O poder público e a proteção de dados pessoais no Brasil: novos desafios, velhas práticas administrativas*

Data protection and public institutions in Brazil: new challenges, old administrative practices

*Lucas Borges de Carvalho***

RESUMO

Desde a sua tramitação no Congresso Nacional, a Lei Geral de Proteção de Dados Pessoais gerou resistências no âmbito do setor público no país, em geral fundadas na concepção de que suas normas constituem um entrave à inovação e à execução eficiente de políticas e serviços públicos. O artigo sustenta que essa retórica da eficiência e da inovação encobre o recurso a velhas práticas administrativas. De um lado, amplas prerrogativas

* Artigo recebido em 14 de novembro de 2022 e aprovado em 10 de janeiro de 2023. DOI: https://doi.org/10.12660/rda.v282.2023.89347.

** Autoridade Nacional de Proteção de Dados (ANPD), Brasília, DF, Brasil. Doutor em direito pela Universidade de Brasília. Procurador federal. Assessor do Conselho Diretor da ANPD. E-mail: lucasbcarvalho@gmail.com.

discricionárias, imunes ao controle social e jurisdicional. De outro, a falta de transparência das operações com dados pessoais realizadas por instituições públicas. Amparado em decisões recentes do Supremo Tribunal Federal, argumenta-se que o direito à proteção de dados pessoais possui uma relevante dimensão política, que promove a transparência e garante aos titulares de dados o controle sobre o fluxo de suas informações na sociedade. Trata-se de uma necessária barreira jurídica para evitar desvios de finalidade e conter os riscos de vigilância e de práticas discriminatórias.

PALAVRAS-CHAVE

democracia — discricionariedade administrativa — Lei Geral de Proteção de Dados Pessoais (LGPD) — proteção de dados pessoais — transparência

ABSTRACT

Since its discussion in National Congress, the General Data Protection Law has generated resistance within the public sector in Brazil, in general, based on the conception that its rules are an obstacle to innovation and the efficient execution of public policies and services. The article argues that this rhetoric of efficiency and innovation masks old administrative practices. On the one hand, broad discretionary prerogatives, immune to social and jurisdictional control. On the other hand, the lack of transparency in the processing of personal data by public institutions. Based on recent Supreme Court decisions, it is argued that data protection rights have a relevant political dimension, which promotes transparency and guarantees data subjects control over the flow of their information in society. This is a necessary legal barrier to avoid misuse and restrain surveillance risks and discriminatory practices.

KEYWORDS

administrative discretion — data protection — democracy — General Data Protection Law (LGPD) — transparency

Introdução

Em abril de 2018, durante a tramitação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Congresso Nacional, o governo federal elaborou um

substitutivo ao então Projeto de Lei (PL) nº 330/2013 com o objetivo de excluir o poder público da incidência das normas de proteção de dados. À época, a proposta foi defendida sob o argumento de que "num ambiente digital, o fluxo de dados não pode ter muitas amarras". Alegava-se que já existiria suficiente "jurisprudência para a proteção de dados" no setor público, a exemplo das disposições da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação — LAI). Ademais, "a necessidade de solicitar o consentimento do cidadão para a efetivação de cada política pública seria um entrave", razão pela qual o modelo sugerido garantiria "segurança ao dado do cidadão sem atravancar a inovação".[1]

Ao final do processo legislativo, a controversa proposta do governo federal não foi acolhida. Como consequência, a redação final da LGPD incluiu expressa previsão de aplicação de suas normas às pessoas jurídicas de direito público (art. 1º), as quais devem observar princípios gerais como os da necessidade, finalidade e adequação (art. 6º), além de obrigações específicas de transparência (art. 23). Da mesma forma, aos usuários de serviços públicos foram assegurados importantes direitos, tais como os de acesso aos dados e correção de dados incompletos, inexatos ou desatualizados (art. 18, II e III), de oposição a tratamento efetuado sem consentimento (art. 18, § 2º) e de revisão de decisões automatizadas (art. 20). Por fim, em caso de irregularidades, a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar sanções administrativas a entidades e órgãos públicos (art. 52, § 3º).

Apesar da expressa decisão tomada no âmbito legislativo, a aprovação da LGPD não afastou a influência e a persistência da concepção de que a legislação de proteção de dados pessoais constitui um entrave à inovação e à execução eficiente de políticas e serviços públicos. Conforme será demonstrado neste trabalho, essa concepção sustentou direta ou indiretamente diversas reações institucionais às mudanças trazidas pela LGPD, levando-se a uma espécie de disputa interpretativa em torno da definição de limites, mais ou menos amplos, ao modo pelo qual as instituições públicas até então lidavam com os dados pessoais de cidadãos.

A hipótese a ser desenvolvida é a de que, apesar da retórica da eficiência e da inovação, a resistência às novas disposições legais se ampara em

---

[1] SOPRANA, Paula. Governo quer lei de proteção de dados que tira responsabilidade do Poder Público. *O Globo*, 11 abr. 2018. Disponível em: https://glo.bo/3d75ym1. Acesso em: 14 out. 2022; LEMOS, Ronaldo. Privacidade vale também para governo. *Folha de S.Paulo*, 16 abr. 2018. Disponível em: https://bit.ly/2NcpvwV. Acesso em: 14 out. 2022.

velhas e bem conhecidas práticas administrativas, associadas, de um lado, à defesa de amplas prerrogativas discricionárias, imunes ao controle social e jurisdicional; e, de outro, ao sigilo e à falta de transparência das operações com dados pessoais realizadas por entidades e órgãos públicos. Por isso, em última análise, o que está em causa na aplicação da LGPD ao setor público é a necessidade de instituição de mecanismos adequados de garantia de direitos, de prestação de contas à sociedade e de controle público sobre o tratamento de dados pessoais realizado pelas instituições públicas.

A abordagem metodológica proposta se baseia em uma análise jurídico-compreensiva, de cunho histórico, efetuada a partir da revisão bibliográfica sobre o tema, da análise e discussão da legislação aplicável, de documentos públicos, de informações divulgadas pela imprensa e de casos paradigmáticos recentes, especialmente decisões do Supremo Tribunal Federal (STF). Assim, propõe-se uma construção analítica capaz de sustentar uma avaliação crítica das diferentes concepções sobre o tratamento de dados pessoais pelo poder público, bem como do processo real de aplicação das normas estabelecidas pela LGPD.

Além desta introdução e da conclusão, o artigo está dividido em três partes. Na primeira, a análise se concentra sobre o veto a alguns dispositivos da LGPD e as sucessivas iniciativas visando postergar a sua vigência. Como será demonstrado, ambas as iniciativas foram justificadas sob o argumento de que a nova legislação de proteção de dados poderia inviabilizar ou afetar a continuidade da prestação de serviços públicos. A segunda parte demonstra que o recurso a amplas prerrogativas discricionárias constitui uma prática recorrente para o tratamento de dados pessoais no setor público, muitas vezes associada a finalidades genéricas e ao potencial desvio de finalidade. A terceira parte discute a dimensão política do direito à proteção de dados pessoais, relacionada com as obrigações de transparência estabelecidas pela LGPD e, de forma mais geral, com o controle democrático de autoridades e instituições públicas.

1. Vetos e vigência da LGPD

A disputa em torno da definição de limites à aplicação da LGPD ao setor público se estabeleceu, de forma ampla e aberta, logo após a publicação da lei, em agosto de 2018. Com efeito, argumentos similares aos apresentados

durante a tramitação legislativa, expressando uma concepção reativa às normas de proteção de dados pessoais, podem ser identificados: (i) nas razões que justificaram parte dos vetos apresentados pelo presidente da República; e (ii) nas sucessivas iniciativas visando postergar a vigência da lei.

Em relação ao primeiro aspecto, merece destaque o veto ao art. 28 da LGPD, que estabelecia uma obrigação simples de transparência, ao determinar que "a comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I do caput do art. 23 desta Lei". Assim, por exemplo, caso um Ministério disponibilizasse a uma autarquia o acesso a determinado banco de dados, deveria conferir publicidade a esta operação. De acordo com o art. 23, I, citado ao final do dispositivo vetado, a publicidade deveria abranger a divulgação de "informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos".

Não obstante a clareza e a objetividade da regra, o veto foi justificado sob o argumento de que a "publicidade irrestrita" prevista na norma poderia "tornar inviável o exercício regular de algumas ações públicas como as de fiscalização, controle e polícia administrativa".[2] Como se pode perceber, subjacente às razões do veto está a concepção de que as normas de proteção de dados — ou, mais especificamente, determinadas obrigações de transparência estabelecidas pela LGPD — seriam incompatíveis com o exercício de atividades essenciais do poder público, como as de fiscalização, controle e polícia administrativa.

