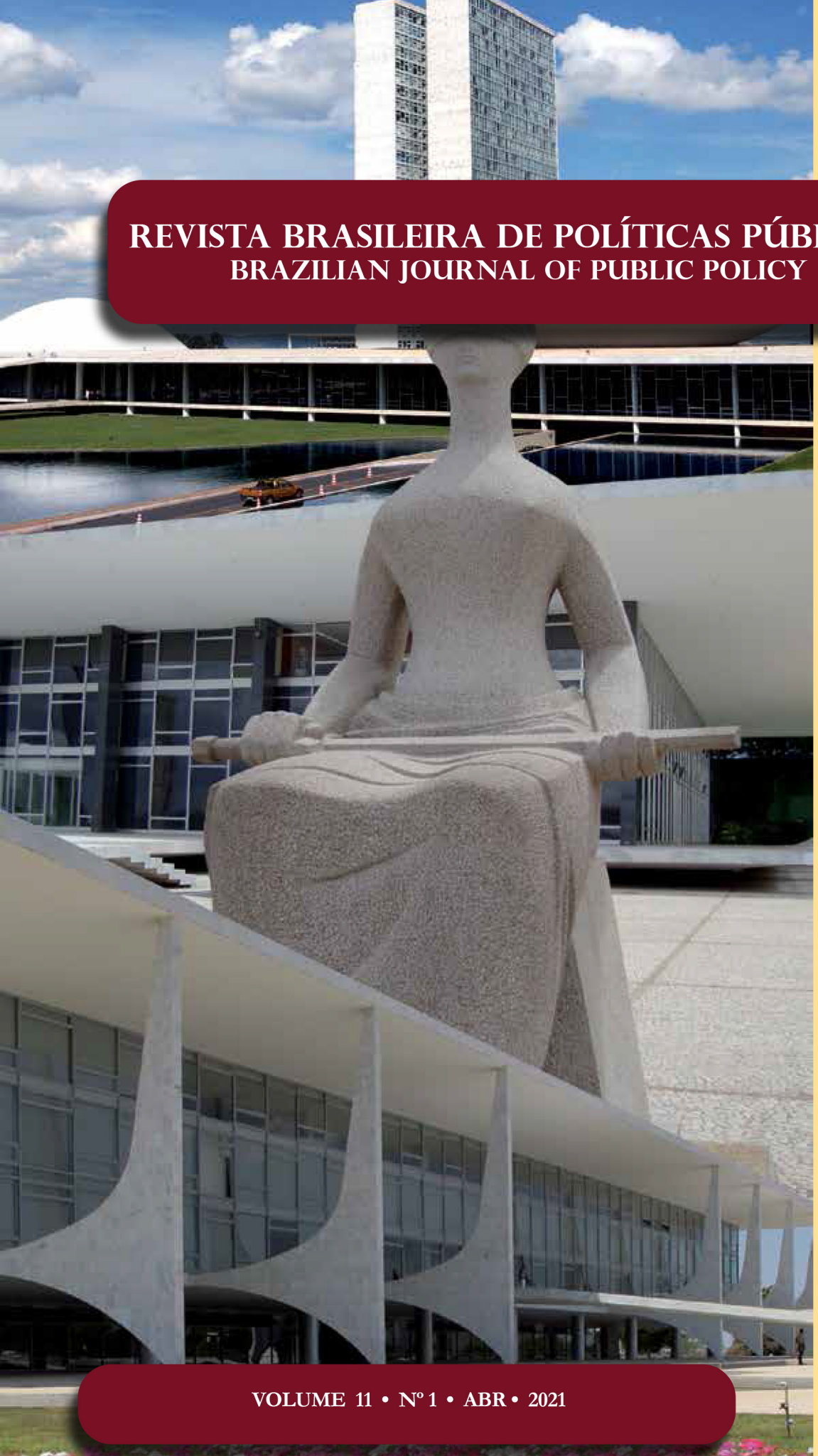

UniCEUB
ISSN 2236-1677

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS
BRAZILIAN JOURNAL OF PUBLIC POLICY

Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia

Limits and possibilities regarding the secondary use of personal data in the public sector: lessons from the pandemic

Miriam Wimmer

VOLUME 11 • Nº 1 • ABR • 2021

Sumário

doi: 10.5102/rbpp.v11i1.7136

Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia

Limits and possibilities regarding the secondary use of personal data in the public sector: lessons from the pandemic

Miriam Wimmer**

Resumo

A partir do contexto de intensificação da coleta, do processamento e da circulação de dados pessoais decorrente da pandemia de Covid-19, o artigo tem por objetivo discutir parâmetros para o compartilhamento e uso secundário de dados pessoais no âmbito do Estado. A ausência de detalhamento da LGPD e a escassa produção acadêmica brasileira sobre o uso secundário de dados pessoais no poder público justificam a relevância da temática escolhida. Assim, a partir de pesquisa bibliográfica e documental, e tendo como referência as críticas à ideia do Estado como unidade informacional, o artigo problematiza os riscos e benefícios do uso secundário de dados pessoais no âmbito do poder público e analisa como as recentes decisões do STF sobre o tema propiciaram a fixação de um importante paradigma para o debate brasileiro acerca do tema: o de que não há uma autorização irrestrita, no ordenamento jurídico brasileiro, ao livre fluxo e compartilhamento de dados no âmbito do Poder Público. Por fim, o artigo analisa em que medida elementos como a compatibilidade de finalidades, o consentimento do titular e a previsão legal poderiam balizar com maior legitimidade o compartilhamento de dados entre órgãos e entidades governamentais.

Palavras-chave: Proteção de dados pessoais. Compartilhamento de dados. Uso secundário. Poder público. Princípio da finalidade.

Abstract

In the context of increased collection, processing and sharing of personal data as a result of the Covid-19 pandemic, the article aims to discuss parameters for data sharing and secondary uses of personal data within the public sector. Based on bibliographic and documentary research, and taking into account the idea that government should not be treated as a single information unit, the article considers the risks and benefits of secondary use of personal data in government and analyzes how recent decisions by the Brazilian Supreme Court have established an important paradigm for the domestic debate on this issue, namely that the Brazilian legal system does not provide for unrestricted authorization to the free flow and sharing of

* Recebido em 17/09/2020
Aprovado em 06/11/2020

** Doutora em Comunicação pela Universidade de Brasília - UnB, Mestre em Direito Público pela Universidade do Estado do Rio de Janeiro – UERJ, professora da Faculdade de Direito do IDP Brasília. E-mail: miriam.wimmer@yahoo.com.br

data between governmental bodies. To conclude, the article examines to which extent elements such as compatibility of purposes, consent and specific legal provisions could provide the basis for greater legitimacy in data sharing between governmental bodies and agencies.

Keywords: Personal data protection. Data sharing. Secondary use of data. Public sector. Purpose limitation.

1 Introdução

O alastramento do novo coronavírus pelo planeta acarretou o rápido surgimento de estratégias para monitoramento e contenção de sua disseminação. Para além das medidas tradicionais de prevenção e controle de doenças epidêmicas, a atuação de governos de todo o mundo no combate à pandemia de Covid-19 caracterizou-se por dois importantes aspectos: de um lado, pelo uso inédito, em termos de intensidade, de tecnologias digitais e de dispositivos móveis de comunicação nos processos de detecção, notificação e investigação da doença; de outro, pela rápida escalada na coleta, análise e compartilhamento de dados pessoais entre atores públicos e privados, assim como entre distintos órgãos e entidades do Poder Público.

No Brasil, tais acontecimentos tiveram por efeito reacender os debates acerca *dos limites e das possibilidades de tratamento de dados pessoais*[1] *no setor público*, e, em especial, reavivar a discussão sobre os *critérios para o seu compartilhamento e uso secundário, isto é, a utilização de dados pessoais para finalidades distintas daquelas que justificaram originalmente a sua coleta.*

A intensa judicialização do tema, exacerbada pela incerteza que cercou a data de entrada em vigor da Lei Geral de Proteção de Dados pessoais – LGPD[2] e pela fragilidade institucional para lidar com o assunto no país[3], teve por foco inicial o uso, por governos estaduais, de dados de geolocalização oriundos de terminais móveis, para fins de elaboração de "mapas de calor" para verificar a observância das medidas de isolamento social. Posteriormente, o debate aprofundou-se no contexto das discussões sobre a inconstitucionalidade da Medida Provisória 954, de 2020, que determinava o compartilhamento de dados entre empresas de telecomunicações e o Instituto Brasileiro de Geografia e Estatística – IBGE, com vistas à realização de pesquisas estatísticas por telefone durante a pandemia.

Muito embora a temática do compartilhamento de dados pessoais envolvendo o poder público já houvesse anteriormente sido tratada pelo Supremo Tribunal Federal – STF, é correto afirmar que o ano de 2020 caracterizou-se pelo amadurecimento dos debates sobre o assunto no Tribunal, com o reconhecimento de um direito autônomo à proteção de dados pessoais[4] e a aplicação de tal compreensão em julgamento subsequente sobre o compartilhamento de dados no âmbito do Poder Executivo[5].

Nesse contexto, a problemática a ser enfrentada neste artigo diz respeito à ausência de critérios claros quanto às possibilidades e aos limites para o compartilhamento e uso secundário de dados pessoais no âmbito do poder público, lacuna que tem conduzido a um cenário de insegurança jurídica decorrente dos distintos entendimentos manifestados pelo Poder Executivo e pelo Poder Judiciário quanto ao tema. A par-

[1] Para os fins deste trabalho, adota-se o conceito amplo de dado pessoal estabelecido pela LGPD, como a informação relacionada à pessoa natural identificada ou identificável.

[2] Lei 13.709, de 14 de agosto de 2018.

[3] Muito embora a LGPD, aprovada em 2018, tenha previsto a criação de uma Autoridade Nacional de Proteção de Dados Pessoais – ANPD como aspecto central de seu modelo de proteção, a efetiva constituição de tal autoridade ocorreu apenas em novembro de 2020, quase dois meses após a data de entrada em vigor da Lei.

[4] Conforme julgamento de 7 de maio de 2020, no âmbito das Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393.

