LIMITES AO ACESSO DE AUTORIDADES PÚBLICAS A *BIG DATA*: EVOLUÇÃO LEGISLATIVA E GOVERNANÇA REGULATÓRIA

LIMITS ON PUBLIC AUTHORITIES' ACCESS TO BIG DATA: LEGISLATIVE EVOLUTION AND REGULATORY GOVERNANCE

Recebimento: 21 maio 2019
Aceitação: 26 maio 2021

Carlos Emmanuel Joppert Ragazzo
Doutor em Direito
Afiliação institucional: Escola de Direito da Fundação Getulio Vargas – FGV Direito Rio – (Rio de Janeiro, RJ, Brasil)
Lattes iD: http://lattes.cnpq.br/9694200934261935
Email: carlos.ragazzo@fgv.br

Marina Rodrigues Cyrino Baleroni
Mestra em Direito
Afiliação institucional: Escola de Direito da Fundação Getulio Vargas – FGV Direito Rio – (Rio de Janeiro, RJ, Brasil)
Lattes iD: http://lattes.cnpq.br/5402216804878762
Email: macyrino@gmail.com

Douglas Wilson Marostica Leite Junior
Mestre em Direito
Afiliação institucional: Escola de Direito da Fundação Getulio Vargas – FGV Direito Rio – (Rio de Janeiro, RJ, Brasil)
Lattes iD: http://lattes.cnpq.br/1089554694096503
Email: douglasleiteadv@gmail.com

Como citar este artigo / How to cite this article (informe a data atual de acesso / inform the current date of access):
RAGAZZO, Carlos Emmanuel Joppert; BALERONI, Marina Rodrigues Cyrino; LEITE JUNIOR, Douglas Wilson Marostica. Limites ao acesso de autoridades públicas a *big data*: evolução legislativa e governança regulatória. **Revista da Faculdade de Direito UFPR**, Curitiba, v. 66, n. 2, p. 9-30, maio/ago. 2021. ISSN 2236-7284. Disponível em: https://revistas.ufpr.br/direito/article/view/67003. Acesso em: 31 ago. 2021. DOI: http://dx.doi.org/10.5380/rfdufpr.v66i2.67003.

RESUMO
Com o aumento da utilização de plataformas de distribuição de conteúdo pela internet (conhecidas como *over the top* ou OTTs) em diversos setores no Brasil, um volume cada vez mais considerável de dados vem sendo armazenado por empresas de tecnologia, havendo, ainda, pouco consenso sobre condições de repasse desses dados às autoridades públicas em atendimento a solicitações ou mesmo em parcerias realizadas entre agentes públicos e privados. Diante desse cenário, este artigo tem por objetivo refletir sobre os limites do poder público no acesso às informações privadas de indivíduos, especialmente quanto a *big data*. Para tanto, analisa-se a evolução dos pedidos de dados apresentados por governos a particulares e o contexto em que tais solicitações se operam. Expõem-se, também, os riscos associados ao tratamento de dados pessoais pelo poder público, além dos marcos regulatórios aplicáveis. O resultado da análise indica as tendências dos ciclos de acesso a dados pelo governo. Por fim, conclui-se que o poder público não deve estar autorizado a solicitar dados pessoais se não houver

meios de comprovar que possui capacidade técnica para realizar o tratamento das informações recebidas e armazená-las com segurança, garantindo-lhes confidencialidade.

PALAVRAS-CHAVE
Big data. OTTs. Regulação. Acesso a dados pessoais.

ABSTRACT
Given the increased use of content provider platforms via internet (also known as over the top or OTTs) in Brazil, a growing amount of data has been stored by technology companies, albeit there is still little consensus on the conditions for the transfer of said data in response to public authorities' requests or due to partnerships between public and private parties. In view of this scenario, this article aims to discuss the limits to public authority's access to private information of individuals, especially for big data requests. To do so, it analyzes the evolution of data requests presented by governments to private parties and the context in which such requests occur. It also exposes the risks associated with the processing of personal data by the government, in addition to the applicable regulatory frameworks. The result of the analysis indicates the trends for cycles of data requests by government. The article concludes that public authorities should not be authorized to request personal data if there is no means to demonstrate technical capacity to process and store them safely, ensuring confidentiality.

KEYWORDS
Big data. OTTs. Regulation. Access to private data.

INTRODUÇÃO

Ao regulamentar a exploração da atividade econômica privada de transporte individual remunerado de passageiros, a Prefeitura de São Paulo editou uma série de atos normativos infralegais a partir de 2016. Em particular, uma das medidas estabelecidas pelo marco regulatório paulistano previa que as empresas operadoras de aplicativos (chamadas, pela norma regulamentadora, de Operadoras de Tecnologia de Transporte Credenciadas – OTTCs) deveriam compartilhar com o Município dados pessoais dos motoristas cadastrados em suas plataformas, o que envolveria um volume considerável de informações, incluindo nome, filiação, data de nascimento, sexo, estado civil, endereço, telefone, endereço eletrônico, RG, CPF, CNH, além de placa do carro e código RENAVAM (SÃO PAULO, 2017).

Nos termos da regulamentação, a Prefeitura tinha o dever de garantir que os dados recebidos das empresas fossem protegidos e gerenciados adequadamente, garantindo-lhes a integridade, confidencialidade e autenticidade, devendo nomear um "Gestor da Informação", a quem competiria garantir o sigilo e a inviolabilidade dos dados (SÃO PAULO, 2016).

