, tais como os dados brutos tratados por um contador inteligente ou por outros tipos de objetos conectados, os registos das atividades e os históricos da utilização de um sítio Web ou das pesquisas realizadas.<sup>45</sup>

Tal debate ainda está em aberto na regulação brasileira, que sequer limita expressamente os dados portáveis aos “dados fornecidos”. Embora a ressalva feita pela LGPD no sentido de se tutelar o segredo de empresa seja uma diretriz, tal previsão também não pode ser vista de forma ampla e independentemente da existência de uma fundamentação correlata, sob pena de esvaziamento da portabilidade sob o argumento de proteger o segredo. Com efeito, reitere-se a menção à relação entre a tutela do segredo de empresa e a concorrência desleal, com a configuração de efetivo prejuízo concorrencial.

Enquanto condição técnica para viabilizar a portabilidade de dados, a LGPD atribui à ANPD a possibilidade de “dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros”, em atenção à necessidade e à transparência, segundo o art. 40. Considerando que uma regulamentação precisa da portabilidade ainda esteja em aberto no Brasil, verifica-se que, a princípio, o controlador poderia não atender à requisição da portabilidade com base em barreiras técnicas, segundo o parágrafo 4º, do art. 18, da LGPD. Assim, como alerta Cravo, as razões de fato e de direito que impedem o atendimento ao requerimento devem ser indicadas de forma clara e inteligível, sob pena de esvaziamento desse direito.<sup>46</sup> Acrescente-se, no imperativo da boa-fé objetiva, que compete ao controlador o ônus de demonstrar que, dentro

---

<sup>44</sup> CRAVO, Daniela Copetti. *O direito à portabilidade na Lei de Proteção de Dados*, cit., p. 359-360.

<sup>45</sup> GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Orientações sobre o direito à portabilidade dos dados*, cit., p. 11.

<sup>46</sup> CRAVO, Daniela Copetti. *O direito à portabilidade na Lei de Proteção de Dados*, cit., p. 361.

do possível, adotou as medidas adequadas e necessárias para viabilizar a concretização do direito à portabilidade.

Outro debate também subjacente à portabilidade é o que se refere à tensão do seu exercício frente ao princípio da segurança, o que se torna mais visível diante da promoção do fluxo de dados e da própria interoperabilidade.<sup>47</sup> A segurança e o sigilo de dados pessoais representam dois elementos incontornáveis para que, de fato, se possa falar em proteção de dados.<sup>48</sup> Em atenção ao fato de que a portabilidade é uma das *Privacy Enhancing Technologies* (PET),<sup>49</sup> emerge a necessidade de se equilibrar controle por parte dos titulares e a segurança.<sup>50</sup>

Outra questão é o potencial conflito entre a portabilidade de dados e o princípio da minimização (GDPR) ou da necessidade (LGPD), na medida em que, como aponta Stefano Troiano, se identifica uma contraposição entre essa principiologia e a ampliação/estímulo à transferência de dados proposta pela portabilidade, enquanto direito verdadeiramente dinâmico.<sup>51</sup>

Em outro aspecto, o inciso III, do art. 16, autoriza o agente de tratamento a conservar os dados pessoais para fins de transferência a terceiros, desde que observados os requisitos legais. A rigor, “o princípio da finalidade ganha, neste âmbito, maior importância, justamente para evitar um desvio na finalidade desta conservação”, considerando que a manutenção dos dados deverá ocorrer estritamente para eventual transferência a terceiros, o que pode estar no âmbito da portabilidade.<sup>52</sup>

Por fim, deve ser oportunizado ao titular exercer o direito à portabilidade de maneira concomitante ao direito à eliminação dos dados, uma vez que o apagamento não pode ser vislumbrado como uma consequência automática da portabilidade, justamente porque os dados podem prestar-se a finalidades diversas e complementares no caso concreto.

---

<sup>47</sup> SOMAINI, Laura. *The right to data portability and user control*, cit., p. 14.

<sup>48</sup> SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 417-441, p. 418.

<sup>49</sup> HERT, Paul de; PAPAKONSTANTINOU, Vagelis; MALGIERI, Gianclaudio; BESLAY, Laurent; SANCHEZ, Ignacio. *The right to data portability in the GDPR*, cit., p. 194.

