REVISTA DA ESDM

ISSNe: 2595-7589

DIREITOS DO TITULAR DOS DADOS NO PODER PÚBLICO: ANÁLISE DA PORTABILIDADE DE DADOS

Data subject rights in the public sector: analysis of the right to data portability

Daniela Copetti Cravo

Procuradora Municipal de Porto Alegre, RS, Brasil. Doutora em Direito pela UFRGS.

Resumo

O direito à portabilidade de dados pessoais é uma das grandes novidades trazidas pela LGPD (Lei Geral de Proteção de Dados). Tal direito, que tem a potencialidade de gerar inúmeros benefícios aos indivíduos, à sociedade e ao mercado, pode ser entendido como a possibilidade do titular de transferir seus dados entre diferentes controladores ou de obter uma cópia dos dados para armazenamento e uso. A proposta desse artigo é investigar se esse direito pode ser exercido pelo titular dos dados perante o Poder Público e, caso positivo, em qual extensão ou profundidade.

Palavras-Chave: Proteção de Dados Pessoais. Portabilidade de Dados. Poder Público.

Abstract

The right to data portability is one of the major novelties brought by the LGPD (General Data Protection Act). Such right, which has the potential to generate countless benefits to individuals, society and the market, can be understood as the possibility for the data subject to transfer his data between different controllers or to obtain a copy of the data for storage and use. The purpose of this article is to investigate whether this right can be exercised by the data subject in the public sector and, if so, to what extent and thoroughness the right can be exercised.

Keywords: Personal Data Protection. Data Portability. Public Sector.

Sumário

1. INTRODUÇÃO

A proteção dos dados pessoais já é uma realidade no Brasil e isso vale também para o Poder Público, como bem decidiu o STF, em maio do presente ano no julgamento da Medida Cautelar da ADI 6387 (STF, 2020). Tal máxima ganha saliência na atual crise sanitária, em que os dados pessoais se tornam um fator importante para o desenvolvimento de políticas de enfretamento à Covid-19.

Um passo importante para evolução do tema no ordenamento jurídico pátrio diz respeito ao início da vigência da LGPD (Lei Geral de Proteção de Dados), que, por meio de novidades e aplicação transversal, buscará garantir segurança jurídica e uniformidade. No combate à fragmentação, a LGPD conjuga em apenas um diploma as normas pertinentes à proteção de dados, tratando como controlador tanto o poder público, quanto o privado.

Além disso, a LGPD também confere ao titular dos dados um catálogo de direitos (alguns de forma originária, outros já existentes no nosso sistema). Estando a mencionada lei próxima de sua entrada em vigor, é importante refletir como os controladores, em especial o Poder Público, deverão estar preparados para observar e promover esses direitos do titular dos dados, como a portabilidade de dados pessoais.

A portabilidade de dados, entendida como a possibilidade do titular de transferir seus dados entre diferentes controladores ou obter uma cópia dos dados para armazenamento e uso, tem a potencialidade de gerar inúmeros benefícios aos indivíduos, à sociedade e ao mercado. Além dos efeitos concorrenciais, por meio da redução das barreiras de entrada e do efeito *lock-in*, a portabilidade de dados pode ser usada como uma ferramenta de gestão dos dados pelos titulares, decidindo com quem desejam compartilhar e manter seus dados. Ainda, os dados podem auxiliar o desenvolvimento de atividades, sejam essas de lazer, sociais, familiares ou profissionais.[1]

Posto isso, surge a dúvida a respeito do exercício desse direito perante o poder público. Será que esse deve cumprir e promover o direito à portabilidade de dados pessoais? Em caso positivo, em qual extensão? A portabilidade deve ser aplicada a qualquer tratamento de dados realizado pela administração pública ou apenas a certas bases legais de tratamento? Responder a tais questionamentos é justamente o objetivo do presente artigo.

2. A PROTEÇÃO DOS DADOS PESSOAIS

A importância dos dados para a economia digital é incontestável. Esses são insumo indispensável para qualquer atividade, proporcionando serviços mais inovadores e de maior qualidade. Da mesma forma, no poder público, especialmente com implantação de um governo digital (WIMMER, 2020, p. 29), os dados pessoais também passam a ter esse caráter de essencialidade e podem servir como uma ferramenta importante para gerar valor ao cidadão, seja por um atendimento mais rápido e prático, seja por meio de políticas públicas ou serviços públicos mais eficientes.