O Município de São Paulo, contudo, antes de demonstrar ter adotado qualquer medida apta a garantir a segurança dos dados, e antes mesmo de nomear o Gestor da Informação, passou a exigir

que as empresas operadoras de aplicativos compartilhassem os dados dos motoristas. A Uber, então, ingressou em juízo pedindo que tal obrigação não lhe fosse exigida até que a Prefeitura estabelecesse meios efetivos de assegurar a proteção das informações[1]. A juíza Carmen Cristina Teijeiro, da 5ª Vara de Fazenda Pública de São Paulo, deferiu liminar em favor da Uber. O Município de São Paulo contestou a ação, insistindo em sua tentativa de receber os dados. Posteriormente, contudo, admitiu que não havia tomado as medidas necessárias e reconheceu a procedência dos pedidos formulados pela Uber, que foram, então, julgados procedentes em sentença de mérito.

O caso serve para ilustrar um novo espaço de conflito entre autoridades públicas e empresas privadas de tecnologia coletoras e armazenadoras de dados particulares. Embora o foco das discussões veiculadas em grandes mídias tenha tratado de questionamentos regulatórios relacionados a assuntos tributários, concorrenciais e, mais recentemente, sobre privacidade[2], as autoridades públicas têm aumentado de forma significativa pedidos de compartilhamento de dados pessoais nos últimos anos (COOPERATION…, 2018).

Nesse sentido, este artigo traz uma pesquisa baseada na análise de casos concretos envolvendo requisições governamentais de dados pessoais por governos a empresas privadas detentoras desses dados no Brasil e no exterior. A hipótese a ser examinada é a de que os benefícios da utilização de *big data* pelo poder público devem ser sopesados com os riscos à privacidade dos indivíduos. A análise parte de referenciais teóricos envolvendo a sociedade de risco, a proteção dos dados pessoais e os perigos envolvidos em processos de anonimização, além dos limites e possibilidades do poder de polícia. Com o propósito de identificar os objetivos públicos associados às solicitações governamentais de dados desde sua origem até hoje, bem como possíveis tendências para os próximos anos, a seção 1, abaixo, examina o contexto em que esses pedidos são endereçados a empresas privadas (de forma contenciosa, como no exemplo acima, ou mesmo em formato de parcerias e colaborações).

Ato contínuo, a seção 2 deste artigo irá examinar os riscos gerados pelos pedidos de bases de dados pessoais por parte de autoridades governamentais, em especial endereçando as vantagens e possíveis problemas associados a técnicas de anonimização, se e quando o pedido governamental for adequado. Na sequência, a seção 3 apresentará os limites que podem ser impostos às autoridades

1 Processo nº 1002511-62.2018.8.26.0053, 5ª Vara de Fazenda Pública de São Paulo.

2 Como exemplo, pode ser citado um episódio ocorrido em janeiro de 2021 envolvendo o vazamento de quantidades de dados pessoais associados a cerca de 223,5 milhões de cidadãos brasileiros. As informações, incluíram nome completo, CPF, data de nascimento, dados de veículos, escolaridade, fotografias, renda e scores de crédito (MEGAVAZAMENTO…, 2021).

governamentais que pretendem coletar dados pessoais, a fim de verificar se o Brasil possui ou não um instrumental legislativo adequado, para, ao fim, estimar como o debate deve ser orientado no País.

1 EVOLUÇÃO E TENDÊNCIAS NO ACESSO A DADOS PESSOAIS PELO PODER PÚBLICO

Para entender de forma correta o movimento consubstanciado pelo pedido feito pela Prefeitura de São Paulo, é necessário avaliar qual tendência ele representa. Na verdade, o acesso a dados pessoais por autoridades públicas ganha relevo a partir do momento posterior aos atentados de 11 de setembro de 2001, em que foi promulgada nos Estados Unidos da América a lei conhecida como Patriot Act, com o objetivo de aumentar os poderes investigativos das autoridades policiais. Sob a justificativa do combate ao terrorismo, o Patriot Act possibilitou que agentes de diversas áreas do governo federal norte-americano tivessem acesso a informações mantidas por entes privados envolvendo dados pessoais, bem como o conteúdo de comunicações privadas de indivíduos, como *e-mails* e mensagens de voz (JAEGER; BERTOT; MCCLURE, 2003).