<sup>50</sup> NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; FERNANDES, Elora Raad. Portabilidade e proteção de dados pessoais: tensões entre pessoa e mercado. *Civilistica.com*. Rio de Janeiro, ano 10, n. 1, 2021. Disponível em: <<http://civilistica.com/portabilidade-e-protecao-de-dados-pessoais/>>. Acesso em: 03 maio 2021.

<sup>51</sup> TROIANO, Stefano. *Il diritto alla portabilità dei dati personali*, cit., n. p.

<sup>52</sup> NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; FERNANDES, Elora Raad. *Portabilidade e proteção de dados pessoais*, cit., p. 21.



## 5. A eliminação de dados pessoais

Além da possibilidade de eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (inciso IV), o inciso VI, do art. 18, versa sobre o direito do titular à eliminação dos dados pessoais que tiverem sido tratados *com a base legal do consentimento*, ou seja, dados que, a princípio, foram tratados licitamente, mas que deveriam ser eliminados com o término do tratamento, com exceção das hipóteses previstas no art. 16 – leia-se, que autorizariam a manutenção dos dados pelo controlador.

Ana Frazão, todavia, pondera que o problema residiria no fato de que o art. 16 estabelece hipóteses demasiado amplas para a manutenção dos dados pessoais pelo controlador, ainda que após o término do tratamento. Um exemplo citado pela autora seria o inciso IV, do art. 16, que autoriza a manutenção dos dados para “uso exclusivo do controlador, vedado seu acesso por terceiro, desde que anonimizados os dados”.<sup>53</sup>

O conceito de eliminação, para a LGPD, consiste na “exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado”. Apesar de não constar na definição do art. 5º, da LGPD, o processo de eliminação dos dados é irreversível.

É possível pensar que, conforme o art. 7º, da LGPD, o consentimento do titular é a primeira base legal autorizadora do tratamento dos dados e, “por evidente, quem fornece o consentimento pode igualmente retirá-lo quando assim lhe aprouver (...), o titular pode postular a eliminação de dados se já não mais existe o consentimento”.<sup>54</sup>

Diferentemente do que ocorre com a correção, o direito à eliminação é irreversível, pois não há mais o consentimento para que seja mantida uma linha histórica de informações pessoais prévias. Sem o consentimento, não há que se falar em manutenção de registros dos dados pessoais que o titular decidiu por solicitar, expressamente, a respectiva eliminação, salvo a existência de obrigação legal nesse sentido.

## 6. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados

---

<sup>53</sup> FRAZÃO, Ana. *Direitos básicos dos titulares de dados pessoais*, cit., p. 44.

<sup>54</sup> MALDONADO, Viviane Nóbrega. *Dos direitos do titular*, cit., p. 232.

O controlador, que efetuou a coleta e o tratamento dos dados pessoais, pode compartilhar essas informações pessoais coletadas com entidades públicas e privadas, desde que esse fato detenha um fundamento normativo e que seja expressamente informado ao titular dos dados. Além da prerrogativa de o titular ser informado sobre o compartilhamento, o responsável pelo tratamento de dados deverá sempre comunicar às entidades com as quais teve qualquer tipo de compartilhamento sobre a eliminação ou a correção dos dados para que, assim, essas entidades possam manter as informações dos titulares atualizadas.

É oportuno, no entanto, fazer uma diferenciação entre uso compartilhado e portabilidade, na medida em que, na portabilidade, o próprio titular solicita a transmissão de seus dados pessoais a outro controlador, enquanto, no uso compartilhado, o controlador faz essa transmissão, independentemente de requerimento do titular.

A propósito, o direito de acesso aos dados pelos titulares também deveria ser compreendido no âmbito das entidades que receberam esses dados por meio de compartilhamento pelo controlador. Com efeito, deve ser garantido ao titular que, mediante requerimento, tenha acesso às suas informações que foram repassadas, para que, se for o caso, possa exercer as demais prerrogativas, como a eliminação ou correção dessas informações, quando impertinentes.

No entanto, a LGPD não dispõe expressamente sobre a obrigatoriedade de informar os dados dessas entidades públicas e privadas com as quais os dados foram compartilhados ao titular, o que pode vir a dificultar o exercício de sua autodeterminação informativa. Na ausência de disposição expressa em lei, o imperativo do princípio da transparência ganha uma importante dimensão no sentido de viabilizar o exercício do controle pelo titular, dando-lhe conhecimento sobre a cadeia dos agentes de tratamento.