Ocorre que apesar dessa faceta de insumo essencial ao desenvolvimento das atividades econômicas e administrativas (poder público), os dados pessoais são um desdobramento da nossa personalidade. Isso porque, muito embora possam representar um mero

registro (abstrato ou concreto), quando mensurados ou classificados podem vir a revelar nossos gostos, preferências e necessidades.

Diante de ferramentas complexas de coleta, armazenamento e processamento de dados, qualquer simples vestígio de dado ou um mero fragmento pode servir de fonte para obtenção de informações relevantes ou sensíveis. No atual estágio da sociedade, não há dados irrelevantes: "um dado sozinho, aparentemente insignificante, pode adquirir um novo valor quando cruzado com outras informações, compartilhado com pessoas ou entidades distintas e utilizado para formar perfis pessoais" (MENDES, 2020).

Justamente pelo incremento na capacidade computacional que se fala em uma proteção de dados e não somente em proteção das informações (que é o resultado obtido pelo tratamento/mensuração do dado bruto). No passado, a proteção era apenas da informação e não dos dados brutos (VERONESE, 2019, p. 389), o que, na realidade atual, além de insuficiente, pode tornar a própria tutela da informação totalmente inócua.

As organizações ou empresas, ao se munirem originariamente com meros fragmentos ou dados, podem, após o uso de certas ferramentas, obter informações suficientes para prever tendências, estimular e/ou influenciar o comportamento dos indivíduos. Assim, caso os dados sejam utilizados de forma desproporcional ou fora de sua finalidade justificante, é possível que haja um comprometimento ao livre desenvolvimento da personalidade, que tem como "valor-fonte" a pessoa (CACHAPUZ, 2017, p. 1130).

Percebe-se, ademais, que a proteção de dados, muito embora herdeira da tutela da privacidade, é mais ampla que essa e apresenta características próprias (DONEDA, 2011, p. 95), razão pela deve ser reconhecida como um direito autônomo. Inicialmente, nas primeiras gerações de leis, a proteção de dados estava ligada ao fenômeno computacional e à ideia da privacidade como uma liberdade negativa.

No entanto, a partir do momento em que se percebeu que os dados pessoais dos cidadãos se tornaram um requisito indispensável para sua participação na vida social, a proteção deixa de ser focada apenas na liberdade de fornecer ou não os dados e migra para uma dimensão positiva da proteção (DONEDA, 2011, p. 97), consubstanciada na autodeterminação informativa,[2] evocada pela Corte Constitucional Alemã, em 1983, na sua famosa *Census Decision*.

O início dessa nova dimensão teve como enfoque o intenso fluxo de informações pessoais utilizado pelo Estado (e também pelos entes privados) que possibilitava até mesmo a obtenção de um quadro completo da personalidade dos indivíduos (MENDES, 2018, p. 188). A partir do momento que os cidadãos não sabem quem e o que se sabe sobre eles, nem quando ou em que circunstância, eles poderão começar a mudar seu comportamento ou adotar novas posturas (talvez até de autocensura), prejudicando a sua personalidade e o desenvolvimento da própria democracia.

Para além de um possível risco de abuso por parte do poder estatal decorrente do acesso a tais informações do indivíduo, a realidade atual, caracterizada por monopólios digitais de grandes plataformas e da digitalização acelerada da sociedade, também coloca

os agentes privados em uma condição de superioridade em decorrência do massivo número de dados pessoais que possuem acesso. E tal realidade é igualmente capaz de prejudicar a personalidade e a democracia, razão pela qual há uma forte preocupação com um possível capitalismo da vigilância (ZUBOFF, 2019).

Diante dessas vulnerabilidades, uma nova geração de legislações específicas sobre proteção de dados foi surgindo nas mais diferentes jurisdições. O maior exemplo é a União Europeia,[3] que substituiu sua antiga Directiva 95/46/EC pelo Regulamento Geral de Proteção de Dados Europeu (RGPD), com início de aplicação em 25 de maio de 2018. O Brasil, depois de um longo período de espera, editou a Lei n.º 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD).