Na mesma ocasião, foram vetados três incisos do art. 52 que autorizavam a ANPD a aplicar as sanções de proibição e de suspensão da atividade de tratamento de dados, bem como a de suspensão parcial do funcionamento de banco de dados. Posteriormente, com a edição da Lei nº 13.853, de 8 de julho de 2019, essas sanções foram reincluídas na LGPD. Mais uma vez, no entanto, foram objeto de veto, que também excluiu da lei o § 3º do art. 52, dispositivo que autorizava a aplicação destas e de outras sanções ao poder público. As razões desse veto seguiram o mesmo padrão discursivo adotado no caso do art. 28 da LGPD. Nesse sentido, considerou-se que as normas em questão poderiam gerar "insegurança aos responsáveis por essas informações […],

[2] BRASIL. Presidência da República. *Mensagem de Veto nº 451, de 14 de agosto de 2018*. Disponível em: https://bit.ly/2N6fp0T. Acesso em: 14 out. 2022.

podendo acarretar prejuízos […] a entes públicos, com potencial de afetar a continuidade de serviços públicos".[3]

Portanto, de modo similar à proposta apresentada durante a tramitação da LGPD, os vetos mencionados também expressam a concepção de que a nova legislação de proteção de dados poderia "inviabilizar" ou "afetar a continuidade" da prestação de serviços públicos. Diante desses evidentes "prejuízos" e da correlata "insegurança jurídica" gerada, o melhor a fazer seria limitar, ainda que parcialmente, a incidência da lei sobre o setor público. Cumpre enfatizar que, apesar da justificativa apresentada nos vetos, os dispositivos em questão fortaleciam garantias essenciais para a proteção de direitos, seja ao impor a necessária transparência para as operações com dados pessoais realizadas por entidades e órgãos públicos, seja ao prever que, em caso de irregularidades, a ANPD poderia impor sanções aos agentes de tratamento responsáveis.

Em reação ao relativo fracasso dessas iniciativas, especialmente em face da derrubada do veto ao art. 52 pelo Congresso Nacional, com o consequente restabelecimento das sanções administrativas aplicáveis pela ANPD,[4] surgiu a estratégia de postergar a vigência da LGPD. A redação original da lei previa a sua entrada em vigor no prazo de 18 meses, isto é, em fevereiro de 2020. Porém, após a edição da Medida Provisória (MP) nº 869, de 27 de dezembro de 2018, convertida na citada Lei nº 13.853/2019, o prazo foi ampliado para 24 meses, ou seja, para agosto de 2020, salvo quanto aos dispositivos relativos à instalação e às competências da ANPD, cuja vigência foi antecipada para dezembro de 2018.

Durante a pandemia da Covid-19, a vigência dos principais dispositivos da LGPD foi mais uma vez postergada, desta feita para maio de 2021, conforme determinado pela MP nº 959, de 29 de abril de 2020. A justificativa apresentada foi a de "uma possível incapacidade de parcela da sociedade em razão dos impactos econômicos e sociais da crise provocada pela pandemia do Coronavírus".[5] Na mesma época, em uma iniciativa similar do Congresso Nacional, foi aprovada e sancionada a Lei nº 14.010, de 10 de junho de 2020, prorrogando para agosto de 2021 a vigência dos artigos 52 a 54 que tratam das

---

3 Presidência da República. *Mensagem de Veto nº 288, de 8 de julho de 2019*. Disponível em: https://bit.ly/2CkTYqE. Acesso em: 14 out. 2022.

4 URUPÁ, Marcos. Congresso derruba vetos na LGPD. *Teletime*, 25 set. 2019. Disponível em: https://bit.ly/3rXjlFy. Acesso em: 14 out. 2022.

5 BRASIL. Presidência da República. *Medida Provisória nº 959, de 29 de abril de 2020. Exposição de Motivos nº 00168/2020*. Disponível em: https://bit.ly/30RKHRb. Acesso em: 14 out. 2022.

sanções administrativas. Ao final, após sucessivas medidas de postergação, a LGPD, que havia sido aprovada em agosto de 2018, com previsão original de vigência a partir de fevereiro de 2020, somente entrou plenamente em vigor em agosto de 2021.

Embora muitas vezes apresentado como medida excepcional e temporária, necessária para conferir um período de adaptação às organizações públicas e privadas ou para mitigar os efeitos sociais e econômicos da pandemia, esse verdadeiro fatiamento da vigência da LGPD pode ser visto como um ponto de uma linha contínua, integrada, ainda, pela tentativa de excluir o poder público da incidência da lei e pelos vetos a dispositivos que previam obrigações de transparência e a aplicação de sanções a entidades e órgãos públicos. Em todos esses casos, há um padrão discursivo similar, que expressa uma concepção reativa às normas de proteção de dados e que será adotado em casos concretos envolvendo o tratamento de dados pessoais pelo poder público nos anos seguintes, conforme demonstrado nas próximas seções deste artigo.

Esse cenário é reforçado pela omissão do Poder Executivo e o correlato descumprimento dos dispositivos da LGPD, vigentes desde dezembro de 2018, que previam a aprovação da estrutura regimental e a instalação da ANPD. Além dos impactos negativos sobre a garantia do direito à proteção de dados, o atraso na instalação do órgão regulador, efetivada somente em novembro de 2020, com a nomeação de seu corpo diretivo, foi também apresentado, em um raciocínio circular, como razão para adiar a vigência da LGPD. Na prática, todos os cenários pareciam gerar insegurança jurídica, seja o de aplicação integral e imediata da lei, seja o de postergação da vigência de seus principais dispositivos.[6]

A esse respeito, é relevante mencionar que a postergação da vigência plena da LGPD por cerca de três anos não foi suficiente para que entidades e órgãos públicos federais implementassem medidas básicas exigidas pela nova

[6] Por exemplo, na justificativa do PL nº 1.027/2020, que propunha o adiamento da vigência dos principais dispositivos da LGPD para fevereiro de 2022, o senador Otto Alencar alegou que, "diante da não instalação da ANPD […] há, a bem da verdade, uma impossibilidade jurídica para que empresas e órgãos e entidades da Administração Pública se considerem *compliants* com a LGPD. Isto porque […] não há como uma entidade se adequar a uma lei não regulamentada. […] Vê-se que a atual conjuntura tem gerado grave insegurança jurídica, tanto para gestores públicos como para empresas privadas, os quais se veem obrigados a dispender recursos e esforços para se adequar a uma Lei carente de regulamentação". BRASIL. Senado Federal. *Projeto de Lei nº 1.027/2020*. Disponível em: https://bit.ly/2NfDoe1. Acesso em: 14 out. 2022.

lei. Conforme recente auditoria realizada pelo Tribunal de Contas da União (TCU), de um total de 382 organizações auditadas, 76,7% estão em um nível classificado como "inexpressivo" ou "inicial" de adequação à LGPD. Entre as demais, cerca de 20% estão no nível "intermediário" e somente 2,9% foram consideradas no nível "aprimorado".[7]

De forma mais específica, isso significa que, entre essas organizações, somente 14% identificaram os dados pessoais que são objeto de tratamento em seus processos internos, incluindo aqueles compartilhados com terceiros. Por sua vez, apenas 17% identificaram todos os processos de negócio que realizam tratamento de dados pessoais. Também é reduzido o percentual (11%) de organizações públicas que identificaram e documentaram as finalidades dos tratamentos de dados pessoais realizados. Da mesma forma, apesar de a maioria (69%) ter indicado encarregado, 82% das organizações não possuem um registro instituído para consolidar informações relacionadas com as características das atividades de tratamento de dados pessoais.[8]

Quanto às medidas de promoção da transparência e de garantia de direitos, o relator do acórdão, ministro Augusto Nardes, destacou o seguinte:

> Nesse particular, foi constatado que 75% das organizações ainda não elaboraram documentação relativa à política de privacidade, o que demonstra que não é dada a devida transparência ao titular de como os seus dados pessoais são tratados. Para os casos em que a organização informasse que possuía Política de Privacidade ou documento similar, era exibida a subquestão para verificar se o artefato estava publicado na internet. As respostas demostraram que a maioria das organizações não comunica, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais. Quanto aos mecanismos para atender os direitos dos titulares, uma vez que a organização deve implementá-los para atender aos nove direitos estabelecidos no art. 18 da LGPD, as respostas mostraram que somente 14% das organizações cumpriram a orientação para atender todos esses direitos elencados no art. 18 da LGPD.[9]

Como se pode verificar, há uma baixa implementação de medidas básicas visando à conformidade das organizações públicas federais com a legislação de proteção de dados pessoais. Muitas dessas organizações sequer realizaram o mapeamento de processos e a identificação de quais dados são tratados e

---

7 BRASIL. Tribunal de Contas da União. *Acórdão nº 13842/2022*. Relator ministro Augusto Nardes, TCU/Plenário, 21 jun. 2022, p. 83. Disponível em: https://bit.ly/3MyEYFv. Acesso em: 15 out. 2022.