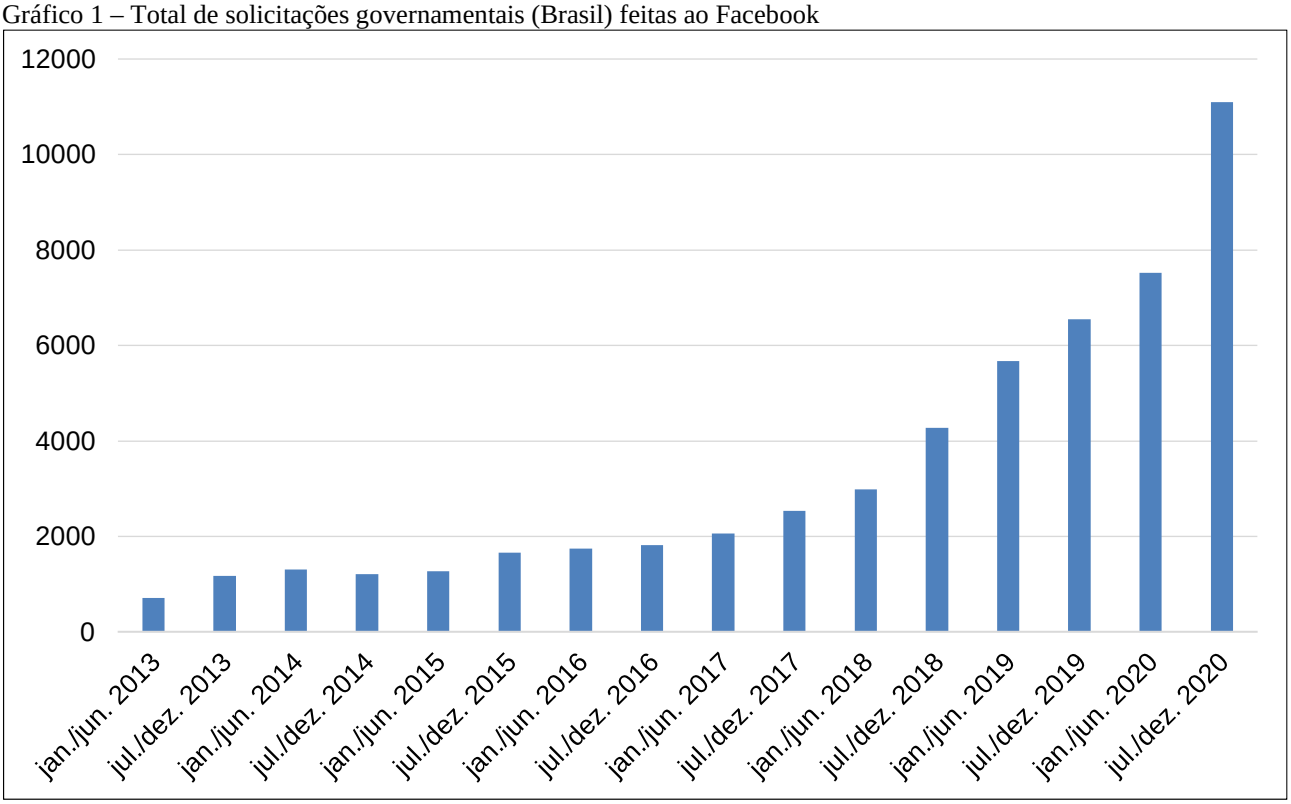
Por meio de alterações ao Foreign Intelligence Surveillance Act, o Patriot Act flexibilizou as condições impostas ao governo para ter acesso a dados de cidadãos, expandindo as circunstâncias autorizadoras da vigilância governamental. Antes do Patriot Act, agentes interessados em obter uma ordem judicial autorizando o acesso a informações privadas deveriam demonstrar que a obtenção dessas informações constituía o propósito de uma investigação envolvendo inteligência estrangeira. Após o advento da nova lei, passou-se a exigir que as informações pretendidas fossem obtidas em investigações que apenas parcialmente se relacionassem ou que tangenciassem questões envolvendo inteligência estrangeira. Como consequência, observou-se um aumento no número de ordens judiciais autorizando acesso de agentes governamentais a dados privados de cidadãos (JAEGER; BERTOT; MCCLURE, 2003).

Em um segundo momento, autoridades públicas, visando fundamentar investigações, passaram a solicitar dados pessoais. Nesse ciclo, iniciado na última década, pôde ser verificado um crescimento relevante, em diversos países, de pedidos de dados pessoais formulados por autoridades governamentais a empresas privadas que administram aplicações de internet. Apenas no Brasil, no primeiro semestre de 2018, o Facebook recebeu 2.991 solicitações advindas de autoridades para compartilhar informações sobre os usuários de sua rede social (GOVERNMENT…, 2019). A grande maioria (92,3%) desses pedidos de dados foi decorrente de processos judiciais, o que é esperado em vista da sistemática estabelecida na Lei Federal 12.965/2014 (“Marco Civil da Internet”), a ser

explicada mais à frente neste artigo, pela qual o provedor responsável pela guarda dos dados somente será obrigado a disponibilizar registros de conexão e acesso a aplicações de internet, de forma autônoma ou associada a dados pessoais, mediante ordem judicial (BRASIL, 2014a).

Nesse contexto, muitos pedidos de dados são feitos por autoridades policiais no âmbito de investigações criminais, o que levou o Facebook a criar e divulgar diretrizes operacionais para autoridades policiais que pretendam solicitar registros ao Facebook e ao Instagram[3]. Já na esfera cível, são comuns pedidos de dados que identifiquem pessoas que causaram danos a outrem na internet, de modo a viabilizar o pagamento da indenização devida[4]. Informações divulgadas pelo Facebook demonstram um crescimento, ao longo dos últimos anos, desse tipo de pedido de dados no Brasil, conforme se observa no Gráfico 1:

Gráfico 1 – Total de solicitações governamentais (Brasil) feitas ao Facebook



Fonte: autoria própria, a partir de dados coletados em Government… (2019).

[3] Disponível em: https://bit.ly/3oWBnW8. Acesso em: 1 maio 2019.

[4] Nesse sentido, a jurisprudência do STJ: "Ao oferecer um serviço por meio do qual se possibilita que os usuários divulguem livremente suas opiniões, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada imagem uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, do dever de informação e do princípio da transparência, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omittendo. Precedentes." (BRASIL, 2014b).