[5] Trata-se do julgado acerca do compartilhamento de dados entre a Agência Brasileira de Inteligência - ABIN e o Departamento Nacional de Trânsito – Denatran, no âmbito da ADPF 695.

tir desse cenário, considerando-se o fenômeno de intensificação da coleta e do compartilhamento de dados pessoais decorrente da pandemia de Covid-19 e as recentes manifestações do STF sobre o assunto, este artigo busca responder à seguinte pergunta: *quais parâmetros poderiam legitimamente balizar o compartilhamento e uso secundário de dados pessoais no âmbito do Estado?*

Como resposta preliminar a tal questão, este artigo apresenta a hipótese de que um primeiro parâmetro a ser considerado para justificar o compartilhamento e uso secundário de dados no poder público é o da compatibilidade de finalidades. Inexistindo tal compatibilidade de finalidades, são aventados dois elementos adicionais que poderiam, observadas determinadas condições, legitimar novo tratamento de dados pessoais: nova autorização fornecida pelo titular do dado; ou a existência de previsão legal específica. Em todos os casos, argumenta-se pela necessidade de aplicação dos princípios de proteção de dados e de adequada informação ao indivíduo afetado, mediante o estabelecimento de salvaguardas materiais e procedimentais associadas ao uso secundário de dados no contexto do Estado, considerando-se os parâmetros protetivos conferidos pelos princípios constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade.

A escassa produção acadêmica brasileira sobre o uso secundário de dados pessoais no poder público e a ausência de detalhamento da LGPD quanto ao tema justificam a relevância da temática escolhida, assim como motivam o recurso à doutrina predominantemente estrangeira. A metodologia adotada é bibliográfica e documental, fazendo-se referência a normas, julgados e decisões administrativas produzidos no Brasil e em outros países. No contexto nacional, o artigo dá destaque aos recentes julgados do STF que, adotados no contexto da pandemia, propiciaram a fixação de um importante paradigma para o debate brasileiro acerca do tema: o de que não há uma autorização irrestrita, no ordenamento jurídico brasileiro, ao livre fluxo e compartilhamento de dados no âmbito do Poder Público. Por fim, tendo-se em conta as críticas à ideia do Estado como unidade informacional, o artigo problematiza os riscos e benefícios do uso secundário de dados pessoais no âmbito do poder público e apresenta uma proposta de critérios que poderiam, com mais legitimidade, orientar e circunscrever o compartilhamento de dados entre órgãos e entidades governamentais.

É o que se passa a examinar.

2 A pandemia e o compartilhamento de dados no poder público: iniciativas, reações e novos paradigmas

Uma primeira reação praticamente universal à pandemia consistiu na intensificação de demandas por compartilhamento de dados, seja entre organizações do setor privado; seja entre o setor privado e o setor público; seja entre órgãos e entidades do setor público, em diferentes níveis federativos; ou, ainda, entre nações. Tal fenômeno gerou importantes reações, seja na esfera administrativa, seja no âmbito do Poder Judiciário. Nesta seção, examinam-se algumas das mais importantes iniciativas de compartilhamento de dados envolvendo o poder público no contexto da pandemia, assim como os parâmetros protetivos enunciados por autoridades de proteção de dados pessoais em outros países, por órgãos do Poder Judiciário e pelo próprio STF.

2.1 Principais iniciativas de compartilhamento de dados pessoais envolvendo o poder público

Cabe, de início, registrar que a intensificação do compartilhamento de dados pessoais foi uma consequência indiscutível da pandemia de COVID-19. Tal reação foi especialmente visível no campo da pesquisa científica, no qual foi observada maior disposição para conceder acesso a dados e a resultados científicos,

assim como o surgimento de parcerias-público privadas envolvendo empresas farmacêuticas, *startups*, agências governamentais, universidades e organizações filantrópicas, em busca do desenvolvimento de medicamentos e vacinas[6].

Outra seara em que se verificou significativo aumento das atividades de compartilhamento de dados refere-se ao contexto das atividades de empresas de telecomunicações e de tecnologia, com vistas ao monitoramento, contenção e mitigação da disseminação do vírus. Dada a possibilidade técnica de utilização de dados de geolocalização oriundos de terminais celulares, uma medida adotada de imediato por diversos países foi a criação de "mapas de calor", utilizando dados anonimizados e agregados, com o objetivo de identificar locais com maior aglomeração de pessoas, observar padrões de deslocamento e estimar o nível de isolamento social da população[7].

A viabilidade de uso de tais tecnologias para identificação da posição unívoca de determinada pessoa também impulsionou iniciativas para monitorar não apenas o comportamento de grupos de pessoas, mas também para controlar, de maneira individualizada, a observância da quarentena por parte de pessoas infectadas ou com suspeitas de infecção[8]. Observou-se, ainda, o surgimento de diversas iniciativas voltadas ao uso de aplicativos de rastreamento de contato *(contact tracing)* com base na emissão de sinais *bluetooth*, o que gerou duas ordens de preocupações: em primeiro lugar, quanto à forma de armazenamento dos dados coletados — de maneira centralizada, em bases de dados governamentais, ou de maneira descentralizada, permanecendo os dados no próprio dispositivo do usuário; e, em segundo lugar, quanto ao caráter voluntário ou compulsório de sua utilização e os impactos de sua adoção para o exercício de direitos e liberdades individuais[9].

---

[6] V. ABI YOUNES, G.; AYOUBI, C.; BALLESTER, O.; CRISTELLI, G.; VAN DEN HEUVEL, M.; ZHOU, L.; PELLEGRINO, G.; DE RASSENFOSSE, G.; FORAY, D.; GAULE, P.; WEBSTER, E. M. *COVID-19*: Insights from Innovation Economists. 14 de abril de 2020. Disponível em: https://ssrn.com/abstract=3575824. Acesso em: jul. 2020.

[7] Registre-se, a título de exemplo, os Relatórios de Mobilidade da Comunidade em função da COVID-19 produzidos pelo Google; os mapas de sintomas e de prevenção de doenças produzidos pelo Facebook; e, no Brasil, os mapas de calor com dados anonimizados e agregados fornecidos por operadoras móveis Claro, Oi, Tim e Vivo, em utilização em doze estados e quatorze prefeituras brasileiras, na data em que este artigo foi concluído. Vale registrar que medidas semelhantes já haviam sido adotadas no combate à malária na Tanzânia, ainda em 2008, e no combate ao vírus Ebola, na África Ocidental, em 2014. Cfr. SINDITELEBRASIL. *12 Estados e 14 Prefeituras já usam a plataforma das operadoras para identificar concentrações*. Nota à Imprensa de 11 de maio de 2020. Disponível em: https://www.sinditelebrasil.org.br/sala-de-imprensa/releases/3380-12-estados-e-14-prefeituras-ja-usam-a-plataforma-das-operadoras-para-identificar-concentracoes. Disponível em: jul. 2020; TATEM, A. J., QIU, Y; SMITH, D. L.; SABOT, O.; ALI, A. S.; MOONEN, B. The use of mobile phone data for the estimation of the travel patterns and imported Plasmodium falciparum rates among Zanzibar residents. *Malaria Journal,* v. 8, n. 1, nov. 2009. Disponível em: https://www.researchgate.net/publication/40681131_The_use_of_mobile_phone_data_for_the_estimation_of_the_travel_patterns_and_imported_Plasmodium_falciparum_rates_among_Zanzibar_residents#fullTextFileContent. Disponível em: jul. 2020; ERIKSON, S. L. Cell Phones as an Anticipatory Technology: Behind the Hype of Big Data for Ebola Detection and Containment. *Working Papers of the Priority Programme 1448 of the German Research Foundation Adaptation and Creativity in Africa: technologies and significations in the making of order and disorder*. Nr. 24, Leipzig and Halle 2018.

[8] Exemplos incluem o uso compulsório de pulseiras localizadoras, como em Hong Kong, a instalação de aplicativos no telefone celular, como na Polônia e na Turquia; e, ainda, a identificação da localização do terminal móvel com base na triangulação de estações rádio base ou por meio de sistemas satelitais, como em Taiwan. Cfr. MEISENZAHL, M. "People arriving in Hong Kong must wear tracking bracelets for 2 weeks or face jail time. Here's how they work. *Business Insider*, 4 de maio de 2020. Disponível em https://www.businessinsider.com/hong-kong-has-tracking-bracelets-to-enforce-coronavirus-quarantine-2020-4. Disponível em: jul. 2020; FRASER, M. Coronavirus contact tracing reignites Polish privacy debate. *Deutsche Welle*, 30 de maio de 2020. Disponível em: https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913. Disponível em: jul. 2020; ÖZKAN, B. Legal issues plague Turkey's pandemic tracking isolation project. *DuvaR.english*, 19 de abril de 2020. Disponível em: https://www.duvarenglish.com/health-2/coronavirus/2020/04/19/legal-issues-plague-turkeys-pandemic-tracking-isolation-project/. Disponível em: jul. 2020; LEE, Y. Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring. *Reuters*, 20 de março de 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK. Disponível em: jul. 2020.

[9] Aplicativos dessa natureza são, em sua grande maioria, baseados na emissão de sinais de *bluetooth*. Os telefones dos usuários dos aplicativos emitem sinais identificadores aleatórios que são registrados quando uma pessoa entre em contato com outra, observados determinados critérios de tempo e de distância. Quando uma pessoa recebe confirmação de que está infectada, pode consentir a que todas as pessoas com as quais teve contato relevante recebam uma notificação com orientações específicas, sem que sua identidade seja revelada. É possível distinguir entre abordagens centralizadas, nas quais os identificadores dos telefones são gerados, armazena-

Já no Brasil, as medidas de monitoramento e contenção da disseminação do vírus na população e os debates acerca de seus impactos sobre proteção de dados pessoais tiveram por pano de fundo dois importantes elementos contextuais: (i) de um lado, o protagonismo dos Estados e dos Municípios na adoção de medidas de enfrentamento à pandemia; e, de outro, (ii) a relevância do papel do Poder Judiciário no estabelecimento das condições de contorno para tais ações, inclusive no que se refere à proteção de dados pessoais.

As principais medidas de enfrentamento ao novo coronavírus foram delineadas pela Lei n. 13.979, de 6 de fevereiro de 2020, que estabeleceu, dentre outras ações, a possibilidade de adoção de medidas de isolamento, de quarentena, de realização compulsória de testes e exames, de restrição de entrada e saída do país e de requisição de bens e serviços de pessoas naturais e jurídicas, mediante posterior pagamento de indenização. Para os fins deste trabalho, importa dar destaque ao disposto no artigo 6º da norma, que determinou a obrigatoriedade de compartilhamento, entre órgãos e entidades da administração pública federal, estadual, distrital e municipal, de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação. Ainda nos termos do referido dispositivo, tal obrigação incide, também, sobre as pessoas jurídicas de direito privado, quando houver solicitação por autoridade sanitária.