8 Ibid., p. 84.

9 Ibid., p. 85.

para quais finalidades, o que indica que esses processos são desconhecidos ou são realizados de forma discricionária e desestruturada, isto é, sem a devida avaliação e motivação quanto à sua adequação à LGPD. Por sua vez, a opacidade das operações realizadas com dados pessoais é atestada pelo reduzido índice de organizações que elaboraram e publicaram política de privacidade ou que instituíram mecanismos para atender aos direitos dos titulares.

Em suma, as informações levantadas pelo TCU revelam a existência e o predomínio de uma postura reativa no setor público federal em face da implementação da LGPD, o que pode ter sido incentivado pelas sucessivas postergações de vigência da lei ou, ainda, pela concepção de que a legislação de proteção de dados pessoais representa um entrave à inovação e à eficiente execução de políticas e serviços públicos.

2. O uso discricionário de dados pessoais pelo poder público

No livro *A guerra do fim do mundo*, baseado nos fatos históricos da Guerra de Canudos (1896-1897), Mario Vargas Llosa relata como um grupo de sertanejos resistiu ao Exército brasileiro em finais do século XIX. Até que as tropas militares destruíssem completamente o local, o que somente ocorreu em sua quarta expedição a Canudos, no interior da Bahia, Antônio Conselheiro e seus seguidores mantiveram os seus ideais contrários a uma série de mudanças que se seguiram à Proclamação da República em 1889. Entre essas, a separação entre Igreja e Estado, o casamento civil, a secularização dos cemitérios e, mais importante para os fins deste trabalho, a realização de um novo censo populacional. À época, acreditava-se que os dados coletados pelo Estado seriam utilizados, em realidade, para fins discriminatórios, incluindo a perseguição religiosa e racial, esta com o fim de restabelecer a escravidão.[10]

[10] "Mas, sim, alguma coisa tinha mudado com a República. Para o mal e a confusão do mundo: a Igreja foi separada do Estado, estabeleceram-se a liberdade de cultos e a secularização dos cemitérios, que não seriam mais atribuição das paróquias e sim dos municípios. […] Assim como, sem dúvida, todas as outras disposições estranhas, suspeitas, de que ia tomando conhecimento nas vilas: o mapa estatístico, o censo, o sistema métrico decimal. Aos atônitos sertanejos que vinham lhe perguntar o que significava tudo aquilo, o Conselheiro explicava, devagar: queriam saber a cor das pessoas para restaurar a escravidão e devolver os negros aos seus amos, e a religião, para identificar os católicos quando começassem as perseguições. Sem levantar a voz, exortava o povo a não responder a tais questionários nem aceitar que o metro e o centímetro substituíssem a vara e o palmo." VARGAS LLOSA, Mario. *A guerra do fim do mundo*. Rio de Janeiro: Alfaguara, 2008. p. 33-34.

A desconfiança sobre a coleta de dados pelo Estado não foi um evento isolado ou exclusivo de Canudos. Cerca de 40 anos antes, em 1852, um levante popular em Pernambuco, conhecido como a Guerra dos Marimbondos, que se alastrou por outras províncias do Império, levou o governo a suspender a aplicação de uma lei que determinava a realização do censo e o estabelecimento do registro oficial de nascimentos e óbitos. Assim como Antônio Conselheiro, a população temia que as informações obtidas com base na nova legislação, que ficou conhecida como "Lei do Cativeiro", fossem utilizadas para identificar e escravizar os mais pobres.

A revolta levou ao adiamento do censo por cerca de 20 anos e do estabelecimento do registro público oficial por cerca de quatro décadas. Embora as autoridades garantissem que não havia qualquer ameaça à liberdade individual, Guillermo de Jesus Palacios y Olivares lembra que o receio de que os dados fossem utilizados para outros fins era generalizado, especialmente entre a população que "levava consigo o estigma da cor, habituada ao proverbial arbítrio de uma sociedade escravista".[11] Ainda segundo o autor:

> O *Registro* e a *Lei do Censo* dirigiam-se explicitamente a contar e descobrir o número dos livres e pobres, e com isso a fazê-los públicos e notórios perante a autoridade do Estado, com nome, endereço e situação familiar; além do mais, dificultava enormemente a transposição da barreira da escravidão, pois aperfeiçoava os mecanismos de identificação da condição jurídica desses setores da população, dentro dos quais escondiam-se muitos devedores da lei, fugitivos do cativeiro. […] Em termos da condição jurídica dos livres e pobres [o *Registro*] confirmava a liberdade dos que podiam comprovar essa abençoada condição, e ameaçava com reconduzir à escravidão os infelizes que não contassem com a documentação necessária para fundamentar sua independência pessoal.[12]

Esses eventos históricos demonstram que as controvérsias associadas ao tratamento de dados pessoais pelo poder público no Brasil vêm de longa data, sendo marcadas pela desconfiança quanto aos riscos de destinação dos dados pessoais para fins não declarados e não compatíveis com o ordenamento jurídico. Nesse sentido, deve-se considerar que o cidadão é o elo mais frágil e vulnerável na relação estabelecida com instituições públicas, uma vez que suas informações pessoais são coletadas de forma compulsória e, se não

---

[11] PALACIOS Y OLIVARES, Guillermo. Revoltas camponesas no Brasil escravista: a "Guerra dos Marimbondos" (Pernambuco, 1851-1852). *Almanack Braziliense*, n. 3, maio 2006, p. 30. Disponível em: https://bit.ly/3TG0Zow. Acesso em: 23 out. 2022.

[12] Ibid., p. 30.

adotadas as devidas salvaguardas, podem ser utilizadas para fins abusivos, associados a práticas de discriminação ou de vigilância.

A principal diferença dos dias atuais em relação ao século XIX é a de que os mecanismos de coleta de informações dos cidadãos pelo Estado estão muito bem estabelecidos e estruturados, envolvendo quantidades massivas de dados pessoais, muitas vezes armazenadas em formato digital e tratadas de forma automatizada. Essa ampliação da coleta de dados é fruto da própria alteração do papel do Estado, que, ao longo das últimas décadas, assumiu a função de formular políticas públicas e garantir direitos sociais, como os relacionados com a educação, a saúde e o trabalho. Nesse sentido, dados pessoais constituem um insumo relevante para ampliar a eficiência da ação estatal, por exemplo, por meio do compartilhamento de informações entre entidades e órgãos públicos ou, ainda, mediante a produção de evidências que embasam a formulação de políticas públicas. Como ressalta Miriam Wimmer:

> A questão sobre o quão bem o Estado deve conhecer seus cidadãos já foi enfrentada em variados contextos e em diferentes momentos históricos, tendo por pano de fundo o reconhecimento de que, ao mesmo tempo que o tratamento de dados pessoais pelo Estado é pré-requisito para o exercício da cidadania, a expansão da quantidade e da variedade de dados pessoais custodiados pelo Estado suscita riscos de violações de direitos. Dito de outro modo, a visibilidade do Estado sobre seus cidadãos permite ampliar a sua capacidade de intervenção, tenha ela por objetivo atingir finalidades sociais justas (*e.g.*, viabilizar a distribuição de benefícios sociais) ou nefastas.[13]

No contexto do século XXI, um dos elementos característicos dos processos de coleta massiva de dados pessoais é a geração de um "excedente comportamental", isto é, uma espécie de sobrevalor, que transcende os propósitos originais da operação de coleta.[14] Como consequência, mesmo após exauridos os seus objetivos iniciais, o uso de um conjunto de dados pessoais tende a permanecer atrativo e valioso para outras finalidades. Esse uso subsequente e contínuo dos dados pessoais permite gerar um valor adicional significativo — seja ele de ordem pública, política ou econômica — a um custo marginal reduzido, em particular diante da possibilidade de

---

[13] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: MENDES, L.; DONEDA, D.; SARLET, I.; RODRIGUES JR., O. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 273.

[14] ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. Nova York: Public Affairs, 2019. p. 74-75.

realização de novas inferências a partir de técnicas de análise de dados ou de simples agregação de novas informações, entre outras possibilidades, sempre visando ao controle, à previsão e ao direcionamento de comportamentos.[15]

Assim, por exemplo, informações de famílias de baixa renda que integram o Cadastro Único para Programas Sociais do Governo Federal (CadÚnico) podem ser utilizadas para formulação e gestão de políticas públicas as mais diversas (art. 13, Decreto nº 11.016, de 29 de março de 2022), como no caso da identificação de beneficiários do auxílio emergencial concedido durante a pandemia da Covid-19 (Lei nº 13.982, de 2 de abril de 2020). Embora a concessão deste benefício específico não integrasse o propósito original do CadÚnico, as informações nele constantes foram utilizadas legitimamente para subsidiar essa nova política pública.

Como demonstra esse exemplo trivial, no setor público, o tratamento de dados pessoais para propósitos distintos daqueles que justificaram a coleta inicial deve, entre outras condições, sempre atender a uma finalidade pública. A LGPD possui normas expressas nesse sentido, como o disposto no art. 26, de acordo com o qual o uso compartilhado de dados pessoais pelo poder público deve atender à "finalidade específica de execução de políticas públicas".