Mais recentemente, surgiu um novo ciclo de tipos de pedidos de compartilhamento de dados (no caso do transporte de passageiros por aplicativo, refletido em obrigações regulatórias), em que a pretensão dos órgãos públicos é a de receberem *big data* de empresas privadas para auxiliar a tomada de decisões de política pública[5], o que já tem ocorrido no Brasil. Como exemplo da busca do poder público brasileiro pela utilização de *big data* de empresas particulares no Brasil, tem-se os decretos municipais das cidades de São Paulo e do Rio de Janeiro que regulamentam a atividade de transporte individual privado de passageiros por meio de aplicativos, os quais contêm previsões de que as empresas operadoras dos aplicativos devem abrir e compartilhar uma série de informações com as administrações locais[6, 7]. Esses decretos, ainda, criaram comitês municipais, que aprofundaram as regulamentações sobre compartilhamento de dados. Vale notar que, embora os pedidos de *big data* sejam, em número, menores do que os verificados no ciclo anterior (ainda em curso, aliás), o volume de informação é significativamente maior, já que bases de dados inteiras são objeto dos pedidos de dados formulados.

Nem sempre o acesso aos dados particulares coletados por aplicações tecnológicas se dá por meio de pedidos expressos ou mesmo via obrigações regulatórias. Existem situações em que os órgãos governamentais realizam parcerias com as empresas privadas, o que pode ser visto, no Brasil, por meio dos exemplos das Prefeituras do Rio de Janeiro e de São Paulo, que anunciaram a realização de parcerias com a empresa responsável pelo aplicativo de trânsito Waze, para fins de gerenciamento do tráfego de veículos no espaço urbano, o que se dá mediante o fornecimento de dados às prefeituras (PREFEITURA…, 2013; PREFEITURA…, 2017). Essas parcerias de prefeituras com o Waze estão inseridas no contexto do programa Connected Citizens, pelo qual o Waze compartilha dados para auxiliar cidades na gestão da mobilidade urbana (WAZE…, 2019). Atualmente, esse programa é implementado em 250 cidades do mundo, incluindo Rio de Janeiro e São Paulo (MOREIRA, 2017).

---

5 *Big data* pode ser entendido como a combinação de diversos bancos de dados digitais para uso em estatísticas e outras técnicas de extração de padrões, correlações ou informações ocultas (RUBINSTEIN, 2012). O conceito de *big data* envolve quatro parâmetros: (*i*) volume de dados; (*ii*) variedade de formatos, fontes e tipos; (*iii*) velocidade de buscas e dados recuperados; e (*iv*) veracidade das conclusões baseadas nos dados (PORCHE et al., 2014).

6 Decreto nº 44.399/2018 do Município do Rio de Janeiro, art. 15: "As PROVER disponibilizarão ao Município, sem ônus e mediante solicitação, equipamentos, programas, sistemas, serviços ou qualquer outro mecanismo físico ou informatizado que viabilize, facilite, agilize e dê segurança à fiscalização de suas operações. Parágrafo único. Para efeito do disposto no caput deste artigo, fica assegurado ao Município o acesso aos sistemas de controle de frota, faturamento, acesso a bases de dados e a percepção de dados estáticos e/ou dinâmicos das PROVER, na forma e parâmetros estabelecidos pelo CMTSVU, inclusive pela integração dos sistemas, para o acompanhamento do serviço ou qualquer outra utilização dos dados compartilhados, observado o interesse público e o sigilo dos dados".

7 Decreto nº 56.981/2016 do Município de São Paulo, art. 35: "As OTTCs credenciadas ficam obrigadas a abrir e compartilhar com a Secretaria Municipal de Mobilidade e Transportes – SMT, na forma e periodicidade definidas pelo Poder Público, os dados necessários ao controle e à regulação de políticas públicas de mobilidade urbana, garantida a privacidade e confidencialidade dos dados pessoais do condutor. (Redação atribuída pelo Decreto nº 58.598/2019)".

Da mesma forma, a empresa que administra o aplicativo Airbnb assinou, em junho de 2018, um acordo com a Secretaria Estadual de Turismo, Esporte e Cultura de Santa Catarina prevendo o compartilhamento de dados agregados sobre a utilização da plataforma no estado. A ideia da parceria é aprimorar o planejamento de estratégias e políticas públicas voltadas para o desenvolvimento do turismo responsável na região (AIRBNB…, 2018).

Na verdade, o Brasil segue a tendência internacional. Em outros países, já é possível citar alguns exemplos concretos de uso de *big data* em políticas públicas. O primeiro, na cidade de Dubuque, estado de Iowa, nos Estados Unidos, envolve a utilização de *big data* de telefones celulares para monitorar trabalhadores pendulares (*commuters*) e buscar a melhora de serviços de trânsito (POELA et al., 2015). Para obter os dados, a cidade de Dubuque possui parcerias com a International Business Machines (IBM) e outras empresas (DUBUQUE…, 2011). Já o governo da Holanda utiliza, para fins estatísticos, diversos dados obtidos por meio da cooperação de empresas privadas, como operadoras de telefonia celular e administradoras de redes sociais (DAAS; LOO, 2013). Ainda, a cidade de Louisville, no estado de Kentucky, nos Estados Unidos, utiliza *big data* para questões de saúde pública de seus cidadãos. A cidade possui muitos habitantes com distúrbios respiratórios, o que, frequentemente, resulta em problemas no atendimento na emergência de hospitais. Inaladores com GPS fornecem dados (local e hora) que são analisados para prever quando e onde tais episódios ocorrerão (POELA et al., 2015). Nesse caso, os inaladores são sincronizados com os *smartphones* dos usuários e, mediante consentimento, podem transferir informações para a administração local.