A aprovação da Lei foi acompanhada da aceleração da implantação da Estratégia de Saúde Digital, com a criação da Rede Nacional de Dados em Saúde – RNDS, descrita como uma plataforma nacional projetada para permitir a integração de informações relativas à atenção à saúde, à vigilância em saúde e à gestão em saúde dos diferentes entes federativos, de entidades públicas e privadas[10].

Muito embora na esfera federal não tenham sido incorporadas, de maneira significativa, medidas tecnológicas de monitoramento de aglomerações e de rastreamento da disseminação do vírus, diversos Estados da federação entabularam parcerias com empresas de tecnologia e com prestadoras de serviços de telecomunicações para monitoramento dos índices de isolamento social e definição da estratégia de combate ao coronavírus a partir da análise de mapas de calor formados a partir de dados anonimizados e agregados. Uma das principais iniciativas nesse sentido foi a adotada pelo Governo de São Paulo, que, a partir de uma parceria com a associação que reúne as operadoras de telefonia móvel, criou o Sistema de Monitoramento Inteligente – SIMI. Os diversos questionamentos judiciais apresentados face à medida foram derrubados por decisão do órgão especial do Tribunal de Justiça de SP, que entendeu, por vinte votos a quatro, não existir ofensa à privacidade e à intimidade dos cidadãos[11]. Ainda antes da fixação de tal entendimento, já havia sido proferida decisão do Superior Tribunal de Justiça – STJ sobre o tema, indeferindo liminarmente um pedido de *habeas corpus* preventivo impetrado contra o Governador do Estado de São Paulo[12]. Dentre as razões de decidir, consta que não foram identificados quaisquer atos objetivos que pudessem causar, direta ou indiretamente, perigo ou restrição à liberdade de locomoção no caso, visto que os usuários não eram individualmente identificáveis.

Por fim, os impactos da pandemia global quanto à escalada na coleta, análise e compartilhamento de dados pessoais não se limitaram, estritamente, às ações para o seu enfrentamento. De fato, a pandemia forçou a súbita migração de inúmeras atividades para o ambiente digital e a aceleração de projetos de transformação

dos e processados em bases de dados governamentais centralizadas, conferindo às autoridades uma visão mais abrangente quanto à disseminação do vírus; e abordagens descentralizadas, em que tais informações são mantidas no próprio dispositivo do usuário, o que oferece aos usuários maior grau de privacidade e proteção contra divulgação indevida de seus dados. O recém anunciado *Pan-European Privacy-Preserving Proximity Tracing Programme* adota tal abordagem descentralizada.

10 Cfr. Portaria do Ministério da Saúde n.º 1.434, de 28 de maio de 2020, que "[i]nstitui o Programa Conecte SUS e altera a Portaria de Consolidação no 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde". No momento de conclusão deste artigo, a página eletrônica do RNDS informava que o projeto havia sido reorientado para receber e compartilhar informações referentes a resultados dos exames relacionados ao COVID-19 oriundos de laboratórios clínicos públicos e privados.

11 Mandado de Segurança n.º 2.073.723-23.2020.8.26.0000 – São Paulo, julgado em 04 de junho de 2020.

12 HABEAS CORPUS n.º 572.996 – SP, Rel. Min. Laurita Vaz, julgado em 16 de abril de 2020.

digital que já estavam em curso. Tais impactos foram sentidos de maneira bastante intensa pelo próprio poder público, que se viu compelido a intensificar esforços para a digitalização de serviços públicos com vistas à continuidade do exercício de suas atribuições legais[13].

No Brasil, iniciativas de governo digital já vinham sendo desenvolvidas há vários anos, merecendo destaque a edição, em 2016, da primeira Estratégia de Governança Digital — hoje já em sua terceira edição. Não há dúvidas, entretanto, de que a pandemia imprimiu um novo ritmo e sentido de urgência ao processo de transformação digital, inclusive por conta da necessidade de viabilizar o pagamento do auxílio emergencial no valor de R$600,00, instituído pela Lei n. 13.982, de 2020:

> a pandemia e as consequências do isolamento social de parte da população acelerou ainda mais a digitalização de serviços públicos. Dos 676 serviços do governo federal transformados em digitais desde janeiro do ano passado, 161 foram entregues ao público em 2020, com destaque para o auxílio emergencial de R$ 600. Neste caso, as tecnologias digitais permitiram — em menos de 30 dias — *o cadastro, o cruzamento de dados e o pagamento* deste necessário apoio aos trabalhadores informais e demais vulneráveis neste momento de crise[14] (grifou-se).

Como não poderia deixar de ser, a migração de serviços e de processos para o ambiente digital veio acompanhada por crescentes demandas de coleta, análise, compartilhamento e cruzamento de dados pessoais no âmbito do Poder Público. No caso do pagamento do auxílio emergencial, por exemplo, acórdão do Tribunal de Contas da União – TCU (2020) apontou para os riscos de inclusão e exclusão indevida de beneficiários, com identificação de seis fatores de risco: (i) baixa integração dos cadastros públicos; (ii) desatualização do Cadastro Único; (iii) dificuldade para identificação inequívoca em cadastros públicos; (iv) limitações para verificação de composição familiar; (v) limitações para verificação de vínculos de emprego e renda; e, (vi) limitações para cadastramento de pessoas com menor acesso a serviços públicos. Para endereçar tais fragilidades, o acórdão apresentou diversas recomendações quanto ao aprimoramento do cruzamento de dados contidos em bases do Poder Público[15].

2.2 Compartilhamento e proteção de dados pessoais: principais reações

É correto afirmar que a implementação de soluções tecnológicas de enfrentamento à pandemia foi recebida com cautela por entidades voltadas à proteção de dados pessoais e, em muitos casos, cercada de questionamentos judiciais[16].

Na Europa, por exemplo, a chegada da pandemia foi acompanhada por manifestações de autoridades de proteção de dados pessoais de diversos países e do próprio Comitê Europeu para a Proteção de Dados[17],

[13] A comprovar tal fato, relatório do Departamento de Assuntos Econômicos e Sociais da Organização das Nações Unidas aponta, durante a pandemia, um aumento no uso de serviços *online* como identidades e assinaturas digitais, associado inclusive ao aumento de pedidos por auxílio-desemprego e outros benefícios sociais. Indica, ademais, que o uso da tecnologia permitiu aos governos tomar decisões rápidas baseadas em análise de dados em tempo real, aprimorando a capacidade de coordenação de autoridades nacionais e locais com vistas à implementação de políticas baseadas em evidências.

[14] UEBEL, P.; MONTEIRO, L. F. S. *Artigo*: Uma Estratégia para o Brasil digital. O Globo**,** 24 de maio de 2020. Disponível em: https://oglobo.globo.com/opiniao/artigo-uma-estrategia-para-brasil-digital-1-24438953. Disponível em: jul. 2020.

[15] Por exemplo, as seguintes recomendações dirigidas ao Ministério da Cidadania:
"9.5.1. inclua nos cruzamentos de dados as bases de folha de pagamento de servidores dos poderes Legislativo e Judiciário federal e de servidores estaduais e municipais, no intuito de verificar renda e composição familiar, com base no § 11 do art. 2º da Lei 13.982/2020; 9.5.2. efetue cruzamentos de dados adicionais para mitigar o risco de pagamento indevido na terceira parcela e eventuais pendências de parcelas anteriores, devido à eventual alteração nas condições de elegibilidade do beneficiário, avaliando a viabilidade operacional e a relação custo-benefício do controle".

[16] Exemplo marcante é o de Israel, em que a Suprema Corte revogou a autorização que ela própria havia, poucos dias antes, concedido para que a Agência de Segurança Israelense, Shin Beth, implementasse política de vigilância digital em massa como parte da estratégia de combate à COVID-19. Em sua decisão, a Suprema Corte ressaltou os riscos de violação do direito constitucional à privacidade e condicionou a continuidade da medida à aprovação de lei específica sobre o assunto. Cfr. WINER, S. High Court: Shin Bet surveillance of virus carriers must be enshrined in law. The Times of Israel, 26 de abril de 2020.

[17] Trata-se do European Data Protection Board – EDPB, organização que reune representantes das autoridades de proteção de

indicando, de maneira unânime, a necessidade de observância dos princípios, das regras e dos direitos estabelecidos no Regulamento Geral de Proteção de Dados Pessoais Europeu – RGPD[18], de modo a viabilizar formas legítimas de tratamento de dados pessoais em situações de emergência sanitária de alcance geral.

É possível identificar, em tais pronunciamentos, uma tônica comum: a de que não haveria incompatibilidade entre proteção de dados pessoais e medidas de combate à pandemia, compreendendo-se ser o arcabouço normativo europeu suficientemente flexível para assegurar a possibilidade de compartilhamento dos dados necessários ao efetivo enfrentamento da situação emergencial. Por outro lado, elementos frisados em tais comunicações referem-se, também, à necessidade de observar a limitação das ferramentas adotadas à *finalidade específica* de combate à pandemia e ao período de tempo estritamente necessário para tanto, observando-se os direitos e liberdades dos cidadãos.

Na ausência de uma autoridade de proteção de dados pessoais no Brasil, que veio a ser criada somente em novembro de 2020, coube ao Comitê Gestor da Internet no Brasil – CGI.br, por meio de Nota Pública datada de 19 de maio de 2020, o papel de externar publicamente a necessidade de observância de princípios relacionados à proteção de dados pessoais, salientando a importância de que as medidas de rastreamento da população fossem excepcionais, limitadas e transparentes.

No que tange, especificamente, ao Princípio da Finalidade, é possível observar, em tais manifestações, a ideia de que "os fins devem ser *suficientemente específicos* para excluir o tratamento posterior para finalidades *não relacionadas com a gestão da crise* sanitária da COVID-19 (por exemplo, fins comerciais ou de aplicação da lei)", e que "uma vez definido claramente o objetivo, será necessário assegurar que a utilização dos dados pessoais seja *adequada, necessária e proporcionada*"[19]. Assim, revela-se, claramente, a preocupação em compatibilizar o uso da tecnologia como ferramenta eficaz de resposta à pandemia com garantias de que esse aparato tecnológico de monitoramento, construído em um momento de excepcionalidade, não se perpetue após o fim da epidemia.

Por outro lado, quando se trata das iniciativas voltadas para a aceleração da migração de serviços e de processos rotineiros de governo para o ambiente digital, fruto indireto da pandemia, observa-se que a discussão sobre o Princípio da Finalidade assume nuances distintas. De fato, os processos de transformação digital de serviços de governo são normalmente concebidos como caminhos sem volta. Assim, elementos como a limitação temporal do tratamento de dados pessoais ao período da pandemia e a utilização de tais dados apenas para a finalidade específica de gestão da crise sanitária, frisados em comunicações de autoridades de proteção de dados pessoais em diferentes países, podem ser colocados em questão, especialmente quando se verifica que os dados coletados e os compartilhamentos realizados podem eventualmente ser úteis para atingir outras finalidades públicas, distintas daquelas que justificaram o tratamento original.