Muitas vezes, no entanto, a legitimidade do uso compartilhado de dados pessoais pelo poder público é controversa. Uma finalidade pública pode contrariar outra finalidade pública ou determinados direitos fundamentais. Dúvidas também podem surgir quanto aos limites aplicáveis às competências de uma autoridade para ter acesso ou realizar o tratamento de informações de natureza pessoal. A legislação pode não ser clara quanto a esses aspectos, as justificativas apresentadas podem ser frágeis ou, ainda, o risco de desvio de finalidade ou de ocorrência de impactos aos titulares pode ser elevado.

Diante de um conflito deste tipo, o STF se manifestou contrariamente ao compartilhamento de dados pessoais obtidos pelo Instituto Brasileiro de Geografia e Estatística (IBGE) e pelo Instituto Nacional de Estudos e Pesquisas

[15] A autora aponta o Google como o pioneiro na utilização desse excedente e, de forma mais ampla, na formação das estruturas essenciais do "capitalismo da vigilância". Nesse sentido, de início, os dados gerados pela atividade do buscador da empresa eram utilizados apenas para incrementar a qualidade do serviço. Com o passar do tempo, e em vista da necessidade de geração de receitas a seus acionistas, a empresa percebeu o valor decorrente dos dados coletados, passando a utilizá-los para um propósito distinto: a venda de anúncios personalizados. Nas palavras da autora, "esses dados comportamentais disponíveis para usos além da melhoria do serviço constituíam um excedente e foi com apoio nesse excedente comportamental que a então jovem companhia encontrou o caminho para a geração dos lucros exponenciais e sustentáveis para garantir a sua sobrevivência". Ibid., p. 74.

Educacionais Anísio Teixeira (Inep). Os dados em questão, que haviam sido coletados para fins estatísticos, seriam utilizados, respectivamente, para permitir que o Ministério Público Federal identificasse crianças não registradas na cidade de Bauru (SP) e que o TCU realizasse uma auditoria no Programa Bolsa Família. Ainda que, em ambos os casos, o compartilhamento de dados fosse destinado para atender a finalidades públicas, a Corte entendeu que, no caso concreto, deveria prevalecer o sigilo estatístico e a finalidade original da coleta, sob pena de violação à privacidade e à intimidade dos titulares. Ademais, caso realizado, o compartilhamento poria em risco a confiança depositada nos órgãos de pesquisa pelos entrevistados e a própria continuidade dessas atividades.[16]

O ponto central a ser considerado é que, movidas por razões legítimas ou não, autoridades públicas possuem incentivos estruturais para se apropriar dos benefícios e dos excedentes comportamentais gerados pelos diversos bancos de dados pessoais armazenados por instituições públicas ou privadas. Em razão disso, muitas vezes, essas mesmas autoridades passam a defender as suas prerrogativas de acesso a esses dados com base na existência de amplos poderes discricionários, isto é, um espaço livre de decisão, imune ao controle jurisdicional e legitimado apenas por conceitos jurídicos abstratos e genéricos, como o de finalidade pública e similares.[17]

A esse respeito, em maio de 2019, o Ministério da Educação solicitou ao Inep acesso à base de dados identificada do Censo da Educação Superior com o propósito de viabilizar a execução de uma nova política pública: a emissão de carteiras estudantis digitais. Críticos da medida apontaram a existência de riscos de vigilância sobre estudantes e de esvaziamento de entidades estudantis em um momento no qual ocorriam, em todo o país, protestos contra cortes orçamentários na educação. O Inep, por sua vez, refutou o compartilhamento dos dados, sob a alegação de sigilo estatístico, nos mesmos moldes da argumentação apresentada no caso julgado pelo STF mencionado anteriormente.[18]

---

16 BRASIL. Supremo Tribunal Federal. *Suspensão de Liminar nº 1.103*. Rel. min. Cármen Lúcia. 2 maio 2017; BRASIL. Supremo Tribunal Federal. *Mandado de Segurança nº 36.150*. Rel. min. Roberto Barroso. 10 dez. 2018.

17 Para uma crítica a essa concepção de discricionariedade administrativa, ver BINENBOJM, Gustavo. *Uma teoria do direito administrativo*: direitos fundamentais, democracia e constitucionalização. 2. ed. Rio de Janeiro: Renovar, 2008. p. 38-42.

18 MARIZ, Renata. MEC quer acessar dados sigilosos de alunos para emitir nova carteirinha estudantil. *O Globo*, 16 maio 2019. Disponível em: https://glo.bo/2H1Odgu. Acesso em: 18 out. 2022.

Diante do impasse, foi editada a MP nº 895, de 6 de setembro de 2019, que autorizava o MEC a emitir a carteira estudantil digital e lhe conferia ampla competência discricionária para coletar e compartilhar dados pessoais de estudantes e docentes, além de outras informações a serem definidas em ato administrativo. A única limitação prevista na norma era a de que o compartilhamento deveria atender à finalidade genérica de "formulação, implementação, execução, avaliação e monitoramento de políticas públicas, observadas as normas e os procedimentos específicos que garantam sua segurança, proteção e confidencialidade", nos termos do art. 1º-B, § 4º, Lei nº 12.933, de 26 de setembro de 2013, com redação dada pela MP nº 895/2019.

Por sua vez, a política de privacidade do aplicativo "ID Estudantil", por meio do qual foram disponibilizadas as carteirinhas digitais, previa que os dados coletados "são de propriedade do MEC".[19] De um lado, essa visão patrimonialista revela a incompreensão quanto à natureza jurídica das informações coletadas, que recaem sobre "aspectos indissociáveis de seu titular", conforme lembra Danilo Doneda,[20] não se constituindo, portanto, como um "bem" sujeito às restrições provenientes de um direito real de um terceiro. Por outro lado, expressa o entendimento de que o cidadão é um mero "fornecedor de dados",[21] sem qualquer poder de controle sobre o uso de suas

---

[19] BRASIL, Ministério da Educação. *Política de privacidade do aplicativo ID Estudantil*. 2020. Disponível em: https://bit.ly/38FDG80. Acesso em: 18 out. 2022. É comum programas e aplicativos governamentais não possuírem políticas de privacidade ou, no caso daqueles que a possuem, adotarem redações genéricas, conforme constatado por ABREU, Jacqueline; MASSARO, Heloisa; LAGO, Lucas. As políticas de privacidade de apps do governo. *InternetLab*, maio 2018. Disponível em: https://bit.ly/2ZtuQWE. Acesso em: 18 out. 2022; e MACHADO, Jorge; BIONI, Bruno. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do 'Nota Fiscal Paulista'. *Liinc em Revista*, Rio de Janeiro, v. 12, n. 2, p. 350-364, nov. 2016.

[20] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 84. O autor critica a posição doutrinária que sustenta a existência de "propriedade sobre os dados pessoais", haja vista "a multiplicidade de situações e interesses presentes em torno dos dados pessoais, que não se limitam a vetores patrimoniais e que seriam irremediavelmente prejudicados se considerados apenas – ou majoritariamente – a partir de seu valor econômico". Ibid., p. 146.

[21] Conforme Stefano Rodotà, "a nova situação determinada pelo uso de computadores no tratamento de informações pessoais torna cada vez mais difícil considerar o cidadão como um simples 'fornecedor de dados', sem que a ele caiba algum poder de controle. De fato, a obrigação de fornecer dados não pode ser simplesmente considerada como a contrapartida dos benefícios sociais que, direta ou indiretamente, o cidadão pode chegar e aproveitar. As informações coletadas não somente tornam as organizações públicas e privadas capazes de planejar e executar os seus programas, mas permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes: consequentemente, os cidadãos têm o direito de pretender exercer um controle direto sobre aqueles sujeitos aos quais as informações fornecidas atribuirão um crescente *plus-poder*". RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 36-37.

informações pessoais, haja vista as correlatas prerrogativas discricionárias atribuídas ao "proprietário" dos dados pessoais.

Mais uma vez, a própria política de privacidade divulgada pelo MEC confirma essa leitura. Com efeito, entre outras finalidades genéricas, os dados — os quais, vale enfatizar, foram originalmente coletados para a emissão de carteiras estudantis — também poderiam ser destinados "para outros objetivos da Administração Pública: auditorias, análises estatísticas, ciência de dados e estudos para lançamento de novos serviços públicos ou para a melhoria dos já existentes, bem como de processos e comunicações".[22] Na prática, tendo em vista a amplitude dos "objetivos da Administração Pública" citados, os dados dos estudantes poderiam ser compartilhados, de forma irrestrita e discricionária, com qualquer outro órgão público e destinados para quaisquer finalidades.