Apesar de a LGPD ainda não estar em vigor no Brasil, não podemos deixar de reconhecer que a proteção de dados já é uma realidade, inclusive confirmada recentemente pelo STF. Nesse sentido, cita-se a paradigmática decisão adotada, durante a pandemia, no bojo da Medida Cautelar em Ação Direta de Inconstitucionalidade n. 6.387/DF (STF, 2020), cujo objeto de controle era a Medida Provisória n. 954/2020.

Essa Medida Provisória previa a disponibilização de dados dos consumidores pelas empresas de telecomunicação prestadoras de serviços de telefonia fixa e móvel pessoal no país à Fundação IBGE, em meio eletrônico, para a produção estatística oficial. No entanto, não trazia em seu bojo a adoção de salvaguardadas adequadas às recomendações internacionais e às boas práticas em relação ao uso legítimo de dados no âmbito do combate ao coronavírus. Ainda, não havia fundamentação motivada ao uso compartilhado dos dados em questão, bem como uma definição específica da finalidade e da necessidade do tratamento de dados a ser realizado.

Além da decisão do STF e da edição da LGPD, cabe dar destaque à Proposta de Emenda à Constituição (PEC) 17/2019, em trâmite no Congresso Nacional, cuja finalidade é adicionar a proteção dos dados pessoais no rol de direitos e garantias fundamentais (artigo 5º, inciso XII), além de estabelecer a competência privativa da União para legislar na matéria (artigo 22, inciso XXX).

Portanto, a proteção de dados pessoais já é uma realidade não só em outros lugares do mundo, como também no Brasil. Estando a LGPD próxima de sua entrada em vigor, é importante refletir como os controladores, em especial o Poder Público, deverão estar preparados para observar e promover os direitos do titular dos dados, como o da portabilidade de dados pessoais.

3. O DIREITO À PORTABILIDADE DE DADOS

A LGPD trouxe inúmeras novidades ao ordenamento jurídico brasileiro. Entre essas, cita-se a tentativa de uniformização do tratamento de dados pessoais, conjugando em apenas um diploma as normas pertinentes ao tema, tratando como controlador tanto o poder público como o privado. Essa simetria entre público e privado no tocante ao uso de dados pessoais é inclusive uma tendência global e pode ser observada nas diretrizes da OCDE sobre proteção da privacidade e fluxos transfronteiriços de dados pessoais e na Convenção

para a Proteção dos Indivíduos com Respeito ao Processamento Automático de Dados Pessoais (WIMMER, 2020, p. 30).

Assim, com algumas exceções de não incidência da lei (a exemplo do artigo 4º), a LGPD tenta combater a fragmentação e aplica-se independentemente se o dado foi originário de uma relação de consumo, tributária, de direito administrativo, de saúde, entre outras complexas relações que o indivíduo atualmente desempenha na pós-modernidade. Veja que mesmo antes da vigência da LGPD, já era possível vislumbrar uma disciplina da proteção de dados no Brasil (embora não fosse completa), mas sua setorização e pulverização (OLIVEIRA; LOPES, 2019, p. 72) eram um dos principais gargalos para a sua efetividade.

Nessa busca por segurança jurídica no cenário brasileiro, a LGPD estabelece quando o tratamento de dados poderá ocorrer, elencando, para tanto, um rol de bases legais nos artigos 7º e 11. Ainda, a LGPD cria uma Autoridade Nacional de Proteção de Dados, e as figuras do controlador, operador e encarregado. A LGPD, portanto, estabelece um vocabulário de definições comuns, que terá aplicabilidade transversal (BIONI, 2019, p. 32).

Destarte, essa lei surge[4] para suprir as omissões existentes no ordenamento jurídico brasileiro e garantir um nível adequado de proteção (CUEVA, 2017, p. 66). Nessa senda, cita-se, ainda, o catálogo de direitos conferidos ao titular dos dados, que o coloca como protagonista na realidade digital vivenciada.

No artigo 18 da LGPD, constam alguns dos direitos do titular dos dados pessoais que podem ser obtidos do controlador, a qualquer momento e mediante requisição. Cabe mencionar que o titular é pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, inciso V, da LGPD); já o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, inciso VI, da LGPD).