As demandas por compartilhamento de dados pessoais associadas à pandemia acabaram por precipitar, no Brasil, uma discussão judicial sobre o tema no âmbito do Supremo Tribunal Federal – STF, com impactos profundos e duradouros para a disciplina de proteção de dados pessoais no país. O caso indubitavelmente mais importante, nesse contexto, é o da decisão do STF de suspender os efeitos da Medida Provisória 954, de 2020, que determinava o compartilhamento de dados detidos pelas operadoras de serviços de telecomunicações com o Instituto Brasileiro de Geografia e Estatística – IBGE, e que trouxe maior clareza quanto às condições para o compartilhamento de dados pessoais com o governo.

dados dos países europeus.

[18] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.

[19] EDPB – EUROPEAN DATA PROTECTION BOARD. *Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19*. Adotadas em 21 de abril de 2020. Disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Disponível em: jul. 2020.

2.3 Os novos parâmetros estabelecidos pelo Supremo Tribunal Federal

Conforme mencionado anteriormente, o tema do compartilhamento de dados pessoais no âmbito do Poder Público e da alteração da finalidade de seu tratamento já havia sido enfrentado pelo STF em diferentes oportunidades, ainda que de maneira menos aprofundada. Em 2017, por exemplo, decisão da Ministra Carmem Lúcia já havia entendido não ser cabível o fornecimento de dados individualizados detidos pelo IBGE ao Ministério Público Federal – MPF, por representar violação ao sigilo estatístico e ensejar potencial abalo à confiança das pessoas que prestam informações ao instituto[20]. Já em 2018, decisão do Ministro Luís Roberto Barroso negou a possibilidade de compartilhamento de dados detidos pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP com o Tribunal de Contas da União – TCU, com base não apenas no entendimento de que tal compartilhamento violaria o dever de preservação do sigilo da informação, mas também com fundamento na ideia de que a mudança de finalidade do tratamento violaria preceitos constitucionais e subverteria a autorização daqueles que forneceram seus dados pessoais[21].

Apesar da importância de tais decisões, que conferiram interpretação bastante restritiva quanto à possibilidade de compartilhamento e uso secundário de dados pessoais no âmbito do poder público, o STF não havia, ainda, se debruçado de maneira mais aprofundada sobre os parâmetros constitucionais a orientar o tratamento de dados pessoais pelo Estado.

Essa questão acabou sendo enfrentada pelo Tribunal justamente no contexto da pandemia de Covid-19. Em razão da impossibilidade de realizar entrevistas presencialmente, o IBGE tomou a decisão de realizar tais atividades por telefone. Para isso, no entanto, seria necessário ter acesso a uma base de dados telefônicos confiável e suficientemente representativa. Assim, foi editada a Medida Provisória 954/2020, que, referindo-se especificamente à situação de emergência de saúde pública de importância internacional decorrente do coronavírus, determinou que as empresas de telecomunicações prestadoras de serviços de telefonia fixa e móvel disponibilizassem à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas. A despeito dos cuidados de que a Medida Provisória buscou se cercar[22], ela foi prontamente contestada por cinco diferentes Ações Diretas de Inconstitucionalidade (ADIs)[23], movidas por partidos políticos de diferentes matizes ideológicas e pelo Conselho Federal da Ordem dos Advogados do Brasil.

O julgamento tornou-se paradigmático porque, dentre outras razões, consagrou o reconhecimento, pelo STF, de um direito autônomo à proteção de dados pessoais[24].

Curiosamente, embora a ideia de finalidade do tratamento tenha sido discutida durante o julgamento, não foi possível observar grande aprofundamento nos debates acerca da *mudança de finalidade* do tratamento dos dados em questão e de eventual incompatibilidade com a finalidade original. De fato, a discussão do Tribunal prendeu-se de maneira mais direta ao fato de que *a nova finalidade não havia sido suficientemente especificada*,

[20] Trata-se da decisão de Medida Cautelar na suspensão de Liminar 1.103-SP, por meio da qual a Ministra Presidente do STF, Carmen Lúcia, suspendeu decisão do TRF da 3a Região que havia determinado que o Instituto Brasileiro de Geografia e Estatística – IBGE fornecesse ao Ministério Público Federal dados necessários à identificação de quarenta e cinco crianças que não haviam sido regularmente registradas nos cartórios de registro civil de Bauru.

[21] A decisão foi proferida pelo Ministro Roberto Barroso, no contexto do Mandado de Segurança 36.150-DF, que havia sido impetrado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP contra acórdão do TCU que determinara a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família.

[22] A Medida Provisória determinou, por exemplo, que tais dados seriam utilizados para a finalidade exclusiva de produção estatística oficial, reafirmou seu caráter sigiloso, vedou seu compartilhamento com terceiros, estabeleceu determinadas obrigações de transparência quanto ao tratamento conferido aos dados e exigiu a eliminação de tais informações das bases de dados do IBGE quando superada a situação de emergência de saúde pública.

[23] ADI 6387, ADI 6388, ADI 6389, ADI 6390 e ADI 6393.

[24] MENDES, L. S. *Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais*. Portal Jota, 10 de maio de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Disponível em: jul. 2020.

conforme se depreende do Informativo 976 do STF:

> o colegiado observou que o único dispositivo da MP 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pelo IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. *Não delimita o objeto da estatística a ser produzida, nem a finalidade específica*, tampouco sua amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados. (Grifou-se).

O acórdão, publicado em novembro de 2020, enfatizou, também, esse ponto:

> 4. Consideradas a *necessidade, a adequação e a proporcionalidade* da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, *interesse público legítimo* no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.
>
> 5. *Ao não definir apropriadamente como e para que serão utilizados os dados* coletados, a MP no 954/2020 desatende a garantia do devido processo legal (art. 5o, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à 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*. (Grifou-se).

Muito embora a decisão do STF nesse caso não tivesse se aprofundado na questão do uso secundário dos dados cadastrais dos usuários de serviços de telecomunicações, ao fixar a ideia de que a proteção de dados pessoais é um direito passível de controle diretamente em face da Constituição Federal, criou as bases para uma análise mais detalhada do tema em um julgado subsequente. Trata-se do caso enfrentado na ADPF 695, na qual se questionava o compartilhamento da base de dados do Departamento Nacional de Trânsito – Denatran com a Agência Brasileira de Inteligência, com base em um simples Termo de Autorização, amparado pelo Decreto n. 10.046, de 9 de outubro de 2019, que será analisado em mais detalhes adiante.

Embora o ato autorizativo tenha sido revogado antes do julgamento, o voto do Ministro Gilmar Mendes, amparando-se no anterior julgado do STF referente à MP 954, revela inúmeras referências à problemática da alteração da finalidade do tratamento, como se depreende dos excertos a seguir reproduzidos:

> assim, no caso em tela, o que está em jogo não é apenas o nível de segurança da informação objeto do compartilhamento entre DENATRAN e ABIN, mas sim a existência de mecanismos adequados de *controle das finalidades* desse compartilhamento. Essa nova abordagem jurídica do direito fundamental à proteção de dados, nesse aspecto, engloba uma proteção abrangente, que desloca o eixo da proteção do conteúdo dos dados para as possibilidades e finalidades do seu processamento.
>
> Todos esses fatores indicam que, a priori, *não há uma autorização irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no Poder Público, inclusive para realização das atividades de inteligência nacional*. Desse modo, convênios e acordos de compartilhamento baseados única e exclusivamente nas disposições do Decreto 10.046/2020 parecem afigurar-se potencialmente lesivos às garantias individuais discutidas nesta ADPF, a depender, é claro, das condições de compartilhamento e dos riscos envolvidos.
>
> O teste de proporcionalidade é plenamente aplicável às relações de tratamento de dados no setor público. *A incidência do princípio da finalidade nessas relações não deve se limitar à busca por uma base legal – que no presente caso sequer é existente – mas deve levar em consideração também elementos como (i) as expectativas razoáveis do titular, (ii) a natureza dos dados processados e (iii) os possíveis prejuízos a serem suportados pelo titular*. (Grifou-se).

Interessa observar que, no caso em tela, o Ministro Relator entendeu que a revogação do Termo de Autorização que autorizara o compartilhamento dos dados não teria acarretado a perda de objeto da ADPF, dada a necessidade de examinar de maneira mais ampla o regime de compartilhamento de dados entre órgãos e instituições do Poder Público, com suposto lastro no Decreto nº. 10.046, de 2019, matéria caracterizada como sendo *"de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea"*.

3 Riscos e benefícios do uso secundário de dados pessoais no âmbito do poder público

As decisões do STF lançaram novas luzes sobre o debate acerca dos benefícios e riscos das atividades de coleta, análise e compartilhamento de dados pessoais entre setor privado e setor público e no âmbito dos diferentes órgãos e entidades do poder público. Tais controvérsias já haviam se manifestado, no Brasil, por ocasião da publicação do Decreto n.º 8.789, de 2016[25], que tratava da governança no compartilhamento de dados no âmbito da administração pública federal, e foram renovadas por ocasião da publicação do Decreto 10.046, de 2019[26], que o substituiu.

Vale recordar que tais normas foram publicadas no contexto de esforços de digitalização e de desburocratização do governo, com as finalidades de promover a simplificação da oferta de serviços públicos, viabilizar a formulação e implementação de políticas públicas baseadas em evidências, combater fraudes na distribuição de benefícios sociais e fiscais, dentre outras. Nessa linha, os mencionados Decretos acompanham a lógica do Decreto 9.094/2017, por exemplo, que dispõe sobre a simplificação do atendimento prestado aos usuários dos serviços públicos, ratifica a dispensa do reconhecimento de firma e da autenticação em documentos produzidos no País e institui a Carta de Serviços ao Usuário; e da Lei n.º 13.726, de 8 de outubro de 2017, que ficou conhecida por vedar a exigência de prova, perante o poder público, relativa ao fato de que já houvesse sido comprovado pela apresentação de outro documento válido.

Por outro lado, não são recentes — e nem exclusividade do Brasil — as preocupações quanto às propostas de ampla interconexão de bases de dados custodiadas pelo Poder Público e quanto ao uso secundário de dados pessoais, ou seja, o uso de dados pessoais para finalidades distintas daquelas que justificaram sua coleta inicial[27].