Ainda sobre o cenário internacional, vale também mencionar a existência de iniciativas macro como a Global Partnership for Sustainable Development Data, uma ação global que busca unir governos, o setor privado e organizações da sociedade civil para utilização de *big data*, como forma de atingir objetivos para o desenvolvimento sustentável. Entre as empresas participantes dessa iniciativa estão Facebook, Microsoft e IBM[8].

Verifica-se, assim, uma tendência de aumento do uso de *big data* por autoridades governamentais, mesmo porque é impossível negar os significativos impactos positivos que essa prática pode proporcionar para a administração pública, como melhorias nos sistemas de trânsito, na prevenção de doenças e na gestão de recursos públicos. Todavia, o avanço da humanidade no campo da ciência e tecnologia, além de gerar como consequência a produção social de riqueza, igualmente implica a produção social de riscos. Ao mesmo tempo que as forças produtivas humanas e tecnológicas evoluem, riscos são desencadeados numa medida até então desconhecida, levando a

[8] Ver http://www.data4sdgs.org/. Acesso em: 3 maio 2019.

sociedade a preocupar-se com sua minimização, de modo a não comprometer o desenvolvimento social. É nesse contexto que o processo de modernização se torna "reflexivo", representando, a um só tempo, tema e problema (BECK, 2011).

Logo, os benefícios da utilização de *big data* pelo poder público devem ser analisados conjuntamente com os riscos dela decorrentes em relação à privacidade dos indivíduos, sobretudo para avaliar as medidas que são utilizadas para mitigá-los. Essa é a maneira correta de identificar quais modelo de proteção (e governança) as autoridades públicas devem seguir, de forma a maximizar os efeitos positivos do acesso a *big data*, prevenindo eventuais prejuízos que podem ser gerados a partir da informação.

2 RISCOS ENVOLVIDOS NO ACESSO E NO ARMAZENAMENTO DE *BIG DATA* PELO PODER PÚBLICO

Independentemente de o acesso a dados ter se originado de parcerias ou mesmo por conta de pedidos encaminhados por autoridades governamentais, o fato é que operações envolvendo tratamento de dados pessoais pelo poder público podem gerar riscos. Talvez o exemplo mais hiperbólico desses riscos se refira ao vazamento maciço de dados pessoais que decorreu a partir das denúncias formuladas pelo ex-técnico da Central Intelligence Agency (CIA), Edward Snowden, que, em 2013, revelou detalhes de programas de vigilância utilizados pelos Estados Unidos da América para espionar a população norte-americana e diversos países da Europa e da América Latina, entre eles o Brasil, o que incluiu o monitoramento de conversas da ex-presidente Dilma Rousseff, além da coleta indiscriminada de dados pessoais de cidadãos brasileiros (BAUMAN et al., 2014).

No entanto, o perfil dos riscos associado ao tratamento de dados pessoais pelo poder público não se limita a possibilidades de vigilância e exposição indevida da intimidade dos indivíduos, o que, por si só, já é algo grave. Existem preocupações das mais diversas, variando de desequilíbrios nas relações de poder entre governos, empresas e indivíduos, a até mesmo possibilidades de classificações, perfilamento (*profiling*) racial ou social, que podem levar à discriminação, segmentação, supercriminalização e outras restrições de liberdades (POLONETSKY; TENE, 2013), com graves consequências comerciais e sociais.

Mas não é só. Os dados pessoais mantidos por empresas privadas aos quais o governo possa pretender ter acesso podem também representar, por vezes, informações confidenciais dessas empresas, protegidas de forma autônoma como segredos de negócio, construídos a partir do desenvolvimento de atividades no segmento durante longo período. É o caso, por exemplo, de bases

de clientes ou fornecedores, bem como de informações que possam gerar vantagem competitiva no mercado. O vazamento desses dados pode causar danos de difícil reparação às empresas titulares das informações confidenciais.

A necessidade de regras protetivas e de uma governança específica para lidar com os riscos apresentados acima surge a partir de uma conclusão bastante relevante: a possibilidade de anonimização pode ser insuficiente para evitá-los. A anonimização é costumeiramente mencionada como a recomendação a ser seguida para mitigar os riscos à privacidade no tratamento de *big data*, a fim de que não seja possível identificar os titulares dos dados que integram o montante coletado (TENE; POLONETSKY, 2012). Apenas para tangibilizar o resultado do processo, a forma tradicional para atingir esse propósito é remover informações pessoais que possam gerar identificação, tais como nome, endereço e números de documentos como carteira de identidade, carteira de trabalho e CPF (ALTMAN et al., 2014). Entretanto, esse processo pode não ser suficiente para evitar os riscos associados.

As dúvidas sobre o processo de anonimização como forma de proteção contra os riscos de uso de dados pessoais não vêm de hoje. No final da década de 1990, Latanya Sweeney, professora da Universidade de Carnegie Mellon, demonstrou como identificar o registro do então governador de Massachusetts pelo conjunto de dados médicos anonimizados, por meio da análise combinada de informações como sexo, código postal e data de nascimento com registros de eleitores disponíveis publicamente (SWEENEY, 2005). Em geral, poucas características são necessárias para identificar uma pessoa[9]. Nos Estados Unidos, 87% da população pode ser identificada pelo uso de data de nascimento, gênero e pelos cinco dígitos do código postal. Ainda, metade da população dos Estados Unidos pode ser identificada com dados referentes à cidade de residência, sexo e data de nascimento (SWEENEY, 2000).