## **7. Informação sobre a possibilidade de não fornecer o consentimento, as consequências da negativa e a revogação do consentimento**

A previsão do consentimento do titular como uma das hipóteses legais para o tratamento dos dados demonstra a preocupação da lei de colocar a pessoa natural como protagonista, uma vez que, tornando necessário seu consentimento quando não existir base legal diversa, permite maior controle de sua parte. A rigor, o consentimento é previsto na LGPD como uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o

tratamento de seus dados pessoais para uma finalidade determinada”.<sup>55</sup>

Como consequência lógica da qualificação do consentimento como *livre*, certo é que o titular dos dados não é obrigado a compartilhar suas informações pessoais diante da ausência de obrigatoriedade legal e, nessa linha, é também seu direito ter conhecimento sobre a possibilidade de não fornecer o consentimento para o tratamento de seus dados. Retome-se, aqui, a associação entre a pessoa humana e os dados que lhe dizem respeito, sobretudo em termos de autonomia.

Entretanto, para além de o titular ter conhecimento sobre a possibilidade da negativa ao fornecimento do consentimento para o tratamento de seus dados, também é prevista a prerrogativa de compreender as consequências dessa negativa. Nessa direção, é razoável que essas informações sobre as consequências de eventual recusa do consentimento sejam ofertadas anteriormente, conferindo-se ao titular a possibilidade de realizar um juízo sobre a conveniência do ato.

A título de exemplo, a empresa pode negar-se a prestar determinado serviço ao titular, caso este decida não permitir o tratamento de seus dados pessoais que seriam necessários para a prestação daquele serviço. Repita-se, os dados devem ser os estritamente necessários, não existindo margem para abusividades, a teor da principiologia exarada na norma. Nesse caso, caberá ao titular decidir se abrirá mão desse serviço em específico ou se permitirá a coleta e o tratamento de seus dados.<sup>56</sup> A adoção do consentimento granular<sup>57</sup> pode ser uma opção nesse cenário, facultando ao titular gradações na sua decisão, e, de acordo com as atividades de tratamento consentidas, diferentes vantagens e ônus deverão ser claramente apresentados.

Além da possibilidade de não fornecer o consentimento, a lei também garante ao titular dos dados a possibilidade de revogar o consentimento, nos termos do art. 8º, parágrafo 5º, da LGPD. Conforme prevê a lei, o consentimento, no passado fornecido, poderá ser

---

<sup>55</sup> Em se tratando do consentimento para o tratamento de dados sensíveis, demanda-se uma maior qualificação. Sobre o tema, cf. KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Dados sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade*. 2019. 118 f. Dissertação (Mestrado) - Curso de Direito e Inovação, Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <http://repositorio.ufjf.br:8080/jspui/bitstream/ufjf/11438/1/mariareginadetonicavalcantirigolonkorkmaz.pdf>. Acesso em: 31 maio 2020.

<sup>56</sup> A propósito: “No sentido de fortalecer o indivíduo, a lei estabelece que, se o tratamento dos dados pessoais for condição para o fornecimento de produto ou serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos enumerados no art. 18 da Lei. Regulamenta-se, assim, a lógica binária das chamadas políticas de tudo ou nada (*take it or leave it choice*), em que o usuário ou aceita todas as disposições e termos do serviço ou não pode utilizá-lo.” (TEPEDINO, Gustavo, TEFFÉ, Chiara S. de. Consentimento e Proteção de Dados Pessoais na LGPD. In: *Revista Brasileira de Direito Civil – RBDCivil*, v. 25, p. 83-116, jul./set. 2020, p. 95).

<sup>57</sup> Cf. BIONI, Bruno. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

revogado pelo titular dos dados a qualquer momento, de forma expressa, gratuita e facilitada.

A revogação do consentimento, portanto, será válida a partir de sua expressa manifestação e, quanto aos dados coletados e tratados enquanto o consentimento era plenamente válido, ratificam-se os tratamentos anteriormente realizados.

Por outro lado, é necessário frisar que a revogação do consentimento poderá não resultar na cessação do tratamento dos dados, porque o consentimento é apenas um dos fundamentos legais para que o tratamento possa ser realizado. Desse modo, o titular deverá verificar se não há qualquer outra base legal para o tratamento de seus dados pessoais e, caso positivo, a revogação do consentimento não terá o condão de interromper o tratamento.