De fato, o debate sobre compartilhamento e sobre o uso secundário de dados no âmbito do Poder Público acaba por suscitar duas perspectivas de difícil conciliação. De um lado, aquela que afirma que o amplo compartilhamento de dados no Poder Público propicia a oferta de melhores serviços públicos, a eficiência e a desburocratização; de outro, aquela que chama atenção para os riscos decorrentes de tais iniciativas. Tal descompasso de discursos já havia sido apontado por Taylor, Lips e Organ, que indicaram que estudos no campo da vigilância adotam, em geral, um enfoque crítico quanto à ampliação da captura e do tratamento de informações e dados pessoais pelo governo, ao passo que estudos no campo da administração pública e referentes à provisão de serviços públicos tendem a adotar uma visão amplamente favorável a tais atividades[28].

---

[25] Por exemplo, a crítica de Cella e Copetti ao Decreto de 2016: "[c]om efeito, a tecnocracia, com seus ideais de eficiência, enxerga no compartilhamento de bancos de dados um bem em si mesmo. Diante desse posicionamento reducionista, resulta, aos olhos delirantes dos burocratas, inquestionável a decisão governamental que se enveredou para esse perigoso rumo de intercâmbio de dados pessoais, cuja implementação, sem que se considerem contrapesos e salvaguardas, pode levar a drásticos efeitos colaterais". Cfr. CELLA, J. R. G.; COPETTI, R. Compartilhamento de Dados Pessoais e a Administração Pública Brasileira. *Revista de Direito, Governança e Novas Tecnologias*, Maranhão, v. 3, p. 39-58, jul./dez. 2017. p. 40.

[26] Por ocasião da publicação do Decreto 10.046, de 2019, chegaram a ser apresentados, no Congresso Nacional, diversos Projetos de Decreto Legislativo com o objetivo de sustar os seus efeitos, argumentando-se ter havido exorbitação do poder regulamentar conferido ao poder Executivo.

[27] Ainda em 2003, o Grupo de Trabalho do Artigo 29 *(Article 29 – Data Protection Working Party)* produziu documento de trabalho sobre governo eletrônico que se debruçou sobre o tema, salientando os riscos associados à generalizada interconexão de bases de dados governamentais. O documento sugere que a análise sobre os riscos e benefícios de tais medidas seja pautada pelas seguintes questões: (i) quais são os benefícios esperados do uso dos dados e de sua interconexão, considerando os objetivos do governo? (ii) há abordagens alternativas para atingir o mesmo objetivo? (iii) quais são os riscos e custos da interconexão? (iv) quais garantias poderiam ser adotadas (por exemplo, tecnologias voltadas à privacidade)? e (v) ao fim da análise, há um equilíbrio entre os benefícios e riscos acarretados pela interconexão pretendida? Cfr. WP 29 – ARTICLE 29 DATA PROTECTION WORKING PARTY. Working Document on E-Government. Adopted on 8 May 2003.

[28] TAYLOR, J.; LIPS, M.; ORGAN, J. Identification practices in government: Citizen surveillance and the quest for public service improvement. *Identity in the Information Society,* v. 1, n. 1, p. 135-154, nov. 2008. Disponível em: https://www.researchgate.net/publication/225422938_Identification_practices_in_government_citizen_surveillance_and_the_quest_for_public_service_improvement#fullTextFileContent. Disponível em: jul. 2020.

Sob outro prisma, quando se trata de debater os limites ao compartilhamento de dados pessoais dentro do governo, a discussão sobre privacidade e proteção de dados pessoais é frequentemente caracterizada como um debate referente a um direito eminentemente individual, colocado em contraposição a interesses sociais mais amplos[29]. Dessa forma, a busca pela satisfação do interesse público ou do bem comum, de um lado, e a proteção da privacidade, de outro, são, muitas vezes, apresentados, de maneira reducionista, como objetivos inconciliáveis.

A doutrina tem buscado superar tal polarização dando ênfase à dimensão social e coletiva dos direitos associados à privacidade e à proteção de dados pessoais, decorrente inclusive do seu papel habilitador para o exercício de inúmeros outros direitos e garantias fundamentais[30].

De fato, como expõe Raab, a ideia de um direito à privacidade e à proteção de dados pessoais para além de sua dimensão individual, dotado de interesse público e baseado em uma visão de complexidade social, traz importantes consequências práticas quando se trata de balancear valores contrapostos, como frequentemente ocorre no âmbito do tratamento de dados pessoais pelo poder público[31]. Assim, é preciso considerar que a despeito dos objetivos frequentemente meritórios e legítimos a justificar o compartilhamento e o uso secundário de dados pessoais no âmbito do Poder Público, a forma concreta de (re)utilização dos dados pode vir a ensejar consequências negativas, decorrentes (i) da quebra de confiança entre o titular dos dados e a organização que os coletou, (ii) da frustração das expectativas do titular quanto ao tratamento que justificou determinada coleta e (iii) da sensação de insegurança quanto à forma em que o dados pessoais serão utilizados no futuro[32]. É interessante notar que tais consequências podem até mesmo colocar em xeque a efetividade da política pública que justificou inicialmente a coleta dos dados, como se pode depreender dos debates havidos no Reino Unido acerca do compartilhamento de informações sobre pacientes entre o *National Health Service* e autoridades de imigração ligadas ao Ministério do Interior *(Home Office)*[33].

O compartilhamento de dados dentro do Poder Público e o seu uso em contextos diversos do original suscitam, ainda, questões mais complexas ligadas ao *design* institucional, chamadas, por Solove[34], de problemas "arquitetônicos". Tais problemas estão associados, de um lado, aos riscos aumentados de danos morais ou materiais decorrentes de uma maior exposição e circulação dos dados[35]; e, de outro lado, à possibilidade de desequilíbrio indesejável do poder social ou institucional, decorrente de uma inadequada distribuição do conhecimento sobre indivíduos entre órgãos públicos com diferentes atribuições.

---

[29] Nessa linha, v. OSWALD, M. Share and Share Alike? An examination of trust, anonymisation and data sharing with particular reference to an exploratory research project investigating attitudes to sharing personal data with the public sector. *Scripted,* v. 11, Issue 3, dez. 2014. Disponível em: http://nrl.northumbria.ac.uk/id/eprint/40603/1/oswald.pdf. Disponível em: jul. 2020; REGAN, P. *Legislating Privacy.* Technology, Social Values, and Public Policy. Chapel Hill, NC: University of North Carolina Press, 1995; e SIMITIS, Spiros. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review 135,* p. 707-746, mar. 1987. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review. Disponível em: jul. 2020.

[30] Cfr. RAAB, C. D. Privacy, Social Values and the Public Interest. In: BUSCH, A; HOFMANN, J. (org.). *Politik und die Regulierung von Information, Politische Vierteljahresschrift Sonderheft 46*. Baden-Baden: Nomos Verlagsgesellschaft, 2012; SOLOVE, D. J. Understanding Privacy. Cambridge: Harvard University Press, 2008; BLACK, G.; STEVENS, L. Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest. *Scripted,* v. 10, n. 1, p. 93-122, Abr. 2013.; MANTELERO, A. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. In: TAYLOR, L.; FLORIDI, L.; VAN DER SLOOT, B. *Group Privacy:* new challenges of data technologies. Dordrecht: Springer, 2017. p. 139- 158.

[31] RAAB, C. D. Privacy, Social Values and the Public Interest. In: BUSCH, A; HOFMANN, J. (org.). *Politik und die Regulierung von Information, Politische Vierteljahresschrift Sonderheft 46*. Baden-Baden: Nomos Verlagsgesellschaft, 2012.

[32] Cfr. SOLOVE, D. J. A Taxonomy of privacy. *University of Pennsylvania Law Review.* v. 154*,* n. 3, Jan. 2006. Disponível em https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2074&context=faculty_publications. Disponível em: jul. 2020.

[33] TRAVIS, A. NHS chiefs urged to stop giving patient data to immigration officials. *The Guardian***,** 31 de janeiro de 2018. Disponível em: https://www.theguardian.com/society/2018/jan/31/nhs-chiefs-stop-patient-data-immigration-officials. Disponível em: jul. 2020.

[34] Cfr. SOLOVE, D. J. A Taxonomy of privacy. *University of Pennsylvania Law Review.* v. 154*,* n. 3, p. 487, Jan. 2006. Disponível em https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2074&context=faculty_publications. Disponível em: jul. 2020.

[35] Por exemplo, os riscos aumentados de furto de identidade ou de incidentes de segurança que possam expor os dados pessoais em questão.

No âmbito doméstico, a questão encontra-se, ainda, revestida de considerável incerteza, visto que a LGPD se limita a enunciar, de maneira bastante vaga, em seu artigo 26, que o uso compartilhado de dados pessoais pelo Poder Público deve atender a *finalidades específicas* de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados na própria Lei. A Lei não enuncia elementos mais detalhados que permitam compreender em que medida os princípios de proteção de dados pessoais — e, em especial, o Princípio da Finalidade[36] — podem impactar o fluxo de dados pessoais dentro do próprio Estado.

Tais reflexões requerem o aprofundamento da análise acerca das possibilidades e limites do compartilhamento de dados pessoais no âmbito do poder público, avaliando-se em que medida o *Princípio da Finalidade* impõe restrições ao uso secundário de dados pelo Estado.

É o que se passa a examinar.

4 O princípio da finalidade e a divisão informacional de poderes

Do que precede, é possível compreender que o debate sobre compartilhamento e uso secundário de dados pessoais remete, fortemente, à discussão sobre o conceito de *autodeterminação informativa*, expresso no paradigmático julgamento do Tribunal Constitucional alemão de 1983[37], no qual se afirmou que o acesso irrestrito a dados pessoais colocaria em risco praticamente todos os direitos constitucionalmente protegidos. Nos termos da decisão, o exercício da autodeterminação informativa ficaria seriamente comprometido caso indivíduos não pudessem, com suficiente segurança, saber quais informações a seu respeito são conhecidas e para quais finalidades tais informações são coletadas e tratadas. No contexto das modernas possibilidades de processamento de dados, afirmou o Tribunal, o livre desenvolvimento da personalidade requer que o indivíduo seja protegido contra a coleta, armazenamento, uso e compartilhamento ilimitado de dados pessoais.