A partir do cruzamento de informações sobre a localização de pessoas no espaço e no tempo (a exemplo dos dados obtidos pelo aplicativo Waze) é possível identificar 95% dos indivíduos (DE MONTJOYE et al., 2013). A rigor, atualmente não existe um método que permita que dados detalhados de localização sejam anonimizados e publicados com segurança (ALTMAN et al., 2014)[10].

[9] Em pesquisa similar, Arvind Narayanan e Vitaly Shmatikov, na Universidade do Texas, conseguiram demonstrar a possibilidade de identificação de usuários do Netflix, serviço que, à época, era de entrega de DVDs e hoje é de *streaming* (NARAYANAN; SHMATIKOV, 2008).

[10] Em 2018, pesquisadores do Beijing National Research Center for Information Science and Technology realizaram estudo demonstrando a vulnerabilidade da anonimização de dados de mobilidade de indivíduos. Por meio de experimentos, foi possível individualizar a trajetória de usuários de telefones celulares com um grau de precisão entre 73% e 91% de milhares de indivíduos (TU et al., 2018).

Mesmo a utilização de dados estatísticos agregados pode resultar na exposição de dados pessoais. O Escritório Central de Estatísticas de Israel forneceu mecanismo público *online* para consultas a estatísticas agregadas sobre os resultados de pesquisas, e estudantes da Universidade de Tel Aviv conseguiram individualizar diversas pessoas com base nesses dados. Nas pesquisas, havia perguntas como "quantas vezes você já foi casado?", "você foi molestado sexualmente nos últimos 12 anos?" e "quais foram seus rendimentos brutos no último mês?" Os estudantes conseguiram identificar os indivíduos a partir de perfis de resposta ou por meio de referências cruzadas com outras bases de dados (AMITAL, 2013).

Além disso, os riscos associados ao uso e armazenamento de dados pessoais aumentam ao longo do tempo. Isso porque dados armazenados por um longo tempo por vezes são utilizados em comparação com outras bases de dados, o que aumenta o risco de identificação de pessoas específicas (TORRA, 2016), sobretudo ao se levar em consideração a evolução da tecnologia: há algoritmos de inferência efetiva que verificam informações sensíveis como a orientação sexual ou filiação política e religiosa de determinado indivíduo. A análise de curtidas em publicações em redes sociais também pode ser utilizada para prever automaticamente e com precisão uma série de atributos pessoais altamente sensíveis, como orientação sexual, etnia, visões religiosas e políticas, traços de personalidade, inteligência, grau de felicidade, uso de substâncias viciantes, estado civil, idade e sexo (KOSINSKI; STILLWELL; GRAEPEL, 2013).

Assim, levando-se em consideração que existem vários riscos associados ao uso e armazenamento de dados pessoais, sendo certo ainda que medidas de anonimização podem ser insuficientes para eliminar tais riscos em casos específicos, como demonstrado amplamente acima, é necessário verificar quais seriam os limites ao poder governamental de requisição de *big data* (ou mesmo condições precedentes para a celebração de parcerias que envolvam a transmissão de dados pessoais em formato de *big data* por parte de empresas privadas para autoridades governamentais).

3 MARCO REGULATÓRIO E ACESSO A *BIG DATA* POR ENTIDADES GOVERNAMENTAIS

Tradicionalmente, os limites associados ao acesso (normalmente, via requisição) de dados pessoais por parte do poder público estão fundados numa análise relacionada ao escopo do poder de polícia. Apenas para relembrar o conceito a partir do qual a análise sobre limites será feita, quando uma empresa privada exerce atividade econômica que possui fortes liames com as necessidades da

coletividade, o Estado pode estabelecer obrigações para que o ente particular contribua para o interesse público setorialmente definido (ARAGÃO, 2007).

Dessa forma, por meio do poder de polícia, o Estado pode, em tese, impor a empresas privadas obrigações de compartilhamento de dados, incluindo *big data*. Tal atuação estatal, contudo, não se dá sem limites, pois o poder de polícia, conquanto seja discricionário, não é arbitrário. O Estado deve sempre observar os ideais do bem comum e ainda está sujeito aos princípios da legalidade e da moralidade administrativa, "devendo respeitar os direitos do cidadão, as prerrogativas individuais e as liberdades públicas" (LAZZARINI, 1994). Vale notar que, na definição trazida pelo Código Tributário Nacional, o exercício do poder de polícia somente é considerado regular "quando desempenhado pelo órgão competente nos limites da lei aplicável, com observância do processo legal e, tratando-se de atividade que a lei tenha como discricionária, sem abuso ou desvio de poder"[11].

Os direitos fundamentais, como é o caso da garantia constitucional de inviolabilidade da intimidade, vida privada, honra e imagem das pessoas[12], podem exercer eficácia bloqueadora do exercício do poder de polícia. A literatura especializada indica que tal situação pode ocorrer em três hipóteses: (*i*) quando a medida de polícia contrariar frontal e literalmente o âmbito de proteção de um direito fundamental; (*ii*) quando a pretensão ordenadora não ultrapassar as máximas inerentes ao dever de proporcionalidade; e (*iii*) quando o exercício da competência ordenadora reduzir, efetiva ou potencialmente, o direito fundamental aquém de um mínimo, desfigurando-o ou anulando-o (BINENBOJM, 2017).