A MP nº 895/2019 caducou em fevereiro de 2019, em razão de sua não apreciação pelo Congresso Nacional. Não obstante, pouco mais de um ano depois, o governo federal recorreu a fundamentos jurídicos similares para editar a MP nº 954, de 17 de abril de 2020, que obrigava as prestadoras de serviços de telecomunicações a fornecer ao IBGE dados pessoais de todos os seus consumidores para fins de "produção estatística oficial". O compartilhamento de dados permitiria a realização de entrevistas não presenciais durante a vigência das restrições impostas pela pandemia da Covid-19.

Em que pese a inegável excepcionalidade da situação e a relevância de manutenção das pesquisas oficiais, a MP nº 954/2020 refletia, com algumas variações, a mesma concepção apresentada no caso das carteiras estudantis: o recurso a uma finalidade genérica, a falta de transparência quanto à motivação do ato e a atribuição de amplos poderes discricionários ao poder público para efetuar o tratamento de uma quantidade massiva de dados pessoais. Por essas e outras razões, a MP nº 954/2020 foi suspensa por medida cautelar proferida pela ministra Rosa Weber, do STF, em uma decisão na qual foi expressamente apontado que o ato normativo:

> Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados […]. Nessa linha, ao não definir propriamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da

[22] BRASIL, Ministério da Educação, *Política de privacidade do aplicativo ID Estudantil*, op. cit.

> sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.[23]

Ainda durante a pandemia do coronavírus e pouco mais de um mês após a decisão do STF, o *Intercept Brasil* revelou que o Departamento Nacional de Trânsito (Denatran) havia autorizado a Agência Brasileira de Inteligência (Abin) a ter acesso a dados pessoais sensíveis de 76 milhões de brasileiros que possuem Carteira Nacional de Habilitação. A obscura transação seria realizada para atender à finalidade genérica de assegurar o "funcionamento da atividade de inteligência".[24]

Em uma manifestação dirigida ao STF, no curso da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695, que questionava a operação, o advogado-geral da União defendeu a sua legalidade e aderência ao Decreto nº 10.046, de 9 de outubro de 2019, norma que possibilitaria "o compartilhamento mais fluido de dados entre órgãos e entidades da Administração Pública". Além disso, argumentou que "a atividade de inteligência é um tipo de política pública consolidada no ordenamento brasileiro", o que autorizaria o compartilhamento dos dados para atender a esta finalidade. Por tais razões, o mais adequado na hipótese seria uma "deferência pela escolha dos representantes eleitos", reconhecendo-se a aptidão do Poder Executivo para decidir sobre o assunto:

> Nessa linha, a estruturação pragmática do sistema de compartilhamento de dados entre os órgãos ou entidades da Administração Pública insere-se na esfera de atribuições do Poder Executivo, cabendo ao Judiciário respeitar o âmbito discricionário dos demais Poderes, sobretudo quando observadas as regras e princípios que conformam a atuação administrativa.[25]

---

[23] BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6387*. Rel. min. Rosa Weber. 24 abr. 2020. A medida cautelar foi referendada pelo Plenário do STF, por 10 votos a um, vencido o ministro Marco Aurélio, em sessão realizada no dia 7 de maio de 2020.

[24] DIAS, Tatiana; MARTINS, Rafael. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. *The Intercept*, 6 jun. 2020. Disponível em: https://bit.ly/2B6uSvy. Acesso em: 2 nov. 2022. Vale mencionar que a íntegra do Termo de Autorização nº 7/2020, firmado em março de 2020 entre as partes, não foi apresentada sequer ao STF. Por isso, o ministro Gilmar Mendes destacou o "caráter obscuro" da operação, ressaltando que, no extrato publicado no *Diário Oficial da União*, não constava "qualquer informação relevante nem sobre a natureza dos dados compartilhados tampouco acerca dos parâmetros objeto do compartilhamento". BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental nº 695*. Rel. min. Gilmar Mendes. 24 jun. 2020.

[25] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 695*. Manifestação do advogado-geral da União. 20 jun. 2020.

Embora a autorização para o compartilhamento de dados com a Abin tenha sido revogada pelo Denatran, o STF prosseguiu com o julgamento da ação. A decisão final foi proferida em setembro de 2022, em julgamento conjunto com a Ação Direta de Inconstitucionalidade (ADI) nº 6.649, que questionava a constitucionalidade, em abstrato, do Decreto nº 10.046/2019.

Em seu voto, o relator, ministro Gilmar Mendes, sustentou que o tratamento de dados pessoais pelo poder público deve observar três balizas constitucionais: (i) justificativa minudente e exaustiva das finalidades; (ii) limitação aos dados estritamente necessários para o alcance das finalidades, adotando-se as medidas de prevenção e segurança proporcionais aos riscos envolvidos no caso; e (iii) transparência e dever de publicidade sobre as informações relativas ao tratamento, garantindo-se ao titular nível de controle suficiente sobre a sua licitude.[26]

Assim, em um voto que foi referendado pelos demais membros do tribunal, o ministro Gilmar Mendes se posicionou contrariamente à concepção de que o tratamento de dados pode se dar de forma discricionária ou com ampla deferência às escolhas dos representantes eleitos. Isso porque o regime constitucional de tutela da privacidade "conduz ao abandono de qualquer interpretação que possibilite um amplo e irrestrito compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública Federal".[27]

Por fim, ressaltou que, não obstante a importância da utilização de novas tecnologias e de ferramentas digitais pelo poder público, a busca pela eficiência e pela instituição de melhores práticas gerenciais não pode servir de "manobra para o descumprimento do princípio da legalidade" nem constitui "um cheque em branco para o administrador público". Da mesma forma, não é "uma licença para o desatendimento dos preceitos éticos que informam o regime constitucional, entre eles os mecanismos de proteção de dados pessoais".[28]

Como se pode observar, as mais recentes decisões do STF estabeleceram parâmetros jurídicos objetivos e vinculantes, que limitam o campo de atuação discricionária de autoridades públicas. Em consonância com as disposições da LGPD, o tribunal deixou claro que o tratamento de dados pessoais pelo poder público pressupõe uma delimitação clara e precisa de sua fundamentação

---

[26] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 695*. Voto do relator, ministro Gilmar Mendes. 15 set. 2022. p. 27.

[27] Ibid., p. 43.

[28] Ibid., p. 51-52.

legal, do valor ou do benefício público gerado e da aderência da operação às competências legais dos órgãos e entidades envolvidos. Por isso, a finalidade deve ser, efetivamente, específica, o que demanda a indicação, também de forma clara e precisa, de qual iniciativa, ação ou projeto será viabilizado pelo uso dos dados.

Trata-se de um ônus argumentativo e de uma exigência de prestação de contas que devem ser assumidos pelos gestores públicos, afastando-se — por se reconhecer, de antemão, como ilegítima — qualquer hipótese de tratamento de dados pessoais sem motivação adequada e baseada apenas em fins genéricos, a exemplo de "formulação, execução e avaliação de políticas públicas", "produção estatística oficial" e "atividades de inteligência".

A proteção de dados pessoais constitui a base sobre a qual se erige a confiança pública nas instituições, conforme já se podia extrair dos eventos que deram causa à Guerra dos Marimbondos, em meados do século XIX. De modo similar, nos dias de hoje, a crescente oferta de serviços públicos digitais, que se pretendem mais simples, práticos e eficientes, somente é viável e sustentável se acompanhada de medidas que promovam a transparência e assegurem o controle dos titulares sobre os seus dados pessoais. Em última análise, e esse é o principal sentido das disposições estabelecidas pela LGPD e reafirmadas pelo STF, trata-se de estabelecer uma necessária barreira jurídica para evitar desvios de finalidade e conter os riscos de vigilância e de práticas discriminatórias.

3. A transparência e a dimensão política do direito à proteção de dados pessoais

De acordo com Norberto Bobbio, a democracia é o "regime do poder visível" ou, ainda, o "governo do poder público em público".[29] Essa definição assume que o princípio da transparência é a base da democracia, de modo que a visibilidade das ações dos governantes constitui um pressuposto necessário para o exercício do controle dessas mesmas ações pelos cidadãos.

Por isso, uma das principais ameaças à realização dos ideais democráticos vem da persistência do recurso ao segredo como prática administrativa. Essa prática daria azo ao chamado "poder invisível", que ganha espaço para se

[29] BOBBIO, Norberto. *O futuro da democracia*. São Paulo: Paz e Terra, 2000. p. 98.

desenvolver pela ação dos serviços secretos, por relações obscuras estabelecidas entre autoridades e grandes grupos econômicos e, principalmente, pela vigilância crescente sobre os cidadãos, possibilitada pelos meios técnicos de controle da informação e da comunicação.