Nesse sentido, a discussão sobre usos secundários de dados pessoais deve também pautar-se pela interpretação do *Princípio da Finalidade*, pilar fundamental das normas de proteção de dados pessoais[38] e que consta também da Lei Geral de Proteção de Dados Pessoais brasileira[39]. Tal princípio, que pode ser compreendido como um desdobramento da autodeterminação informativa, é, de fato, capaz de estabelecer importantes restrições ao uso secundário de dados pessoais, visto que condiciona a realização do tratamento para propósitos específicos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

De fato, no entender de Mendes e Doneda, a aplicação de tal princípio, que vincula o tratamento de dados a determinada função, tem por efeito "afetar" dados pessoais a determinada finalidade, impedindo que sejam considerados como mera *res in commercium*[40]. Na mesma linha, Doneda e Viola consideram o Princípio da Finalidade como corolário de um pressuposto segundo o qual a informação pessoal, por ser expressão

[36] Cfr. Artigo 6º, inciso I da LGPD:
"Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, *sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*." (Grifou-se).

[37] Volkszählungsurteil (BVerfGE 65, 1)

[38] De fato, a ideia de finalidade consta de documentos como a Carta dos Direitos Fundamentais da União Europeia (artigo 8.2); a Convenção para a Proteção das Pessoas Relativamente aos Dados de Caráter Pessoal - Convenção 108 (art. 5º, "b"); e as Diretrizes sobre Privacidade da Organização para a Cooperação e Desenvolvimento Econômico – OCDE (artigos 9 e 10).

[39] Cfr. Artigo 6º, inciso I da LGPD:
"Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, **sem possibilidade de tratamento posterior de forma incompatível com essas finalidades**." (Grifou-se).

[40] MENDES, L. S.; DONEDA, D. Reflexões iniciais sobre a nova Lei geral de Proteção de Dados. *Revista de Direito do Consumidor,* São Paulo, v. 120. Ano 27. p. 469-483, nov. dez. 2018. p. 474.

direta da personalidade de seu titular, permanece sempre vinculada a ele. É justamente o Princípio da Finalidade, segundo os autores, que limita a possibilidade de utilização secundária da informação pessoal à revelia de seu titular, possibilidade que tornaria inócuos outros meios de proteção e controle os dados pessoais por parte da pessoa a quem se referem[41].

4.1 **Autodeterminação informativa e o princípio da finalidade:** delineamentos sobre a compatibilidade de finalidades secundárias no poder público

O Princípio da Finalidade gera também relevantes desdobramentos com relação ao tratamento de dados pessoais no âmbito do poder público. É com base nesse significativo princípio que parte importante da doutrina argumenta que o Estado não deve se configurar como uma "unidade informacional", devendo os dados pessoais ser tratados em conformidade com as funções específicas do órgão público e com a finalidade específica que justificou sua coleta, conforme exposto por Simitis:

> a limitação do tratamento vinculado pela finalidade afeta não apenas a manipulação dos dados, mas tem também extensas consequências organizacionais. A finalidade condiciona tanto o uso interno como externo. Seja o usuário um membro da organização ou não, *a finalidade específica que legitima a coleta restringe qualquer tratamento adicional. Consequentemente, o governo, em particular, não pode mais ser tratado como uma única unidade informacional*, a justificar o livre fluxo de dados entre todas as unidades governamentais. As funções específicas de uma agência e sua relação com a finalidade específica que conduziu à coleta dos dados determinam a possibilidade de acesso à informação, e não apenas o fato de que tal agência faz parte do governo. A estrutura interna do governo, portanto, precisa ser readequada para fazer frente às exigências de separação funcional que inibem as tendências de proliferação[42]. (Grifou-se).

Assim, a noção de divisão informacional de poderes tem sido utilizada para fundamentar o entendimento de que a finalidade de coleta e tratamento de dados pessoais por cada órgão público circunscreve-se à estrita definição de sua competência legal, sendo vedado o uso para outra finalidade dentro da Administração[43]. Embora o conceito seja recente no contexto brasileiro, observa-se, na experiência de outros países, que as políticas de governo digital frequentemente incorporam a ideia de que os cidadãos podem possuir múltiplas relações com o Estado, por meio de seus diferentes órgãos e entidades, e que deve caber ao indivíduo a decisão de permitir que uma entidade tenha visibilidade sobre as demais relações de identidade por ele mantidas[44].

Por outro lado, é correto afirmar que o Princípio da Finalidade não corresponde a um impedimento absoluto ao uso secundário de dados pessoais, mas impõe a observância de que eventual nova finalidade seja *compatível* com a finalidade original[45].

---

41 DONEDA, D. VIOLA, M. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. *Revista Brasileira de Risco e Seguro*, Rio de Janeiro, v. 5, n. 10, p. 85-102, our. 2009/mar.2010. p. 98.

42 Cfr. SIMITIS, Spiros. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review 135,* p. 707-746, mar. 1987. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review. Disponível em: jul. 2020. p.741. Tradução livre de: "The limitation of purpose-bound processing not only affects the actual handling of the data but also has far-reaching organizational consequences. The purpose delineates both the internal and the external use. Whether the user is an insider or an outsider, the specific aim legitimating the collection restricts any further processing. Consequently, government in particular no longer can be treated as a single information unit, justifying a free flow of data among all governmental units. An agency's specific functions and their relationship to the particular purpose that led to the collection of the data determine the access to the information, not the mere fact that the agency is part of the government. The internal structure of government, therefore, must be reshaped to meet the demands of functional separation that inhibits proliferation tendencies".

43 V. MARANHÃO, J; CAMPOS, R. *A divisão informacional de Poderes e o Cadastro Base do Cidadão*. Portal Jota, 18 de outubro de 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019. Disponível em: jul. 2020.

44 Cfr. FISHENDEN, J. eID: Identity Management in an Online World. *5th European Conference on e-Government* (ECEG 2005). Disponível em: https://ntouk.files.wordpress.com/2015/05/eid-identity-management-in-an-online-world-paper.pdf. Disponível em: jul. 2020; e FISHENDEN, J. *Federated Identity for Access to UK Public Services: 1997–2020. An overview*. 29 de junho de 2020. Versão 1.0. Disponível em: https://www.researchgate.net/publication/342623905_Federated_Identity_for_Access_to_UK_Public_Services_1997-2020. Disponível em: 10 set. 2020.

45 Tal entendimento já havia sido expresso pelo Working Party 29 ainda em 2013. ARTICLE 29 DATA PROTECTION WORK-

A ideia de "compatibilidade" é, decerto, dotada de enorme abertura conceitual, requerendo elaboração adicional no campo da doutrina e da regulamentação brasileira. Nessa linha, Doneda e Viola, em trabalho publicado quase uma década antes da aprovação da LGPD, já indicavam que a compatibilidade entre o motivo da coleta e a utilização do dado pessoal em questão poderia ser verificada pela aplicação do Princípio da Proporcionalidade, o que permitira verificar, nos casos concretos, (i) se a utilização do dado não seria abusiva; (ii) se tal uso secundário não ultrapassaria os limites de uso que os titulares pudessem razoavelmente cogitar no momento do fornecimento do dado; e (iii) se haveria interesses relevantes que pudessem sugerir a necessidade de maior elasticidade e tolerância com utilizações mais amplas de dados pessoais[46].

Alguns parâmetros adicionais podem ser depreendidos da experiência europeia. O Regulamento Geral de Proteção de Dados, por exemplo, estabelece que o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais (art. 5º) e, para os demais casos, estabelece alguns critérios que permitem avaliar a compatibilidade de tratamento de dados pessoais para uma finalidade distinta da original (art. 6.4). São eles: a existência de vínculos entre a finalidade original e a nova finalidade; o contexto em que os dados pessoais foram coletados, em particular no que tange ao relacionamento entre o titular dos dados e o controlador; a natureza dos dados pessoais; as possíveis consequências do tratamento adicional dos dados para os titulares; e a existência de salvaguardas apropriadas, que podem incluir o uso de criptografia ou de pseudonimização.

Tal conceito de compatibilidade de finalidades como condição para usos secundários de dados pessoais tem sido reiterado em inúmeras oportunidades em manifestações de autoridades de proteção de dados, que têm, de maneira indireta, remetido à noção de integridade contextual desenvolvida por Helen Nissenbaum[47], que coloca ênfase sobre o atendimento às razoáveis expectativas dos indivíduos quanto à forma em que seus dados são tratados e compartilhados. No Brasil, também Bioni utiliza o conceito de privacidade contextual para refletir sobre usos secundários de dados pessoais, argumentando que a elasticidade do conceito, amparado nas legítimas expectativas dos titulares quanto às características contextuais da relação estabelecida entre controlador e titular, é que permite governar os usos secundários de dados que não podem ser previamente especificados e controlados de maneira rígida[48].

4.2 Usos secundários no poder público: é possível remediar a incompatibilidade de finalidades?

Por fim, diante do exposto, pode-se compreender que um grande desafio que se coloca para o setor público, nos casos em que se pretenda compartilhar dados pessoais entre distintos órgãos e entidades, está não apenas em verificar a existência de uma base legal para o tratamento dos dados, mas também em aferir se a nova finalidade que justifica o compartilhamento — que deve ser específica, e não genérica — possui compatibilidade com a finalidade original. Tais preocupações são particularmente relevantes no contexto do Poder Público, dada a natureza assimétrica, não facultativa e continuada das relações entre indivíduos e Estado.

Por outro lado, coloca-se a seguinte questão: caso se constate que determinado uso secundário é, de fato, incompatível com a finalidade original que justificou a coleta de dados, seria possível "remediar" tal incompatibilidade de finalidades? Se sim, de que forma?

Trata-se de questão não trivial. A Opinião n. 3/2003 do *Working Party 29*, por exemplo, expedida antes da aprovação do RGPD, sustentava que um tratamento incompatível não poderia ser remediado mediante a simples invocação de uma nova base legal. Na visão da organização, seria contrário ao espírito do Princípio

ING PARTY. Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013.

[46] DONEDA, D. VIOLA, M. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. *Revista Brasileira de Risco e Seguro*, Rio de Janeiro, v. 5, n. 10, p. 85-102, our. 2009/mar.2010. p. 100.

[47] Cfr. NISSENBAUM, H. *Privacy in Context*. Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

[48] BIONI, B. R. *Proteção de Dados Pessoais*. A função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 243 ss.

da Finalidade admitir que se pudesse, mediante simples modificação do contrato com o titular dos dados ou invocação de um interesse legítimo do controlador, "legalizar" um tratamento de dados pessoais que seria, em outras circunstâncias, incompatível com a finalidade original.