## 8. Prerrogativas diante das decisões automatizadas

No paradigma da sociedade da informação, os processos decisórios, antes atribuídos a seres humanos, são cada vez mais definidos por sistemas automatizados sob o argumento de maior racionalização e eficiência. De fato, a capacidade humana de processar uma miríade de dados não se compara à de sistemas como os de Inteligência Artificial (IA). Todavia, são gerados múltiplos desafios que transcendem a esfera jurídica, mas que dela demandam resposta.

Mittlestadt *et al.* apresentam alguns dos eixos de desafios éticos – sejam eles epistêmicos ou normativos – sobre a utilização de algoritmos<sup>58</sup> enquanto possíveis mecanismos para a tomada de decisões automatizadas.<sup>59</sup> Primeiro, esses algoritmos podem gerar evidências inconclusivas,<sup>60</sup> as quais, não raro, também são inescrutáveis. O fato de que o *output* de dados

---

<sup>58</sup> No presente artigo, adota-se um conceito amplo de algoritmos como construção matemática, bem como as suas implementações enquanto programas e configurações (aplicações). (TSAMADOS, Andreas; AGGARWAL, Nikita; COWLS, Josh; MORLEY, Jessica; ROBERTS, Huw; TADDEO, Mariarosaria; FLORIDI, Luciano. The ethics of algorithms: key problems and solutions. *AI & Society*, [s. l.], 20 fev. 2021. Springer Science and Business Media LLC. <<http://dx.doi.org/10.1007/s00146-021-01154-8>>.).

<sup>59</sup> Em 2021, parte do grupo de pesquisadores envolvidos nesse mapeamento de dilemas éticos sobre algoritmos publicou um artigo que ratificou o mapa anteriormente apresentado, mas com as suas atualizações próprias dos avanços na pesquisa e no campo da tecnologia. Ressalvou-se, todavia, a crescente defesa da “Artificial Intelligence (AI) for social good”, destacando-se que para esse objetivo devem igualmente ser endereçados, de maneira satisfatória, os riscos que cada uma das seis categorias indicadas no mapa apontou. (TSAMADOS, Andreas; AGGARWAL, Nikita; COWLS, Josh; MORLEY, Jessica; ROBERTS, Huw; TADDEO, Mariarosaria; FLORIDI, Luciano. *The ethics of algorithms*, n. p.).

<sup>60</sup> Registre-se o fenômeno da *apofenia*, ao qual esses sistemas estão suscetíveis, que se traduz em enxergar padrões onde não existem, mas que se justificariam pela ostensiva quantidade de dados que pode oferecer conexões em todas as direções. (BOYD, Danah; CRAWFORD, Kate. Critical Questions for Big Data. *Information, Communication & Society*, [s. l.], v. 15, n. 5, p. 662-679, jun. 2012. Informa UK Limited. <http://dx.doi.org/10.1080/1369118x.2012.678878>. Disponível em:

não pode ir além do *input* considerado pelo sistema também contribui para um desafio a que os autores se referem como “evidência mal orientada”. A possibilidade de resultados injustos é apontada, no sentido de que, embora um resultado seja estatisticamente correto, sua aplicação pode promover discriminações. Os efeitos transformativos dos algoritmos sobre a forma através da qual conceituamos o mundo são também reconhecidos – e exemplos são as práticas de *profiling*.<sup>61</sup> Por fim, os autores enfatizam a dificuldade de apuração e de responsabilização diante dos danos causados por algoritmos.<sup>62</sup>

A súmula dos desafios apontados por Mittelstadt *et al.* facilita a compreensão das possibilidades e das limitações das prerrogativas do titular dos dados em face das decisões automatizadas, decisões estas que vêm sendo utilizadas para definir o valor de prêmios do seguro de saúde, para conceder-se crédito, para determinar quem deve ter acesso a moradias subsidiadas pelo governo, como nos Estados Unidos, para apontar quem deve ser excluído de uma seleção profissional, entre outros. Com efeito, assim dispõe o art. 20 da LGPD:

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. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

De plano, identifica-se que o regime protetivo previsto na LGPD não se destina a toda e qualquer decisão automatizada, mas àquelas “destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade”. Ou seja, deve existir uma interferência sensível na realidade da pessoa, a partir de uma determinada decisão, para que o regime jurídico da LGPD seja aplicável.<sup>63</sup>

---

<<https://www.tandfonline.com/doi/abs/10.1080/1369118X.2012.678878>>. Acesso em: 09 mar. 2021).