Quanto a este último aspecto, Bobbio apontava, ao final do século XX, a existência de fortes riscos de as novas tecnologias serem utilizadas para uma espécie de inversão da equação democrática, consistente na ampliação dos mecanismos de controle dos indivíduos pelo Estado. Em suas palavras:

> E por que o mesmo uso dos computadores não poderia tornar possível um conhecimento capilar dos cidadãos de um grande Estado por parte de quem detém o poder? […] Se esta perspectiva é apenas um pesadelo ou um destino ninguém está em condições de prever. Seria de todo modo uma tendência oposta à que deu vida ao ideal de democracia como ideal do poder visível: a tendência não mais rumo ao máximo controle do poder por parte dos cidadãos, mas, rumo ao máximo controle dos súditos por parte de quem detém o poder.[30]

Nos dias de hoje, de fato, os riscos de controle e de vigilância dos cidadãos por parte das instituições estatais foram ampliados em razão do intenso processo de transformação digital verificado nas últimas décadas e que atinge todos os setores sociais e econômicos. Entre outros fatores, a transformação digital foi impulsionada pela disseminação do acesso à internet, pela proliferação de dispositivos eletrônicos portáteis e pelo uso crescente de algoritmos e sistemas de inteligência artificial, como os que permitem o reconhecimento de uma pessoa com base em seus dados biométricos.

No setor público, entre outras inovações, o processo de digitalização permite que informações que, há algumas décadas, estavam registradas apenas de forma analógica, muitas vezes impressas em documentos arquivados em armários nas diversas repartições públicas, possam ser armazenadas em formato digital, em computadores com alta capacidade de processamento. Com isso, é possível não somente ampliar e acelerar a coleta de informações pessoais, como também inferir novas informações ou realizar o cruzamento entre as diversas bases de dados, destinando-as para múltiplas finalidades, em particular mediante o seu uso compartilhado com outros órgãos públicos e entidades privadas.

---

[30] Ibid., p. 120.

Nessa linha, estudo realizado pela Organização para Cooperação e Desenvolvimento Econômico (OCDE) destaca que a capacidade de facilmente referenciar e reciclar dados armazenados é um dos fatores que impulsionaram a transformação digital. Com efeito,

> A digitalização aumenta o uso e o valor das informações passadas, tornando-as mais acessíveis, úteis e reutilizáveis. A digitalização tornou o texto pesquisável, compressível, facilmente manipulável e vinculável [a outras informações], e permite que os produtos do passado sejam preservados, analisados, indexados, reaproveitados, reinterpretados e revendidos. […] A capacidade tecnológica de preservar e usar informações passadas e combiná-las com novas informações continua a sustentar uma rápida expansão da economia digital.[31]

Como mencionado anteriormente, esse processo de inovação é fundamental para ampliar a eficiência da atuação do Estado. Ao mesmo tempo, ampliam-se os riscos de abusos e de violação a direitos dos titulares, que podem decorrer do mau uso de seus dados pessoais. Nesse contexto, para além de assegurar um espaço privado, alheio à interferência de terceiros, o direito à proteção de dados pessoais assume uma dimensão essencialmente política, vinculada ao controle do titular sobre o fluxo de suas informações na sociedade[32] e, mais especificamente, ao efetivo controle democrático de autoridades públicas pelos cidadãos.

É esse o principal direcionamento conferido pela LGPD ao regulamentar o tratamento de dados pessoais pelas instituições públicas. Nesse sentido, a lei expressamente determina que entidades e órgãos públicos sejam transparentes quanto às operações realizadas com dados pessoais. Por um lado, conforme o art. 23, I, é necessária uma atuação proativa, mediante a divulgação

---

[31] ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Vectors of digital transformation*. OECD Digital Economy Papers, n. 273, jan. 2019. p. 15. Disponível em: https://bit.ly/3fDfbQx. Acesso em: 6 nov. 2022.

[32] De acordo com Stefano Rodotà, "na sociedade da informação, tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. Assim a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações". Stefano Rodotà, *A vida na sociedade da vigilância*, op. cit., p. 92. Na mesma linha, Laura Schertel Mendes argumenta que o direito à proteção de dados pode ser concebido em uma dupla dimensão, que consiste, ao mesmo tempo: "(i) na proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e (ii) na atribuição ao indivíduo da garantia de controlar o fluxo de seus dados na sociedade". MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 176.

de "informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos". Por outro lado, sempre que solicitadas pelos titulares, entidades e órgãos públicos devem fornecer informações sobre o tratamento de seus dados pessoais e adotar as providências cabíveis, na forma do art. 18 da LGPD.

Como demonstrado, essas obrigações de transparência encontraram forte resistência no setor público. Assim, por exemplo, o veto ao art. 28 da LGPD foi justificado sob o argumento de que a "publicidade irrestrita" prevista na norma poderia inviabilizar atividades essenciais do poder público. Da mesma forma, auditoria realizada pelo TCU identificou um alto índice de organizações públicas que não possuem política de privacidade e não estão preparadas para atender às solicitações dos titulares de dados.[33]

Aliado a isso, e apesar de seu estreito vínculo com o princípio da transparência, a LGPD vem sendo interpretada no sentido oposto, isto é, como uma lei que fortalece e amplia o sigilo das práticas administrativas. É o que se verifica em alguns casos recentes, nos quais a nova legislação de proteção de dados pessoais foi utilizada como justificativa por autoridades públicas para negar o acesso a determinadas informações, muitas de evidente interesse público, como o registro de visitantes do Palácio do Planalto e os comprovantes de pagamento de verbas indenizatórias a servidores públicos.[34]

É certo que a LGPD demanda de entidades e órgãos públicos, conforme a orientação da ANPD, "uma posição de cautela e de análise de riscos a respeito da divulgação de informações pessoais".[35] Não obstante, isso não implica confundir ou limitar a proteção de dados pessoais à atribuição ampla e irrestrita de sigilo às informações pessoais coletadas pelo Estado.

Conforme previsto na LAI (art. 31, § 3º, V), informações pessoais podem ser divulgadas, entre outras hipóteses, sempre que necessário "à proteção do interesse público geral e preponderante". Nessa linha, o STF decidiu que as informações relativas à remuneração de servidores públicos são de interesse coletivo e geral, de modo que podem ser legitimamente divulgadas por órgãos

---

33 Cf. a Seção 2 anterior, "Vetos e vigência da LGPD".

34 ARCOVERDE, Léo; RAMOS, Maria Vitória; ZANATTA, Rafael. Transparência sob ataque. *Folha de S.Paulo*, 4 nov. 2021. Disponível em: https://bit.ly/3Nwy6ci. Acesso em: 2 nov. 2022.

35 BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Tratamento de dados pessoais pelo poder público (guia orientativo)*. Brasília: jan. 2022. Disponível em: https://bit.ly/3gXPEBR. Acesso em: 2 nov. 2022.

e entidades públicos, especialmente a fim de viabilizar o exercício do controle social da atuação do Estado.[36]

De forma similar, em resposta a consulta formulada pelo Ministério do Trabalho e Previdência, a ANPD se manifestou pela possibilidade de divulgação das listas de beneficiários de auxílios pagos a taxistas e transportadores autônomos de carga. Na ocasião, a ANPD considerou que a divulgação desses dados pessoais, por estar associada à execução de uma política pública específica, "está de acordo com a persecução do interesse público, mencionada no art. 23 da LGPD", com a ressalva de que deve se limitar aos "dados necessários para cumprir o princípio da publicidade e o disposto na LAI", além de ser informado aos beneficiários, em atenção ao princípio da transparência, que "seus nomes serão divulgados".[37]

Em outro caso, a ANPD sustentou que "a LGPD não estabeleceu a anonimização como condição técnica para a divulgação pública […] de dados pessoais por entidades e órgãos públicos". Assim, ainda que ocorra a "eventual identificação dos titulares" ou se verificado "algum grau de risco de sua identificação", a LGPD admite a divulgação de dados pessoais "quando necessário para atender, por exemplo, determinações legais, o interesse público e o direito de acesso à informação […], desde que adotadas as salvaguardas apropriadas".[38]

Desse modo, não obstante o sigilo ser medida protetiva necessária em determinadas circunstâncias, principalmente quando assim determinado por lei ou em face de dados sensíveis, como os referentes à saúde, pode-se afirmar que as autoridades públicas possuem um duplo dever de publicidade em relação às operações realizadas com dados pessoais.

Primeiro, o de divulgar ativamente as informações relativas aos tratamentos de dados realizados e o de atender às solicitações apresentadas pelos

---

[36] BRASIL. Supremo Tribunal Federal. *Suspensão de Liminar nº 623*. Rel. min. Ayres Britto. 10 jul. 2012.

[37] BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Nota Técnica nº 92/2022/CGF/ANPD*. Disponível em: https://bit.ly/3DDNpeV. Acesso em: 3 nov. 2022.