Por outro lado, é possível encontrar, em documentos internacionais, entendimentos mais flexíveis quanto ao tema. Ainda em 1974, Resolução do Conselho da Europa sobre a proteção da privacidade de indivíduos face a bases de dados eletrônicas no setor público afirmava que os dados armazenados não deveriam ser utilizados para outras finalidades além daquelas definidas, a não ser que houvesse (i) exceções previstas em lei; (ii) permissão por autoridade competente; ou (iii) que houvesse emendas às regras sobre o uso da base de dados eletrônica (art. 3, "c"). Também as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico – OCDE sobre privacidade, expedidas em 1980 e atualizadas em 2013, afirmam que dados pessoais não devem ser divulgados, tornados disponíveis ou utilizados para finalidades distintas daquelas que justificaram a coleta a não ser que haja (i) consentimento por parte do titular dos dados; ou (ii) previsão legal.

Essa é, também, a lógica adotada pelo RGPD, que, em seus prolegômenos, lança luz sobre a questão:

> o tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for *compatível* com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. [...]
>
> Caso o titular dos dados tenha dado o seu *consentimento* ou o tratamento se baseie em *disposições do direito da União ou de um Estado-Membro* que constituam uma medida necessária e proporcionada, numa sociedade democrática, para salvaguardar, em especial, os *importantes objetivos de interesse público geral*, o responsável pelo tratamento deverá ser autorizado a proceder ao tratamento posterior dos dados pessoais, *independentemente da compatibilidade das finalidades*.
>
> Em todo o caso, deverá ser garantida a aplicação dos princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os seus direitos, incluindo o direito de se opor. (Grifou-se).

Assim, apesar das controvérsias que circundam o tema, é possível identificar, no cenário internacional, uma certa consistência de entendimentos segundo os quais seria possível superar a incompatibilidade de finalidades por meio do consentimento do titular ou com base em previsão legal específica, necessária e proporcional, observando-se o pleno respeito aos demais princípios e direitos associados à proteção de dados pessoais. Nesse sentido, ganha particular importância o dever de transparência perante o titular, que se caracteriza como condição objetiva para o exercício de direitos como o de oposição ao novo tratamento[49].

Cabe recordar, por fim, que, quando se trata das relações entre indivíduo e Estado, o uso da base legal do consentimento para fundamentar o tratamento de dados pessoais pode ser considerado problemático em alguns aspectos, dada a assimetria de forças entre cidadão e Estado, o que dificulta a obtenção de um consentimento livro, informado e inequívoco *(meaningful consent)* [50]. A superação de eventual incompatibi-

[49] Interessante, nesse sentido, observar manifestação da Information Comissioner's Office – ICO, autoridade britânica de proteção de dados pessoais, que assinala que "[n]ão pode haver a obrigação de fornecer dados pessoais para oferecer serviços públicos importantes e depois usá-los para serviços que não justificariam tal obrigação, sem que haja nova consulta ao indivíduo ou previsão legal específica." (Tradução livre, grifou-se). Cfr. ICO – INFORMATION COMMISSIONER'S OFFICE. *The Information Commissioner's response to a call for evidence on digital identity from the Secretary of State for the Department for Digital, Culture, Media and Sport.* 13 Sep. 2019. Disponível em: https://ico.org.uk/media/about-the-ico/consultation-responses/2019/2616260/ico-response-dcms-call-for-evidence-20190913.pdf. Disponível em: jul. 2020. p. 8.

[50] Mesmo fora do contexto das relações cidadão – Estado, a base legal do consentimento para justificar usos secundários de dados pessoais é criticada por parte da doutrina. Simitis, por exemplo, afirma que o processo de consentimento é uma "mistificação" que desconsidera o fato de que o valor de uma doutrina regulatória como a do "consentimento informado" depende integralmente do contexto econômico e social da atividade em questão. V. SIMITIS, Spiros. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review 135,* p. 707-746, mar. 1987. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review. Disponível em: jul. 2020. p. 737. Também Cohen questiona a "retórica do consentimento" utilizada para legitimar tais tratamentos secundários, retórica essa que, em sua visão, obscurece as escolhas políticas subjacentes às atuais políticas de privacidade de dados. Para a autora, a "escolha" que tal modelo protege não é a escolha individual, mas

lidade de finalidades, no contexto do uso secundário de dados pessoais no âmbito do Poder Público, requer, portanto, análise criteriosa acerca da base jurídica mais apropriada para sustentar o novo tratamento, considerando que nem sempre o consentimento será a opção mais adequada. Além disso, como se pode depreender tanto da experiência internacional como do debate doméstico sobre o tema, previsão normativa genérica a autorizar o compartilhamento de dados pessoais parece carecer dos elementos necessários para legitimar usos secundários de dados pessoais no âmbito do Estado, sendo necessária a previsão de finalidade suficientemente especificada, que permita a avaliação do interesse público a ser atingido, assim como a necessidade e adequação de tal medida.

Por último, o reconhecimento dos profundos impactos que a circulação de dados pessoais no âmbito do Estado pode ensejar para a esfera de direitos dos indivíduos impõe que usos secundários de dados pessoais venham acompanhados não apenas da identificação de uma base legal apropriada, mas também de avaliação sobre as consequências de tais novas utilizações para os direitos e liberdades do titular, estabelecendo-se, com transparência, as políticas e salvaguardas adequadas para a mitigação de eventuais riscos identificados.

5 Considerações finais: consequências para o debate brasileiro

Ao longo deste artigo, buscou-se demonstrar que a pandemia de Covid-19 teve por efeito intensificar e acelerar as iniciativas de compartilhamento de dados pessoais com o Poder Público e entre seus órgãos e entidades, precipitando discussões judiciais que acabaram por estabelecer novos paradigmas para o tratamento de dados pelo Estado. Assim, uma situação extraordinária, muitas vezes invocada para sustentar a adoção de medidas de excepcionalidade, deixou um legado inesperado: a fixação definitiva, na jurisprudência, de parâmetros interpretativos sobre o tratamento de dados no poder público, com impactos duradouros e estruturantes para o debate doméstico sobre o tema.

Assim, a partir do reconhecimento pelo STF de um direito fundamental à proteção de dados pessoais (ADI 6387), decisão subsequente fixou o entendimento de que não há uma autorização irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no âmbito do Poder Público (ADPF 695), e que eventuais usos secundários de dados pessoais, a partir de seu compartilhamento entre diferentes órgãos e entidades, devem levar em consideração elementos como as expectativas razoáveis do titular, a natureza dos dados processados e os possíveis prejuízos a serem suportados pelo titular.

Os julgados em questão são de enorme importância para o debate nacional sobre o tratamento de dados pessoais no âmbito do Estado e impõem, para a doutrina e para o próprio Poder Executivo, a necessidade de aprofundamento da discussão sobre os critérios que podem viabilizar o legítimo compartilhamento de dados entre órgãos e entidades do poder público.

Com base na experiência internacional e à luz do próprio texto da LGPD, é possível compreender que não haveria impedimentos *a priori* ao compartilhamento de dados com vistas ao tratamento de dados pessoais para finalidades *compatíveis* com aquelas que justificaram a coleta original, desde que observadas as regras procedimentais e, principalmente, os princípios aplicáveis ao tratamento de dados pessoais, tais como a necessidade, a adequação e a transparência. É certo, por outro lado, que a indeterminação e a abertura do conceito de "compatibilidade" indicam a premência do desenvolvimento de parâmetros mais objetivos para sua aferição nos casos concretos.

Por outro lado, quando se trata de *usos secundários incompatíveis* com a finalidade original, coloca-se a questão de saber se tal incompatibilidade teria por efeito excluir, de maneira definitiva, a possibilidade do

a escolha dos controladores de dados sobre como, e para quais finalidades, classificar os indivíduos. COHEN, J. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review 52*, p. 1373-1438, 2000. Disponível em: https://scholarship.law.georgetown.edu/facpub/810. Disponível em: jul. 2020. p. 1399.

tratamento pretendido, ou se seria possível superar tal incompatibilidade mediante a invocação de novas bases legais.

Embora a questão não seja incontroversa, a experiência internacional indica, nesses casos, que nova autorização do titular ou previsão legal específica poderiam fundamentar tais novos tratamentos, desde que garantida a aplicação dos princípios de proteção de dados e, em especial, a adequada informação ao indivíduo afetado. No caso de usos secundários no âmbito do poder público, a assimetria de forças e o caráter não voluntário da relação entre cidadão e Estado impõem a necessidade de cautela adicional na utilização da base legal do consentimento para legitimar tal novo tratamento.

Esse entendimento é, de certo modo, compatível com o julgamento do STF no caso da MP 954, que determinava o compartilhamento de dados entre empresas de telecomunicações e o IBGE. Conforme exposto anteriormente, a censura do Tribunal não recaiu sobre a mudança de finalidade, mas voltou-se, principalmente, para a insuficiente especificação da finalidade do compartilhamento, o que, no entender no STF, tornaria impossível aferir o interesse público, a necessidade, a adequação e a proporcionalidade da medida. A decisão monocrática proferida no âmbito da ADPF 695 também parece seguir tal linha de raciocínio, ao indicar a necessidade de que a mudança de finalidade do tratamento encontre não apenas uma base legal, mas também observe critérios substantivos que permitam salvaguardar as expectativas dos titulares, assim como os seus direitos.

De ambas as decisões, é possível extrair a ideia de que ainda que se possa, em determinadas circunstâncias, admitir o compartilhamento de dados pessoais no âmbito do poder público com mudança das finalidades que justificaram sua coleta, não basta simplesmente conferir um verniz de legalidade para formalmente justificar tal uso secundário. É necessário, ao invés, o estabelecimento de salvaguardas materiais e procedimentais e a observância de todo o conjunto de direitos e princípios associados à proteção de dados pessoais, justificando-se, claramente, o interesse público específico a ser atingido, tendo em vista os parâmetros protetivos conferidos pelos princípios constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade.

Definir a maneira concreta pela qual tal exercício de balanceamento pode ser realizado, com segurança e legitimidade, à luz das disposições da LGPD e da Constituição Federal, é tarefa ainda a ser enfrentada no campo normativo e doutrinário.

Referências

ABI YOUNES, G.; AYOUBI, C.; BALLESTER, O.; CRISTELLI, G.; VAN DEN HEUVEL, M.; ZHOU, L.; PELLEGRINO, G.; DE RASSENFOSSE, G.; FORAY, D.; GAULE, P.; WEBSTER, E. M. *COVID-19*: Insights from Innovation Economists. 14 de abril de 2020. Disponível em: https://ssrn.com/abstract=3575824. Acesso em: jul. 2020.