<sup>61</sup> O *profiling* através de algoritmos tem lugar em um período indefinido de tempo, no qual os indivíduos são categorizados de acordo com uma lógica interna de cada sistema, devendo-se acrescentar ainda a fluidez nessa categorização, uma vez que os perfis são alterados na medida em que são atualizadas as informações obtidas pelo sistema. (TSAMADOS, Andreas; AGGARWAL, Nikita; COWLS, Josh; MORLEY, Jessica; ROBERTS, Huw; TADDEO, Mariarosaria; FLORIDI, Luciano. *The ethics of algorithms*, cit., n. p.).

<sup>62</sup> MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. *Big Data & Society*, [s. l.], v. 3, n. 2, p. 1-21, dez. 2016. SAGE Publications.< <http://dx.doi.org/10.1177/2053951716679679>>.

<sup>63</sup> O art. 22 (1) do GDPR dispõe que “O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar”. O Grupo de Trabalho do Artigo 29 traz

Além disso, a LGPD expressamente demanda, como requisito para o direito à revisão, disposto no *caput* do art. 20, que as decisões sejam “tomadas unicamente com base em tratamento automatizado de dados pessoais”. Nesse ponto, merecem atenção os riscos da chamada *fabricação de intervenção humana*. Isto é, para que uma decisão perca sua natureza de totalmente automatizada, a intervenção humana deve ser consistente e ter, de fato, a aptidão de alterar o resultado. Nessa direção adverte o Grupo de Trabalho do Artigo 29, diante do modelo da União Europeia.<sup>64</sup>

Uma segunda questão diz respeito às alterações legislativas que o regime jurídico das decisões automatizadas na LGPD já suportou. A mais significativa diz respeito à supressão da exigência de que a revisão da decisão automatizada seja realizada por uma pessoa natural, através da Lei 13.853 de 2019.<sup>65</sup> A partir da nova redação, poderia um algoritmo revisar a decisão de outro algoritmo, não havendo a necessidade de uma pessoa natural fazê-lo. Nada impediria, no entanto, que o agente de tratamento voluntariamente realizasse a revisão humana, como fruto de uma política interna mais benéfica ao titular.

As dificuldades decorrentes dessa alteração legislativa são claras quando se consideram os desafios éticos apresentados, sobretudo a possibilidade de a decisão se basear em evidências inconclusivas, frequente natureza inescrutável da decisão, sua possível má-orientação e aptidão de gerar efeitos injustos. Embora a possibilidade de enviesamento ou discriminação em uma decisão humana não seja descartável e em se mapeando os argumentos

---

sugestões possíveis do que poderia, no contexto do GDPR, ser compreendido dentro do escopo do que teria o condão de afetar significativamente o titular: “significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals; (...) decisions that affect someone’s financial circumstances, such as their eligibility to credit; decisions that affect someone’s access to health services; decisions that deny someone an employment opportunity or put them at a serious disadvantage; decisions that affect someone’s access to education, for example university admissions”. (ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*. 2017. Adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018, p. 21-22. Disponível em: <[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053)>. Acesso em: 08 ago. 2019.).

<sup>64</sup> ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, cit., p. 21.

<sup>65</sup> Enquanto linhas centrais do processo legislativo, em dezembro de 2018, o então Presidente da República, Michel Temer, adotou a Medida Provisória (MP) 869, que, dentre as alterações promovidas, modificou a redação do art. 20 na parte que demandava a revisão “por pessoa natural”. Com o trâmite da MP 869/2018, a revisão por pessoa natural chegou a ser reinserida no corpo da lei pela Câmara dos Deputados, ratificada pelo Senado Federal, no parágrafo 3º do art. 20, com a ressalva de que seria demandada regulamentação da ANPD, de acordo com a natureza e o porte da entidade ou o volume das operações de tratamento de dados. Retornando à Presidência da República, o parágrafo 3º do art. 20 foi vetado, entre nove vetos, suprimindo, novamente, a revisão humana, de acordo com a publicação da Lei n. 13.853 de 2019. O argumento favorável à alteração é pragmático: o vultoso número de decisões automatizadas inviabilizaria a revisão humana e afetaria modelos de negócios e análises de créditos.