[38] No caso em questão, o Inep havia suspendido a divulgação de determinadas informações dos censos educacionais que eram tradicionalmente divulgadas na internet. Tais medidas restritivas foram adotadas com base em estudo técnico, segundo o qual haveria o risco de identificação dos titulares dos dados, apesar dos meios técnicos utilizados para proteger a sua identidade e assegurar o sigilo estatístico. BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Nota Técnica nº 46/2022/CGF/ANPD*. Disponível em: https://bit.ly/3WN8ivW. Acesso em: 29 dez. 2022. Em sentido similar à manifestação da ANPD, ver BRASIL. Controladoria-Geral da União. *Nota Técnica nº 1136/2022/CGAT/DTC/STPC*. Disponível em: https://bit.ly/3Q46dJR. Acesso em: 29 dez. 2022.

titulares. Neste caso, a transparência é um pressuposto necessário e direto para a prestação de contas à sociedade e para que os titulares possam exercer o controle sobre o fluxo de seus dados pessoais no âmbito do setor público. Em segundo lugar, há o dever de, em determinadas circunstâncias, divulgar dados pessoais, observadas as cautelas e restrições aplicáveis, sempre que essa medida for necessária para o atendimento a interesse público geral e preponderante e para assegurar o direito de acesso à informação. Neste caso, a transparência se vincula, de forma mais ampla, ao exercício do controle democrático sobre a atuação das instituições e das autoridades administrativas competentes, uma garantia que também é promovida pela LGPD e compatível com o direito à proteção de dados pessoais.

Importante mencionar que essa leitura encontra amparo na decisão proferida pelo STF no julgamento da ADPF nº 695 e da ADI nº 6.649. Nos termos do voto do ministro relator, o princípio da transparência impõe à administração pública a obrigação de assegurar ao titular um "nível de controle suficiente para a verificação prospectiva da licitude do tratamento de dados". De forma mais específica, essa garantia se desdobra em um "dever de publicidade que seja capaz de fornecer condições mínimas de proceder a um controle da forma como o Estado lida com dados pessoais". Ademais, a vinculação desse dever de publicidade a princípios da administração pública e a direitos fundamentais implica que eventual transgressão dolosa "importará a responsabilização do agente estatal por ato de improbidade administrativa".[39]

Na mesma decisão, o STF declarou inconstitucional a composição do Comitê Central de Governança de Dados (CCGD), órgão instituído pelo Decreto nº 10.046/2019, com competência para estabelecer orientações e parâmetros para o compartilhamento de dados pessoais no âmbito da administração pública federal. Conforme o voto do relator, a tutela efetiva do direito à privacidade demanda que as instituições competentes sejam formadas "a partir de uma composição plural e democrática, aberta, em alguma medida, a constante diálogo com a sociedade civil".[40] A composição do CCGD não atendia a essa exigência, uma vez que o órgão era formado apenas por representantes do Poder Executivo, sem independência ou

[39] BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Voto do relator, ministro Gilmar Mendes. 15 set. 2022, p. 27 e 69.

[40] Ibid., p. 61.

garantias contra influências indevidas. O órgão possuía, portanto, um "perfil insular, hostil a qualquer proposta de abertura democrática e de pluralização do debate", o que poderia acarretar "um autêntico desmonte dos pilares estruturantes da LGPD".[41]

Diante desse cenário, conclui-se que, apesar de usualmente a privacidade ser identificada com a noção de sigilo, contrapondo-se ao princípio da publicidade, a proteção de dados pessoais, na forma estabelecida pela LGPD e ratificada pelo STF, está mais relacionada com a ideia de controle do titular sobre o uso de suas informações e, de forma mais geral, sobre a atuação de autoridades e instituições públicas. Não por outro motivo, a LGPD não revogou ou alterou a LAI nem estabeleceu qualquer regramento sobre a atribuição de sigilo a informações pessoais detidas pelo Estado. Assim, os dispositivos legais que tratam do direito de acesso à informação e do direito à proteção de dados são "sistematicamente compatíveis entre si", de modo que não há que se falar em antinomia entre essas normas.[42]

Esse é um ponto fundamental, especialmente no âmbito do setor público, pois os dados pessoais constituem uma fonte de poder, no sentido de que, quanto mais conhecimento alguém ou uma instituição detém sobre uma pessoa, mais poder exercerá sobre ela. Como aponta Carissa Véliz, "a privacidade importa porque a sua falta confere poder aos outros sobre você".[43] No mesmo sentido, Daniel Solove argumenta:

> A privacidade é um limite ao poder do governo e das empresas. Quando se trata de dados pessoais, conhecimento é poder. Dados pessoais estão envolvidos em muitas decisões importantes sobre a vida das pessoas. Dados pessoais podem

---

41 Ibid., p. 62. Em atendimento à decisão do STF, o presidente da República editou o Decreto nº 11.266, de 25 de novembro de 2022, que deu nova redação ao Decreto nº 10.046/2019, para incluir, entre os membros do CCGD, dois representantes de "organizações da sociedade com atuação comprovada na temática de proteção de dados pessoais" (art. 22, IX). Também foi estabelecida a possibilidade de participação no CCGD de representantes do Conselho Nacional de Justiça, do Senado Federal e da Câmara dos Deputados, na qualidade de membros convidados (art. 22, § 4º).

42 Conforme o Enunciado nº 4, de 10 de março de 2022, da Controladoria-Geral da União: "a LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais — LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos". BRASIL. Controladoria-Geral da União. *Enunciado nº 4, de 10 de março de 2022*. Disponível em: https://bit.ly/3NwDkEW. Acesso em: 3 nov. 2022.

43 VÉLIZ, Carissa. *Privacy is power*: why and how you should take back control of your data. Londres: Corgi Books, 2021. p. 56.

> ser usados prontamente para afetar reputações, moldar a tomada de decisões e influenciar o comportamento. Nas mãos erradas, dados pessoais podem ser usados para causar danos graves às pessoas.[44]

Assim, reconhecer a existência de uma dimensão política do direito à proteção de dados pessoais implica conceber a privacidade para além da dimensão binária sigilo-publicidade, refutando-se interpretações simplórias da LGPD, que a utilizam, de forma indevida, como fundamento para atribuir sigilo irrestrito a informações de evidente interesse público. Como destaca Stefano Rodotà:

> Este conjunto de indicações obrigam-nos a uma revisão dos esquemas comumente adotados em matéria de privacidade; e faz com que nos deparemos com alguns paradoxos. O primeiro deles decorre do fato de que a ampliação da tutela da esfera privada dos sujeitos cujas informações são coletadas, graças à atribuição a eles de poderes diretos de controle, determinou uma maior transparência da esfera dos coletores de informações, sejam aparatos públicos ou organizações privadas. As regras sobre a privacidade, concebidas para assegurar opacidade e segredo à esfera individual, tornam-se o meio para uma transparência social mais acentuada.[45]

Em suma, embora a atribuição de sigilo a dados pessoais seja necessária em determinadas circunstâncias, o direito à proteção de dados se constitui como uma barreira jurídica ao poder exercido por autoridades e instituições públicas. Trata-se, por outras palavras, de uma garantia que promove o controle do titular sobre o fluxo de suas informações pessoais, impondo a entidades e órgãos públicos um dever de publicidade, que assegure a existência de mecanismos de participação e prestação de contas, responsivos aos interesses dos cidadãos e de organizações da sociedade civil.

Reafirma-se, dessa forma, a existência de uma conexão intrínseca entre a proteção de dados pessoais, a transparência e o exercício das liberdades políticas. Afinal, como bem ressalta Neil Richards, não há democracia funcional sem privacidade e proteção de dados pessoais, uma vez que esses direitos constituem "uma fonte essencial de poder político para os cidadãos em face do Estado", que "impulsiona o desenvolvimento de ideias e expressões políticas" e lhes "permite agir como cidadãos autônomos".[46]

---

[44] SOLOVE, Daniel. The myth of the privacy paradox. *The George Washington Law Review*, v. 89, n. 1, jan. 2021. p. 38. Disponível em: https://bit.ly/3FMNCyR. Acesso em: 5 nov. 2022.

[45] Stefano Rodotà, *A vida na sociedade da vigilância*, op. cit., p. 129.

[46] RICHARDS, Neil. *Why privacy matters*. Nova York: Oxford University Press, 2022. p. 132.

Conclusão

No Brasil, o tratamento de dados pessoais pelo poder público se baseou, tradicionalmente, em duas bem conhecidas práticas administrativas. De um lado, o recurso a prerrogativas discricionárias, imunes ao controle social e jurisdicional, permitia que autoridades e instituições públicas lidassem com dados pessoais, coletados de forma compulsória dos cidadãos, com ampla margem decisória, como se esses mesmos dados fossem uma espécie de "bem", cujo "proprietário" era o Estado. De outro lado, a amplitude dessas prerrogativas era reforçada pela opacidade das operações realizadas com dados pessoais e pela ausência de mecanismos efetivos de participação e prestação de contas à sociedade.