ABREU, J. D. S. *O Compartilhamento de Dados Pessoais no Decreto n. 8.789/16*: um Frankenstein de dados brasileiro? Portal Jota, 8 julho 2016. Disponível em: https://bit.ly/2Fsqwge Disponível em: jul. 2020.

BIONI, B. R. *Proteção de Dados Pessoais.* A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLACK, G.; STEVENS, L. Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest. *Scripted*, v. 10, n. 1, p. 93-122, Abr. 2013.

CELLA, J. R. G.; COPETTI, R. Compartilhamento de Dados Pessoais e a Administração Pública Brasileira. *Revista de Direito, Governança e Novas Tecnologias*, Maranhão, v. 3, p. 39-58, jul./dez. 2017.

CGI.br - COMITÊ GESTOR DA INTERNET NO BRASIL. *Nota Pública sobre tratamento de dados pessoais e vigilância no período de isolamento social pela pandemia da COVID-19*. 19 de maio de 2020. Disponível em: https://cgi.br/esclarecimento/nota-publica-sobre-tratamento-de-dados-pessoais-e-vigilancia-no-periodo-de-isolamento-social-pela-pandemia-da-covid-19/. Disponível em: jul. 2020.

CoE - COUNCIL OF EUROPE. *Resolution 74(29) on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies. Disponível em: https://rm.coe.int/09000016807aa909. Disponível em: jul. 2020.

COHEN, J. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review 52*, p. 1373-1438, 2000. Disponível em: https://scholarship.law.georgetown.edu/facpub/810. Disponível em: jul. 2020.

DONEDA, D. *Da privacidade à proteção de dados pessoais:* elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thompson Reuters, 2019.

DONEDA, D. VIOLA, M. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. *Revista Brasileira de Risco e Seguro*, Rio de Janeiro, v. 5, n. 10, p. 85-102, our. 2009/mar.2010.

EDPB – EUROPEAN DATA PROTECTION BOARD. *Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19*. Adotadas em 21 de abril de 2020. Disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Disponível em: jul. 2020.

ERIKSON, S. L. Cell Phones as an Anticipatory Technology: Behind the Hype of Big Data for Ebola Detection and Containment. *Working Papers of the Priority Programme 1448 of the German Research Foundation Adaptation and Creativity in Africa: technologies and significations in the making of order and disorder*. Nr. 24, Leipzig and Halle 2018. Disponível em: https://lost-research-group.org/wp-content/uploads/2018/01/WP24_Erikson_180115.pdf. Disponível em: jul. 2020.

FISHENDEN, J. *Federated Identity for Access to UK Public Services: 1997–2020. An overview*. 29 de junho de 2020. Versão 1.0. Disponível em: https://www.researchgate.net/publication/342623905_Federated_Identity_for_Access_to_UK_Public_Services_1997-2020. Disponível em: 10 set. 2020.

FISHENDEN, J. eID: Identity Management in an Online World. *5th European Conference on e-Government* (ECEG 2005). Disponível em: https://ntouk.files.wordpress.com/2015/05/eid-identity-management-in-an-online-world-paper.pdf. Disponível em: jul. 2020.

FRASER, M. Coronavirus contact tracing reignites Polish privacy debate. *Deutsche Welle*, 30 de maio de 2020. Disponível em: https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913. Disponível em: jul. 2020

GINSBURG, T.; VERSTEEG, M. Binding the Unbound Executive: Checks and Balances in Times of Pandemic. *Virginia Public Law and Legal Theory Research Paper No. 2020-52; U of Chicago, Public Law Working Paper No. 747*. 9 de junho de 2020. Disponível em https://ssrn.com/abstract=3608974. Disponível em: jul. 2020.

ICO – INFORMATION COMMISSIONER'S OFFICE. *The Information Commissioner's response to a call for evidence on digital identity from the Secretary of State for the Department for Digital, Culture, Media and Sport*. 13 Sep. 2019. Disponível em: https://ico.org.uk/media/about-the-ico/consultation-responses/2019/2616260/ico-response-dcms-call-for-evidence-20190913.pdf. Disponível em: jul. 2020.

ICO – INFORMATION COMMISSIONER'S OFFICE. *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (2017). Disponível em: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Disponível em: jul. 2020.

LEE, Y. Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring. *Reuters*, 20 de março de 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK. Disponível em: jul. 2020.

MANTELERO, A. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. In: TAYLOR, L.; FLORIDI, L.; VAN DER SLOOT, B. *Group Privacy:* new challenges of data technologies. Dordrecht: Springer, 2017. p. 139- 158.

MARANHÃO, J; CAMPOS, R. *A divisão informacional de Poderes e o Cadastro Base do Cidadão*. Portal Jota, 18 de outubro de 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019. Disponível em: jul. 2020.

MEISENZAHL, M. "People arriving in Hong Kong must wear tracking bracelets for 2 weeks or face jail time. Here's how they work. *Business Insider*, 4 de maio de 2020. Disponível em https://www.businessinsider.com/hong-kong-has-tracking-bracelets-to-enforce-coronavirus-quarantine-2020-4. Disponível em: jul. 2020.

MENDES, L. S. *Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais*. Portal Jota, 10 de maio de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Disponível em: jul. 2020.

MENDES, L. S.; DONEDA, D. Reflexões iniciais sobre a nova Lei geral de Proteção de Dados. *Revista de Direito do Consumidor,* São Paulo, v. 120. Ano 27. p. 469-483, nov. dez. 2018.

NISSENBAUM, H. *Privacy in Context*. Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

OECD – ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *The OECD Privacy Frameword*. (2013). Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Disponível em: jul. 2020.

OECD – ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. *The Path to Becoming a Data-Driven Public Sector*. Paris: OECD Publishing, 2019.

OSWALD, M. Share and Share Alike? An examination of trust, anonymisation and data sharing with particular reference to an exploratory research project investigating attitudes to sharing personal data with the public sector. *Scripted,* v. 11, Issue 3, dez. 2014. Disponível em: http://nrl.northumbria.ac.uk/id/eprint/40603/1/oswald.pdf. Disponível em: jul. 2020.

ÖZKAN, B. Legal issues plague Turkey's pandemic tracking isolation project. *Duva*R.*english*, 19 de abril de 2020. Disponível em: https://www.duvarenglish.com/health-2/coronavirus/2020/04/19/legal-issues-plague-turkeys-pandemic-tracking-isolation-project/. Disponível em: jul. 2020.

RAAB, C. D. Privacy, Social Values and the Public Interest. In: BUSCH, A; HOFMANN, J. (org.). *Politik und die Regulierung von Information, Politische Vierteljahresschrift Sonderheft 46*. Baden-Baden: Nomos Verlagsgesellschaft, 2012.

REGAN, P. *Legislating Privacy*. Technology, Social Values, and Public Policy. Chapel Hill, NC: University of North Carolina Press, 1995

SIMITIS, Spiros. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review 135,* p. 707-746, mar. 1987. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review. Disponível em: jul. 2020.

SINDITELEBRASIL. *12 Estados e 14 Prefeituras já usam a plataforma das operadoras para identificar concentrações.* Nota à Imprensa de 11 de maio de 2020. Disponível em: https://www.sinditelebrasil.org.br/sala-de-im-

prensa/releases/3380-12-estados-e-14-prefeituras-ja-usam-a-plataforma-das-operadoras-para-identificar--concentracoes. Disponível em: jul. 2020.

SOLOVE, D. J. A Taxonomy of privacy. *University of Pennsylvania Law Review.* v. 154, n. 3, Jan. 2006. Disponível em https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2074&context=faculty_publications. Disponível em: jul. 2020.

SOLOVE, D. J. *Understanding Privacy.* Cambridge: Harvard University Press, 2008.

STF - SUPREMO TRIBUNAL FEDERAL. *Informativo de Jurisprudência 976 – 4 a 8 de maio de 2020*. Disponível em http://www.stf.jus.br/arquivo/informativo/documento/informativo976.htm. Disponível em: jul. 2020.

TATEM, A. J., QIU, Y; SMITH, D. L.; SABOT, O.; ALI, A. S.; MOONEN, B. The use of mobile phone data for the estimation of the travel patterns and imported Plasmodium falciparum rates among Zanzibar residents. *Malaria Journal,* v. 8, n. 1, nov. 2009. Disponível em: https://www.researchgate.net/publication/40681131_The_use_of_mobile_phone_data_for_the_estimation_of_the_travel_patterns_and_imported_Plasmodium_falciparum_rates_among_Zanzibar_residents#fullTextFileContent. Disponível em: jul. 2020.

TAYLOR, J.; LIPS, M.; ORGAN, J. Identification practices in government: Citizen surveillance and the quest for public service improvement. *Identity in the Information Society,* v. 1, n. 1, p. 135-154, nov. 2008. Disponível em: https://www.researchgate.net/publication/225422938_Identification_practices_in_government_citizen_surveillance_and_the_quest_for_public_service_improvement#fullTextFileContent. Disponível em: jul. 2020.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. *Acórdão 1428/2020* - Plenário, Rel. Min. Bruno Dantas. Processo 016.827/2020-1. Data da sessão: 3 de junho de 2020. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-avalia-a-implementacao-do-auxilio-emergencial.htm. Disponível em: jul. 2020.

TRAVIS, A. NHS chiefs urged to stop giving patient data to immigration officials. *The Guardian*, 31 de janeiro de 2018. Disponível em: https://www.theguardian.com/society/2018/jan/31/nhs-chiefs-stop-patient--data-immigration-officials. Disponível em: jul. 2020.

UEBEL, P.; MONTEIRO, L. F. S. *Artigo*: Uma Estratégia para o Brasil digital. O Globo, 24 de maio de 2020. Disponível em: https://oglobo.globo.com/opiniao/artigo-uma-estrategia-para-brasil-digital-1-24438953. Disponível em: jul. 2020.

UNDESA – UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS. *E--Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development (with addendum on COVID-19 Response)*. New York: United Nations, 2020.

WINER, S. High Court: Shin Bet surveillance of virus carriers must be enshrined in law. *The Times of Israel*, 26 de abril de 2020. Disponível em: https://www.timesofisrael.com/high-court-shin-bet-surveillance-of--virus-carriers-must-be-enshrined-in-law/. Disponível em: jul. 2020.

WP 29 – ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 03/2013 on purpose limitation.* Adopted on 2 April 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion--recommendation/files/2013/wp203_en.pdf. Disponível em: jul. 2020.

WP 29 – ARTICLE 29 DATA PROTECTION WORKING PARTY. *Working Document on E-Government.* Adopted on 8 May 2003. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion--recommendation/files/2003/e-government_en.pdf. Disponível em: jul. 2020.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.