no sentido de mitigar a discriminação nos algoritmos *by design*,<sup>66</sup> identifica-se um vetor, no cenário internacional, no sentido de assegurar a interferência humana nas decisões. Nesse sentido está o GDPR, que além de apresentar um regime mais rigoroso nesse cenário em favor do titular, endereça a intervenção humana como uma das prerrogativas aplicáveis quando a decisão automatizada for autorizada nas restritas hipóteses do regulamento.<sup>67</sup> Em uma interpretação sistemática da LGPD, sobretudo de sua principiologia, bem como diante dos reconhecidos limites desses sistemas no atual estado da arte da tecnologia, a garantia da supervisão humana se parece impor, o que não é suscetível de se endereçar nessa sede.

Por seu turno, o direito à explicação, alvo de tantas controvérsias no contexto da União Europeia, parece sedimentar seu fundamento do parágrafo 1º, do art. 20, da LGPD, especificamente no trecho que atribui ao controlador, quando solicitado, o dever de apresentar “informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial”. De início, verifica-se que essa previsão, com uma maior densidade normativa, se apresenta como um reflexo da principiologia estabelecida na regulação brasileira, como os princípios do livre acesso, da transparência e da não-discriminação.

Ainda, é importante destacar o papel assumido pelo regime do direito de acesso na consolidação do direito à explicação no GDPR. Na LGPD, por seu turno, o art. 9, incisos I e II, bem como o art. 18, incisos I e II – acima apresentados –, consolidam um robusto regime de acesso à informação,<sup>68</sup> dialogando e complementando o escopo do direito à explicação.

Como destacam Wachter, Mittelstadt e Floridi, “the rights to contest a decision, to obtain human intervention or to express views granted in Article 22 (3) may be meaningless if

---

<sup>66</sup> Neste sentido, cf. SUNSTEIN, Cass R. Algorithms, correcting biases. *Social Research*, [s. l], v. 86, n. 2, p. 499-511, summer 2019. Published by Johns Hopkins University Press.

<sup>67</sup> “Artigo 22.o Decisões individuais automatizadas, incluindo definição de perfis 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O n.o 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. 3. Nos casos a que se referem o n.o 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4. As decisões a que se refere o n.o 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.o, n.o 1, a não ser que o n.o 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular”. Cf. o Considerando 71 do GDPR.

<sup>68</sup> SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. In: DONEDA, Danilo *et al.* (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. cap. 12. p. 243-270, p. 263-264.

the data subject cannot understand how the contested decision was made”.<sup>69</sup> Vale dizer, o direito à explicação se apresenta como um pressuposto indispensável para proporcionar uma contestação efetiva da decisão automatizada, inclusive judicialmente.

A propósito, Carlos Affonso Souza, Christian Perrone e Eduardo Magrani enfatizam que a transparência apresenta múltiplas dimensões, as quais transcendem a esfera meramente individual do titular. Com efeito, no âmbito do direito à explicação, a excessiva oferta de informações, bem como sua apresentação de maneira obscura, pode repercutir uma verdadeira negativa de informação. Assim, como referido pelo legislador, as informações devem ser claras e adequadas, possibilitando ao titular compreender a racionalidade da decisão para, se for o caso, impugná-la. Vale dizer, a explicação deve ser efetivamente inteligível, além de orientar-se pela boa-fé, como preceitua o *caput* do art. 6º, da LGPD.

Neste cenário, um exemplo dentre vários que vêm sendo construídos de explicação – considerando a natureza dos sistemas – são as contrafactuais, compreendidas como a explicação de como o mundo deveria ser diferente para que se obtivesse outro resultado desejável naquele processamento automatizado.<sup>70</sup>

De outra parte, registre-se que a LGPD não determina em que momento o requerimento da revisão e/ou das informações apontadas no parágrafo 1º poderá ser formulado, o que, a princípio, ficará a critério do titular, mas que poderá ser objeto de regulamentação por parte da ANPD.

Enquanto uma prerrogativa não propriamente da pessoa à qual os dados se referem, o parágrafo 2º, do art. 20, determina que em caso de negativa das informações que consolidariam a explicação com base no segredo de empresa, a ANPD poderá realizar auditoria para a verificação de aspectos discriminatórios no tratamento de dados. A rigor, para além de mera faculdade, os interesses em questão parecem sugerir tratar-se de um dever da autoridade.