Dentre esses direitos do artigo 18 da LGPD, está, no inciso V, o direito à portabilidade de dados. Apresentando poucas disposições sobre esse direito, a LGPD foi extremamente sintética, limitando-se a afirmar que (i) a portabilidade será realizada entre um fornecedor a outro, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial (inciso V); (ii) que não se inclui nessa os dados já anonimizados (art. 18,§7º); (iii) que a autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade (art. 40); e (iv) que o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde é vedado, exceto, entre outras exceções, para permitir a portabilidade de dados quando solicitada pelo titular (§4º, inciso I, do art.11).

Além dessas disposições específicas à portabilidade, no exercício desse direito, deverá ser observado o §3º do artigo 18 que prevê a necessidade de requerimento expresso do titular ou de representante legalmente constituído ao agente de tratamento (veja que a lei aqui se refere ao agente de tratamento, que pode ser o controlador ou operador, este é aquele que realiza o tratamento de dados pessoais em nome do controlador).

Também tem aplicabilidade à portabilidade de dados o §4º do mesmo artigo que dis-

põe que no caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: (i) comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; (ii) indicar as razões de fato ou de direito que impedem a adoção imediata da providência. Ainda, o § 5º do referido artigo menciona que o requerimento será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento, o que vale também para a portabilidade.

Apesar dessas disposições, há dúvidas quanto ao conceito de portabilidade de dados pessoais no direito brasileiro, nomeadamente para saber se essa se limita à transferência de dados entre fornecedores, como previsto literalmente no inciso V do artigo 18. Comparando a LGPD com outras legislações, é possível verificar que não há uma definição comum para a portabilidade.

No âmbito europeu, temos o artigo 20 do Regulamento Geral de Proteção de Dados Europeu (RGPD). Esse artigo dispõe que "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.

Nos Estados Unidos da América, a *California Consumer Privacy Act* (CCPA) prevê a portabilidade de dados por meio do fornecimento das informações pessoais em formato facilmente utilizável para permitir que o consumidor, caso queira, transfira essas informações para outra entidade sem impedimentos.

Fato é que cada legislação tem definido de forma diversa o direito à portabilidade de dados. Algumas enfocam no direito à transmissão direta dos dados a um novo controlador, outras no direito de receber os dados e armazená-los em algum dispositivo pessoal ou no envio dos dados pelo próprio titular ao novo controlador.

Entende-se que a portabilidade de dados no Brasil deve ter um conceito amplo, podendo ser definida da seguinte forma: a portabilidade de dados pessoais é o direito do titular dos dados (i) de receber do controlador os dados pessoais que lhe digam respeito, num formato eletrônico, para uso e/ou armazenamento (ii) de transmitir esses dados a outro controlador, no momento presente ou futuro, e (iii) de requerer que os seus dados pessoais sejam transferidos diretamente a outro controlador (receptor), sempre que isso seja tecnicamente possível.

Veja que as duas primeiras hipóteses (i) e (ii) já encontram embasamento legal no Brasil, muito embora dentro do direito de acesso, como pode ser visualizado no §3º do artigo 19 da LGPD. Assim, essas duas formas de exercício podem ser exigidas pelo titular, bem como a hipótese (iii), prevista no próprio inciso da portabilidade de dados (art. 18, inciso V, da LGPD).

Cabe a reflexão, no entanto, se essa divisão da portabilidade (duas primeiras hipóteses dentro do direito de acesso e a terceira no direito à portabilidade) pelo legislador foi acertada, uma vez que parece existir um certo descompasso e desarmonia entre o previsto

no inciso V do artigo 18, que não limita à portabilidade ao tratamento embasado no consentimento ou em um contrato, e o disposto no §3º, do artigo 19 da LGPD. Justamente para evitar essa fragmentação, entende-se que essas formas de exercício (cópia dos dados e utilização/transferência a outro controlador) deveriam constar dentro da disciplina da portabilidade, como ocorrido no RGPD, no artigo 20 (n.º 1 e n.º 2).

Outro ponto importante é que no caso da transferência direta dos dados a outro controlador (art. 18, inciso V), entende-se que essa forma de exercício não implica, por si só, o encerramento da relação estabelecida entre o titular e o controlador (transmissor), exceto se assim desejar o titular. Há casos que o titular desejará apenas usar os dados em outro serviço, que às vezes sequer é um concorrente direto do controlador, mas um mero serviço complementar. Cita-se como exemplo o uso já corrente de API (*Application Programming Interface*) para transferências de dados, como ocorre nos social logins.