Assim, diante de doutrinas mais tradicionais, para que o Estado possa, por meio do poder de polícia, exigir o compartilhamento de dados pessoais por particulares, é necessária a clara demonstração do interesse público a ser atingido. Ainda, o pedido deve ser emanado de órgão competente, respeitando princípios constitucionais, sem abuso ou desvio de poder e, sobretudo, levando em consideração que a privacidade é um direito fundamental, que não pode ser violado a pretexto de se satisfazer o interesse público.

Esses limites ao poder de polícia, no entanto, são insuficientes para endereçar de maneira adequada os riscos identificados na seção anterior, o que gerou movimentos legislativos que

[11] BRASIL. Lei nº 5.172, de 25 de outubro de 1966, art. 78: "Considera-se poder de polícia atividade da administração pública que, limitando ou disciplinando direito, interêsse ou liberdade, regula a prática de ato ou abstenção de fato, em razão de intêresse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de concessão ou autorização do Poder Público, à tranqüilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos. Parágrafo único. Considera-se regular o exercício do poder de polícia quando desempenhado pelo órgão competente nos limites da lei aplicável, com observância do processo legal e, tratando-se de atividade que a lei tenha como discricionária, sem abuso ou desvio de poder".

[12] BRASIL. Constituição Federal, art. 5º, X.

construíram regras gerais, desenhando, inclusive, um modelo de governança que provavelmente está mais correspondente ao universo do *big data*, não dependendo, portanto, de legislações específicas relacionadas a marcos regulatórios, tal como aquele que está descrito na introdução deste artigo, tratando de aplicações de transporte urbano. Além dos limites ao uso do poder de polícia, existem outros conectados à ideia de proteção da privacidade e segurança dos indivíduos titulares dos dados pessoais, impondo soluções ativas de governança para viabilizar o acesso a dados, além de obrigações direcionadas a órgãos públicos que pretendem tratar *big data*, a fim de assegurar os objetivos a serem alcançados por meio do tratamento desses dados, de modo que não haja ineficiência ou ineficácia do uso das informações ao não se saber onde se quer chegar (GIEST, 2017).

3.1 LIMITES IMPOSTOS PELO MARCO CIVIL DA INTERNET E SEU DECRETO REGULAMENTADOR

O Marco Civil da Internet e seu decreto regulamentador (Decreto nº 8.771/2016) trazem disposições que limitam a atuação do poder público quando da requisição de dados pessoais a entes privados, dando início a um novo modelo de acesso a dados. O art. 10, § 1º, do Marco Civil estabelece que os provedores de aplicações de internet somente serão obrigados a disponibilizar os registros de conexão e de acesso dos usuários, de forma autônoma ou associados a outros dados pessoais, mediante ordem judicial. Já nos termos do art. 10, § 3º, dados cadastrais que informem qualificação pessoal, filiação e endereço somente podem ser solicitados, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

O mesmo decreto regulamentador traz ainda previsão importante acerca da governança dos pedidos de dados pessoais realizados por entes públicos. O art. 12 do Decreto nº 8.771/2016 determina que todos os órgãos da administração pública federal deverão publicar anualmente na internet relatórios estatísticos de requisição de dados cadastrais, contendo: (*i*) o número de pedidos realizados; (*ii*) a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; (*iii*) o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e (*iv*) o número de usuários afetados por tais solicitações. Contudo, dois anos após a entrada em vigor do referido decreto, o centro de pesquisa Internetlab divulgou levantamento expondo que o dever de transparência vem sendo negligenciado por parte das autoridades federais, que não disponibilizam as informações ao público (ABREU; MASSARO, 2018).