---

<sup>69</sup> WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, [s. l.], v. 7, n. 2, pp. 76-99, may 2017. Oxford University Press (OUP). <<http://dx.doi.org/10.1093/idpl/ix005>>. p. 97.

<sup>70</sup> Sandra Wachter, Brent Mittelstadt e Chris Russell esclarecem a explicação contrafactual representa um primeiro passo para equilibrar transparência, explicabilidade e responsabilidade com outros interesses, a exemplo de uma minimização da carga regulatória sobre os interesses comerciais, a privacidade, além de promover a aceitação pública da decisão automatizada (WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual explanations without opening the black box: automated decisions and the GDPR. *Harvard Journal Of Law & Technology*, Cambridge, v. 31, n. 2, p. 841-887, 2018. Disponível em: <<https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>>. Acesso em: 09 jul. 2020).



## 9. Conclusão

O livre desenvolvimento da personalidade, na era da informação, não prescinde de uma efetiva agenda de proteção de dados pessoais. Apesar da prévia disciplina pontual no ordenamento jurídico brasileiro, a LGPD vem apresentar uma densidade normativa sem precedentes para a proteção da pessoa com relação a seus dados, sobretudo conferindo-lhe um rol de prerrogativas para viabilizar o exercício de sua autodeterminação informativa.

A pessoa natural ganha protagonismo no cenário em que suas informações estão, progressiva e constantemente, sendo coletadas e utilizadas por agentes públicos e privados, movidos pelos mais diversos propósitos. Emerge, com efeito, o imperativo de assegurar o controle sobre as informações, coordenando as perspectivas individual e coletiva, tendo aquela significativa expressão nos direitos dos titulares estabelecidos na regulação nacional.

Embora tenha sido possível identificar determinados limites legais e interpretativos nos chamados “Direitos do titular” na LGPD, suas potencialidades em conferir à pessoa humana um instrumental para sua autodeterminação nesse campo são múltiplas. Em última análise, a noção de corpo eletrônico da pessoa construída por Stefano Rodotà apresenta a precisa dimensão da tutela dos dados pessoais, seu fundamento e sua extensão como balizas para efetivamente assegurar a autonomia da pessoa humana na era digital.

## Referências

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*. 2017. Adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018. Disponível em: <[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053)>. Acesso em: 08 ago. 2019.

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

BOYD, Danah; CRAWFORD, Kate. Critical Questions for Big Data. *Information, Communication & Society*, [s. l.], v. 15, n. 5, p. 662-679, jun. 2012. Informa UK Limited. <http://dx.doi.org/10.1080/1369118x.2012.678878>. Disponível em: <<https://www.tandfonline.com/doi/abs/10.1080/1369118X.2012.678878>>. Acesso em: 09 mar. 2021.

CRAVO, Daniela Copetti. O direito à portabilidade na Lei de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters

Brasil, 2019, p. 347-365.

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

FORTALECENDO o debate sobre portabilidade de dados no Brasil | Simpósio ITS. [S. l.]: Instituto de Tecnologia e Sociedade, 2020. (175 min.), son., color. Disponível em: <<https://www.youtube.com/watch?v=iNvr9ZStqEM>>. Acesso em: 15 nov. 2020.

FRAZÃO, Ana. Direitos básicos dos titulares de dados pessoais. In: Lei Geral de Proteção de Dados Pessoais. *Revista do Advogado*, v. 144, nov. 2019.

FRAZÃO, Ana. *Nova LGPD: direito de anonimização, bloqueio ou eliminação de dados*. Jota. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-de-anonimizacao-bloqueio-ou-eliminacao-de-dados-31102018>>. Acesso em: 01 out. 2020.

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Orientações sobre o direito à portabilidade dos dados*. [S. l.], 2017. Disponível em: <[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611233](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233)>. Acesso em: 17 mar. 2020.

HERT, Paul de; PAPAKONSTANTINOU, Vagelis; MALGIERI, Gianclaudio; BESLAY, Laurent; SANCHEZ, Ignacio. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, [s. l.], v. 34, n. 2, p.193-203, abr. 2018. Elsevier BV.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Dados sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade*. 2019. 118 f. Dissertação (Mestrado) - Curso de Direito e Inovação, Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <<http://repositorio.ufjf.br:8080/jspui/bitstream/ufjf/11438/1/mariareginadetonicavalcantirigolonkorkmaz.pdf>>. Acesso em: 31 maio 2020.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. vol. 998. Caderno Especial, p. 99-128. São Paulo: Ed. RT, dezembro 2018.