Com o advento da LGPD, essas duas práticas administrativas foram postas em xeque. Contrapondo-se à discricionariedade administrativa, a nova lei passou a exigir uma motivação minudente das operações realizadas com dados pessoais, as quais devem se amparar em uma hipótese legal, estar vinculadas a finalidades específicas e se limitar aos dados estritamente necessários para alcançar essas finalidades, além de observar outros princípios e regras previstos na norma. Como contraponto à opacidade e à cultura do sigilo, a LGPD se somou à LAI para exigir maior transparência e a instituição de mecanismos de atendimento às solicitações de titulares de dados.

A resistência a essas regras surgiu ainda durante a tramitação da LGPD no Congresso Nacional, ocasião na qual a legislação de proteção de dados foi apontada como um obstáculo à eficiência, à inovação e à regular prestação de serviços públicos. Com algumas variações, argumentos similares foram utilizados para justificar vetos a dispositivos da LGPD e para postergar, por mais de uma vez, a sua vigência. Da mesma forma, finalidades genéricas, acompanhadas de medidas pouco transparentes e sem motivação adequada, serviram de fundamento para iniciativas controversas, tais como a emissão de carteiras estudantis digitais, o compartilhamento de dados de prestadoras de serviços de telecomunicações com o IBGE e a disponibilização de dados de motoristas para atender às "atividades de inteligência" da Abin.

Conforme demonstrado ao longo deste trabalho, esses argumentos foram expressamente rechaçados por decisões recentes do STF. A Corte Constitucional reconheceu que o direito à proteção de dados pessoais impõe limites à atuação de autoridades e instituições públicas, nos termos da LGPD. Ao garantir ao titular o controle sobre o fluxo de suas informações na sociedade, o direito à proteção de dados pessoais assume uma relevante dimensão

política, associada ao controle democrático de autoridades e instituições públicas. Assim, a fim de conter os riscos de desvios de finalidade, a busca pela eficiência e pela inovação no setor público deve ser compatibilizada com as garantias de transparência, participação da sociedade civil, definição de finalidades específicas e motivação de decisões administrativas.

Apesar da relevância dos parâmetros jurídicos estabelecidos, é preciso reconhecer que as decisões do STF constituem apenas um primeiro passo de um longo caminho a ser percorrido com vistas ao estabelecimento de uma cultura da proteção de dados no setor público. É certo que o futuro passa pela digitalização de serviços, pela contínua inovação e pela busca de maior eficiência das ações estatais. Mas é certo também que esses novos desafios não podem ser utilizados como pretexto para sustentar velhas práticas administrativas. Afinal, cada vez mais, a confiança dos cidadãos nas instituições públicas pressupõe a efetiva proteção de seus dados pessoais.

Referências

ABREU, Jacqueline; MASSARO, Heloisa; LAGO, Lucas. As políticas de privacidade de apps do governo. *InternetLab*, maio, 2018. Disponível em: https://bit.ly/2ZtuQWE. Acesso em: 18 out. 2022.

ARCOVERDE, Léo; RAMOS, Maria Vitória; ZANATTA, Rafael. Transparência sob ataque. *Folha de S.Paulo*, 4 nov. 2021. Disponível em: https://bit.ly/3Nwy6ci. Acesso em: 2 nov. 2022.

BINENBOJM, Gustavo. *Uma teoria do direito administrativo*: direitos fundamentais, democracia e constitucionalização. 2. ed. Rio de Janeiro: Renovar, 2008.

BOBBIO, Norberto. *O futuro da democracia*. São Paulo: Paz e Terra, 2000.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Tratamento de dados pessoais pelo poder público (guia orientativo)*. Brasília: jan. 2022. Disponível em: https://bit.ly/3gXPEBR. Acesso em: 2 nov. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Nota Técnica nº 46/2022/CGF/ANPD*. Disponível em: https://bit.ly/3WN8ivW. Acesso em: 29 dez. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Nota Técnica nº 92/2022/CGF/ANPD*. Disponível em: https://bit.ly/3DDNpeV. Acesso em: 3 nov. 2022.

BRASIL. Controladoria-Geral da União. *Enunciado nº 4, de 10 de março de 2022*. Disponível em: https://bit.ly/3NwDkEW. Acesso em: 3 nov. 2022.

BRASIL. Controladoria-Geral da União. *Nota Técnica nº 1136/2022/CGAT/DTC/STPC*. Disponível em: https://bit.ly/3Q46dJR. Acesso em: 29 dez. 2022.

BRASIL. Ministério da Educação. *Política de privacidade do aplicativo ID Estudantil*. 2020. Disponível em: https://bit.ly/38FDG80. Acesso em: 18 out. 2022.

BRASIL. Presidência da República. *Mensagem de Veto nº 451, de 14 de agosto de 2018*. Disponível em: https://bit.ly/2N6fp0T. Acesso em: 14 out. 2022.

BRASIL. Presidência da República. *Mensagem de Veto nº 288, de 8 de julho de 2019*. Disponível em: https://bit.ly/2CkTYqE. Acesso em: 14 out. 2022.

BRASIL. Presidência da República. *Medida Provisória nº 959, de 29 de abril de 2020*. Exposição de Motivos nº 00168/2020. Disponível em: https://bit.ly/30RKHRb. Acesso em: 14 out. 2022.

BRASIL. Senado Federal. *Projeto de Lei nº 1.027/2020*. Disponível em: https://bit.ly/2NfDoe1. Acesso em: 14 out. 2022.

BRASIL. Supremo Tribunal Federal. *Suspensão de Liminar nº 623*. Rel. min. Ayres Britto. 10 jul. 2012.

BRASIL. Supremo Tribunal Federal. *Suspensão de Liminar nº 1.103*. Rel. min. Cármen Lúcia. 2 maio 2017.

BRASIL. Supremo Tribunal Federal. Mandado de Segurança nº 36.150. Rel. min. Roberto Barroso. 10 dez. 2018.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387. Rel. min. Rosa Weber. 24 abr. 2020.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Manifestação do advogado-geral da União. 20 jun. 2020.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental nº 695. Rel. min. Gilmar Mendes. 24 jun. 2020.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 695. Voto do relator, Ministro Gilmar Mendes. 15 set. 2022.

BRASIL. Tribunal de Contas da União. Acórdão nº 13842/2022. Relator ministro Augusto Nardes, TCU/Plenário, 21 jun. 2022. Disponível em: https://bit.ly/3MyEYFv. Acesso em: 15 out. 2022.

DIAS, Tatiana; MARTINS, Rafael. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. *The Intercept*, 6 jun. 2020. Disponível em: https://bit.ly/2B6uSvy. Acesso em: 2 nov. 2022.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

LEMOS, Ronaldo. Privacidade vale também para governo. *Folha de S.Paulo*, 16 abr. 2018. Disponível em: https://bit.ly/2NcpvwV. Acesso em: 14 out. 2022.

MACHADO, Jorge; BIONI, Bruno. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do 'Nota Fiscal Paulista'. *Liinc em Revista*, Rio de Janeiro, v. 12, n. 2, p. 350-364, nov. 2016.

MARIZ, Renata. MEC quer acessar dados sigilosos de alunos para emitir nova carteirinha estudantil. *O Globo*, 16 maio 2019. Disponível em: https://glo.bo/2H1Odgu. Acesso em: 18 out. 2022.

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

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Vectors of digital transformation.* OECD Digital Economy Papers, n. 273, jan. 2019. Disponível em: https://bit.ly/3fDfbQx. Acesso em: 6 nov. 2022.

PALACIOS Y OLIVARES, Guillermo. Revoltas camponesas no Brasil escravista: a "Guerra dos Marimbondos" (Pernambuco, 1851-1852). *Almanack Braziliense*, n. 3, p. 9-39, maio 2006. Disponível em: https://bit.ly/3TG0Zow. Acesso em: 23 out. 2022.

RICHARDS, Neil. *Why privacy matters*. Nova York: Oxford University Press, 2022.

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

SOLOVE, Daniel. The myth of the privacy paradox. *The George Washington Law Review*, v. 89, n. 1, p. 1-51, jan. 2021. Disponível em: https://bit.ly/3FMNCyR. Acesso em: 5 nov. 2022.

SOPRANA, Paula. Governo quer lei de proteção de dados que tira responsabilidade do Poder Público. *O Globo*, 11 abr. 2018. Disponível em: https://glo.bo/3d75ym1. Acesso em: 14 out. 2022.

URUPÁ, Marcos. Congresso derruba vetos na LGPD. *Teletime*, 25 set. 2019. Disponível em: https://bit.ly/3rXjlFy. Acesso em: 14 out. 2022.

VARGAS LLOSA, Mario. *A guerra do fim do mundo*. Rio de Janeiro: Alfaguara, 2008.

VÉLIZ, Carissa. *Privacy is power*: why and how you should take back control of your data. Londres: Corgi Books, 2021.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, L.; DONEDA, D.; SARLET, I.; RODRIGUES JR., O. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 271-288.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. Nova York: Public Affairs, 2019.