Apresentado o conceito que se entende correto para a disciplina da portabilidade de dados no Brasil (cópia dos dados, mera transferência dos dados e portabilidade de dados propriamente dita com o encerramento da relação), cabe verificar a quem essa se aplica. Será que se aplica ao poder publico?

4. PORTABILIDADE DE DADOS NO PODER PÚBLICO?

Conforme visto anteriormente, um dos objetivos da LGPD é dar uniformidade à disciplina da proteção de dados, que se aplica tanto ao poder público como ao privado. Isso inclusive é uma tendência global, que tem sido adotada em várias legislações e convenções internacionais.

No entanto, não se pode descurar que a relação entre poder público e administrado é diferente da relação poder privado e indivíduos, razão pela qual a própria LGPD destinou um capítulo próprio ao poder público (arts. 23 a 30 da LGPD). Na maioria das vezes, o tratamento de dados feito pelo poder público decorre do cumprimento de seus deveres constitucionais e legais, ou seja, situações que, como regra, não são embasadas no consentimento.

Justamente por isso, é válida a reflexão acerca dos direitos dos titulares previstos no artigo 18 e se esses devem se aplicar indistintamente aos controladores, como previsto na sua redação, independente de serem entes públicos ou privados. Em especial, precisa-se observar com mais cuidado o cumprimento da portabilidade de dados pessoais pelo poder público[5] e até mesmo investigar a necessidade da edição de alguma legislação específica (art. 23, §3º, da LGPD).

Uma leitura rápida e literal do artigo 18, inciso V, da LGPD, poderia levar à conclusão que a portabilidade de dados apenas se aplicaria aos agentes de tratamento que se enquadrassem no conceito de “fornecedor”. E, para definir esse conceito, seria necessário um diálogo com as normas do Código de Defesa do Consumidor (CDC).

Com efeito, nessa interpretação literal, o poder público só estaria obrigado a observar a portabilidade nos casos em que atua como fornecedor, ou seja, em casos em que há a incidência do artigo 3º do CDC. Em geral, com exceção das empresas públicas e sociedades de economia mista que atuem na atividade econômica em sentido estrito, o poder público é

considerado fornecedor quando presta serviços públicos que sejam singulares e remunerados por tarifa (STJ, 2005).

Pois bem, nesse caso, a portabilidade de dados se aplicaria quase que de forma "excepcional" no poder público, já que a maioria das suas atividades não se enquadra nas características acima descritas. No entanto, não se pode fazer uma interpretação em tiras da LGPD, nem ignorar seus princípios e outras regras gerais. Assim, a interpretação do inciso V do artigo 18 da LGPD precisa ser sistemática, de modo que a portabilidade de dados deveria ser destinada a um contexto não restrito apenas às relações de consumo.

Nesse ponto, entende-se que a LGPD não adotou a melhor técnica ao utilizar a expressão "fornecedor" no inciso V do artigo 18, até mesmo porque tal conceito cria fragmentação jurídica, indo de encontro como o objetivo de uma lei geral: garantir uniformidade e segurança jurídica. Ademais, o próprio caput do artigo 18 estabelece o controlador como o responsável pela promoção dos direitos dos titulares, o que deveria valer também para a portabilidade, já que está topograficamente inserida nesse artigo.

Lado outro, entende-se que uma abrangência muito ampla da portabilidade pode ter efeitos colaterais, justamente pela dificuldade e pelos custos decorrentes do *compliance*. Uma solução para tanto poderia ser estabelecer o controlador como o responsável pela portabilidade de dados, seja esse um ente público ou privado, mas limitar esse direito para as hipóteses de tratamento realizadas com base no consentimento ou necessárias para a execução de contrato, como fez o Regulamento Europeu de Proteção de Dados – RGPD (considerando 68 e artigo 20, n. 1, alínea "a").

Nesse cenário, o poder público não estaria obrigado, por exemplo, a realizar a portabilidade dos dados tratados para a execução de políticas públicas ou no cumprimento de deveres legais, como a execução de serviço público, entre outras hipóteses. Destarte, haveria uma redução significativa da incidência do inciso V do artigo 18 da LGPD nas atividades desenvolvidas pela administração pública, o que parece ser razoável e condizente com o estado de coisas buscado pela portabilidade, além de estar em harmonia com o previsto no artigo 19, §3º da LGPD (que apesar de estar dentro do direito de acesso, pode ser considerado como uma das formas de exercício da portabilidade).