MALDONADO, Viviane Nóbrega. Dos direitos do titular. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). *LGPD: lei geral de proteção de dados comentada*. 2. ed. rev. ampl. atual. São Paulo: Thomson Reuters Brasil, 2019. cap. 3, p. 215-245.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. *Big Data & Society*, [s. l.], v. 3, n. 2, p. 1-21, dez. 2016. SAGE Publications. <<http://dx.doi.org/10.1177/2053951716679679>>.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Autonomia privada, portabilidade de dados pessoais e planejamento sucessório. In: TEIXEIRA, Daniele Chaves (Coord.). *Arquitetura do Planejamento Sucessório*. Belo

Horizonte: Fórum, 2021, p. 659-674. Tomo II.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; FERNANDES, Elora Raad. Portabilidade e proteção de dados pessoais: tensões entre pessoa e mercado. *Civilistica.com*. Rio de Janeiro, ano 10, n. 1, 2021. Disponível em: <<http://civilistica.com/portabilidade-e-protecao-de-dados-pessoais/>>. Acesso em: 03 maio 2021.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Working Party on Security and Privacy in the Digital Economy*. 2014. Disponível em: <[https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg\(2014\)3&doclanguage=en](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en)>. Acesso em: 01 dez. 2020.

PASQUALE, Frank. *The black box society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

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

RODOTÀ, Stefano. Transformações do corpo. *Revista Trimestral de Direito Civil*, v. 19, p. 91-107, 2004.

SILVA, Priscilla Regina. Os direitos dos titulares de dados. In: MULHOLLAND, Caitlin (Org.) *LGPD e o Novo Marco Normativo no Brasil*. Porto Alegre: Arquipélago, 2020.

SOMAINI, Laura. The right to data portability and user control: ambitions and limitations. *Rivista di Diritto Dei Media*, Milano, v. 2018, n. 3, p.1-27, out. 2018. Disponível em: <<http://www.medialaws.eu/rivista/the-right-to-data-portability-and-user-control-ambitions-and-limitations/>>. Acesso em: 02 fev. 2020.

SOUZA, Carlos Affonso. *Eles sabem quem é você? Entenda o monitoramento de celulares na quarentena*. Disponível em: <<https://tecfront.blogosfera.uol.com.br/2020/04/17/eles-sabem-quem-e-voce-entenda-o-monitoramento-de-celulares-na-quarentena/>>. Acesso em: 14 fev. 21.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 417-441.

SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. In: DONEDA, Danilo *et al.* (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. cap. 12, p. 243-270.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Direitos do titular de dados pessoais na Lei 13.709/2018: uma abordagem sistemática. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019, p. 243-286

SUNSTEIN, Cass R. Algorithms, correcting biases. *Social Research*, [s. l.], v. 86, n. 2, p. 499-511, summer 2019. Published by Johns Hopkins University Press.

TEPEDINO, Gustavo, TEFFÉ, Chiara S. de. Consentimento e Proteção de Dados Pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

TROIANO, Stefano. Il diritto alla portabilità dei dati personali. In: GALGANO, Nadia Zorzi (Org.). *Persona e mercato dei dati. Riflessioni sul GDPR*. Milano: Cedam, 2019. cap. 7, p. 195-218. E-book.

TSAMADOS, Andreas; AGGARWAL, Nikita; COWLS, Josh; MORLEY, Jessica; ROBERTS, Huw; TADDEO, Mariarosaria; FLORIDI, Luciano. The ethics of algorithms: key problems and solutions. *AI & Society*, [s. l.], 20 fev. 2021. Springer Science and Business Media LLC. <http://dx.doi.org/10.1007/s00146-021-01154-8>.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, [s. l.], v. 7, n. 2, pp. 76-99, may 2017. Oxford University Press (OUP). <<http://dx.doi.org/10.1093/idpl/ix005>>.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual explanations without opening the black box: automated decisions and the GDPR. *Harvard Journal Of Law & Technology*, Cambridge, v. 31, n. 2, p. 841-887, 2018. Disponível em: <<https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>>. Acesso em: 09 jul. 2020.

Recebido em: 22/06/2021

1º Parecer em: 05/07/2021

2º Parecer em: 12/07/2021