Veja-se que muito embora a legislação brasileira não vede a utilização da base legal do consentimento por órgãos públicos (WIMMER, 2020, p. 32), essa possível aplicação será, na prática, vestigial. A título de exemplo, o poder público pode ser obrigado a implementar a portabilidade com relação aos dados pessoais que coleta por meio da disseminação de newsletter (EUROPEAN COMMISSION, 2018).

Pontua-se ainda que a vedação ao Poder Público de transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, prevista no artigo 26, §1º, da LGPD, não atinge o direito à portabilidade. Tendo em vista que a transferência se dará com base no exercício de um direito pelo próprio titular dos dados, entende-se pela legitimidade da transferência, que tem respaldo legal no artigo 18, inciso V, da LGPD.

Em última análise, defende-se que a portabilidade de dados deve ser observada pelo

poder público. No entanto, sugere-se que essa deve incidir apenas nos casos de tratamento de dados realizado com base no consentimento ou quando necessário para a execução de um contrato.

5. CONSIDERAÇÕES FINAIS

A entrada em vigor da LGPD se aproxima e, mesmo que as sanções venham em um momento posterior, os direitos precisarão ser promovidos, inclusive pelo próprio poder público (resta saber em qual extensão ou profundidade). Portanto, a extensão e a profundidade de alguns direitos dos titulares de dados perante o poder público precisam ser endereçadas e discutidas o quanto antes possível, até mesmo para verificar a necessidade da inclusão de tais preceitos em uma legislação específica ou em regulamento (art. 18, §5º e art. 23, §3º da LGPD).

Nessa linha, o presente artigo, a partir de uma investigação específica sobre o direito à portabilidade de dados, concluiu que esse deve ser aplicado ao poder público, mas sugere algumas propostas interpretativas nessa aplicação. Incialmente, defende-se que a LGPD não adotou a melhor técnica ao utilizar a expressão “fornecedor” no inciso V do artigo 18, até mesmo porque tal conceito cria fragmentação jurídica, indo de encontro como o objetivo de uma lei geral: garantir uniformidade e segurança jurídica. Ademais, o próprio caput do artigo 18 estabelece o controlador como o responsável pela promoção dos direitos dos titulares, o que deveria valer também para a portabilidade, já que está topograficamente inserida nesse artigo.

Lado outro, entende-se que uma abrangência muito ampla da portabilidade pode ter efeitos colaterais, justamente pela dificuldade e pelos custos decorrentes do *compliance*. Uma solução para tanto poderia ser estabelecer o controlador como o responsável pela portabilidade de dados, seja esse um ente público ou privado, mas limitar esse direito para as hipóteses de tratamento realizadas com base no consentimento ou necessárias para a execução de contrato, como fez o Regulamento Europeu de Proteção de Dados – RGPD (considerando 68 e artigo 20, n. 1, alínea “a”).

Nesse cenário, o poder público não estaria obrigado, por exemplo, a realizar a portabilidade dos dados tratados para a execução de políticas públicas ou no cumprimento de deveres legais, como a execução de serviço público, entre outras hipóteses. Destarte, haveria uma redução significativa da incidência do inciso V do artigo 18 da LGPD nas atividades desenvolvidas pela administração pública, o que parece ser razoável e condizente com o estado de coisas buscado pela portabilidade, além de estar em harmonia com o previsto no artigo 19, §3º da LGPD (que apesar de estar dentro do direito de acesso, pode ser considerado como uma das formas de exercício da portabilidade).

6. NOTAS

1. A portabilidade de dados é uma ferramenta que pode facilitar nossa vida ou gerar alguma utilidade, principalmente na tomada de decisões. Nesse sentido, ela poderá nos auxiliar a verificar o impacto do nosso padrão de consumo e a adoção de hábitos mais sustentáveis, entre outras possibilidades. Um exemplo seria a transferência de nossas listas de compras a um aplicativo de aconselhamento nutricional ou a utilização dos nossos dados de consumo em transporte e energia para criar um índice de carbono

individual. A esse respeito, cita-se a seguinte reportagem: https://www.latribune.fr/opinions/la-portabilite--des-donnees-un-levier-citoyen-pour-la-transition-ecologique-854175.html

2. Fabiano Menke afirma que a autodeterminação informativa confere ao indivíduo o poder de decisão quanto à divulgação ou utilização de seus dados pessoais. Essa se insere no direito à autoapresentação, que é uma das três categorias do direito geral da personalidade. (MENKE, 2014, p. 210-211).

3. Stefano Rodotà informa que a União Europeia é o lugar do mundo com maior desenvolvimento em matéria de proteção de dados pessoais e de direitos fundamentais. (RODOTÀ, 2014).

4. Como narra Anderson Schreiber (2019, p. 369), até 2018, a proteção de dados pessoais era meramente reflexa no nosso ordenamento, sendo tangenciada por leis esparsas ou setoriais. Diante da insuficiência dessas disposições, os esforços acabaram recaindo sobre a doutrina (em especial as obras de Danilo Doneda, em 2006, e de Laura Mendes, em 2014). Veja que ausência de uma lei apropriada para reger o tratamento de dados pessoais no Brasil é considerada espantosa quando comparada com outros países da própria América Latina, que além de possuírem legislações gerais de proteção de dados pessoais, também já contam com mecanismos específicos para assegurar os direitos positivados e com a criação de agências reguladoras (ZANATTA, 2015, p. 453).

5. A análise feita nesse artigo tem como enforque a administração pública em geral, com exceção das empresas públicas e sociedade de economia mista que atuem em regime de concorrência, já que essas receberam o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, conforme previsto no artigo 24 da LGPD.

REFERÊNCIAS

BRASIL. Supremo Tribunal Federal. **Medida Cautelar em Ação Direta de Inconstitucionalidade n. 6.387/DF**. Brasília: STF, 2020. Plenário, maio de 2020.

BRASIL. Superior Tribunal Justiça (2. Turma). **REsp 609.332/SC**. Relatora: Min. Eliana Calmon, 9 de agosto de 2005. Brasília: STJ, 2005. Diário de Justiça, 05 set. 2005.

BIONI, Bruno. Inovar pela lei. **GV EXECUTIVO**, v. 18, p. 31-33, 2019.

CACHAPUZ, Maria Cláudia. Direitos de personalidade e responsabilidade civil na perspectiva da ética do discurso. **RJLB - Revista Jurídica Luso-Brasileira**, v. 4, p. 1123-1154, 2017.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 13, ano 4, p. 59-67, out./dez., 2017.

DONEDA, Danilo. A proteção de dados com um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez., 2011

EUROPEAN COMMISSION. **GDPR Data Portability and Core Vocabularies**, 2018.

MENDES, Laura Schertel. A encruzilhada da Proteção de Dados no Brasil e o Caso do IBGE. **Jota**, 2020.

MENDES, Laura Schertel. Habeas data e autodeterminação informativa. **Revista Brasileira de Direitos Fundamentais & Justiça**, p. 185-216, 12 (39), 2018.

MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In:* MENDES, Gilmar; SARLET, Ingo;

COELHO, Alexandre (org.). **Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2017. p. 210-211.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela. Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena (org.). **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. v. 1, p. 53-84.

RODOTÀ, Stefano. Las lecciones de wikileaks: nueva transparencia y nueva distribución de poder. *In:* Mañas, José Luis Piñar (org.). **Transparencia, acceso a la información y protección de datos**. Madrid: Editorial Reus, 2014. p. 9-17.

SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena (org.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. v. 1, p. 367-383.

VERONESE, Alexandre. Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena (org.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. v. 1, p. 385-415.

WIMMER, Miriam. Cidadania, Tecnologia e Governo Digital: Proteção de Dados Pessoais no Estado Movido a Dados. *In:* BARBOSA, Alexandre F. (org.). **TIC Governo Eletrônico 2019**. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. São Paulo: Comitê Gestor da Internet no Brasil, 2020. v. 1, p. 27-36.

ZANATTA, Rafael. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito e Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015. p. 447-470.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. Londres: Profile Books Ltd., 2019.

Recebido em: 20/08/2020

Aceito em: 21/08/2020