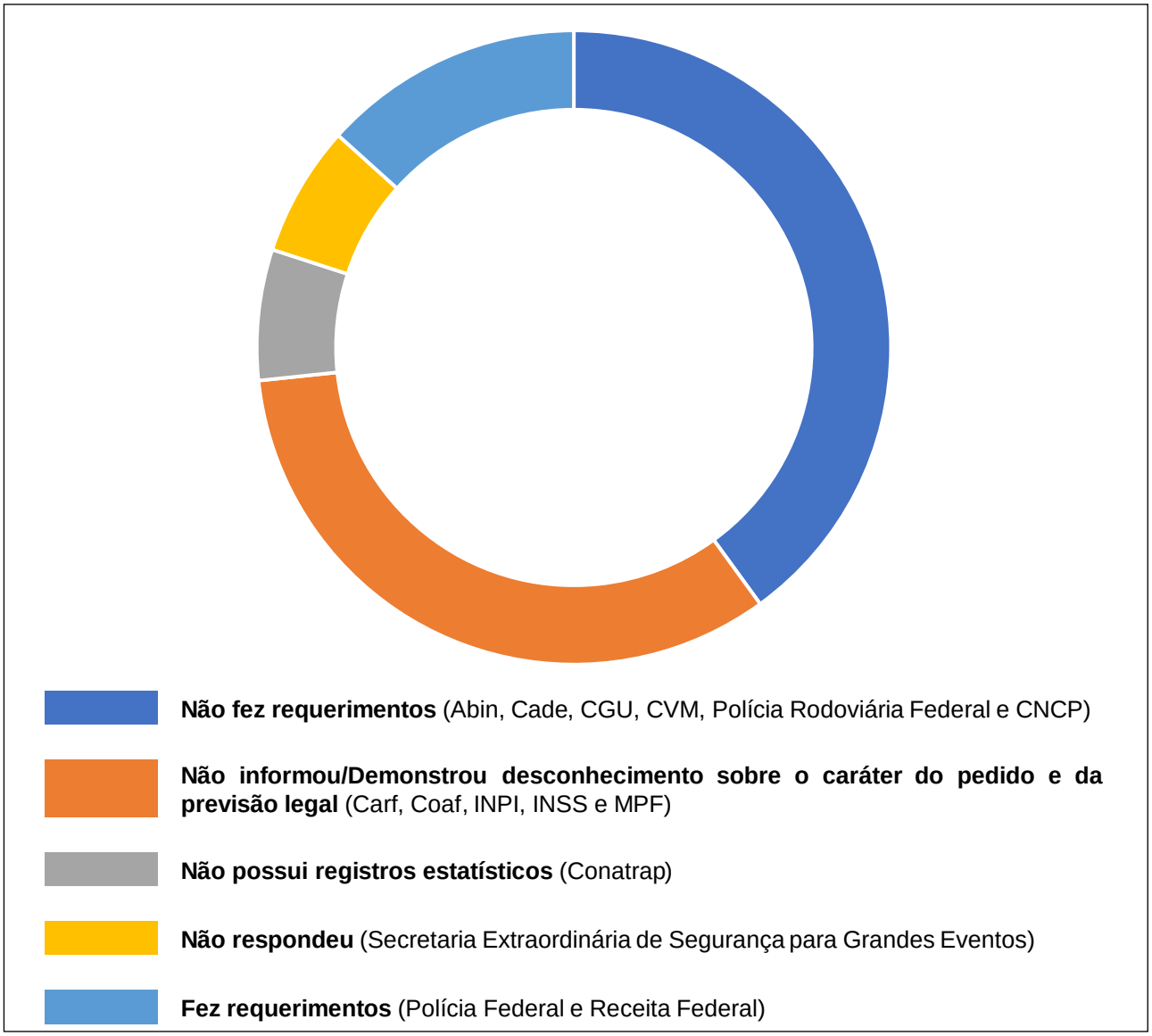
Com base na Lei de Acesso à Informação, o Internetlab consultou diferentes órgãos da administração pública federal indagando a respeito do cumprimento do dever previsto no art. 12 do

Decreto nº 8.771/2016. Os seguintes órgãos foram consultados pelo centro de pesquisa em direito e tecnologia: Abin, Cade, Carf e Coaf, CGU, CVM, INPI, INSS, MPF, Polícia Federal, Polícia Rodoviária Federal, Receita Federal, Comitê Nacional de Enfrentamento ao Tráfico de Pessoas, Conselho Nacional de Combate à Pirataria e Secretaria Extraordinária de Segurança para Grandes Eventos.

De todos os órgãos, apenas a Polícia Federal e a Receita Federal disponibilizaram as informações requeridas. Todavia, a Polícia Federal forneceu informações sem o grau de detalhamento exigido pelo Decreto, enquanto a Receita, conquanto tenha fornecido as informações detalhadas, não especificou os períodos. Os demais órgãos informaram não terem feito requerimentos (Abin, Cade, CGU, CVM, Polícia Rodoviária Federal e Conselho Nacional de Combate à Pirataria) ou não apresentaram as informações requeridas/demonstraram desconhecimento sobre o caráter do pedido e da previsão legal (Carf e Coaf, INPI, INSS e MPF[13], Comitê Nacional de Enfrentamento ao Tráfico de Pessoas e Secretaria Extraordinária de Segurança para Grandes Eventos). A partir do Gráfico 2, é possível entender o *status* do cumprimento da legislação:

[13] O Ministério Público Federal não é parte da administração pública, mas foi incluído na pesquisa por se enquadrar como autoridade "administrativa" no âmbito do Marco Civil. O órgão informou estatísticas sobre interceptações telefônicas.

Gráfico 2 – Cumprimento do dever de informação por órgãos federais



Fonte: autoria própria, a partir de dados coletados em Abreu; Massaro (2018).

3.2 LIMITES IMPOSTOS PELA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Em 2018, foi promulgada no Brasil a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), com o objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", criando um marco regulatório específico sobre dados no Brasil. A legislação coloca o indivíduo no seu centro, conferindo-lhe uma série de direitos. Não é por acaso o uso do termo "proteção" no título da Lei; ela efetivamente busca empoderar as pessoas físicas, que têm seus dados pessoais cotidianamente tratados por diferentes empresas com fins econômicos. De acordo com a LGPD, os dados pertencem ao indivíduo a quem

se referem, tanto que este é designado pela lei como "titular". Ao indivíduo, portanto, cabe a tomada de decisões acerca do que pode ser feito com seus dados pessoais, com base na autodeterminação informativa, um dos fundamentos da lei.

A LGPD disciplina o tratamento de dados pessoais pelo poder público no seu capítulo IV, destacando que ele "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". A lei estabelece duas condições para que tal tratamento ocorra. A primeira é de que as pessoas jurídicas de direito público informem as hipóteses em que realizam o tratamento de dados pessoais, fornecendo informações claras, atualizadas e acessíveis sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desse tratamento. Ou seja, tal como as instituições privadas, o poder público igualmente deve apresentar uma finalidade clara e transparente para efetuar o tratamento de dados pessoais, que deve ter por base a perseguição do interesse público (PINHEIRO, 2018).

Ou seja, não pode o Estado simplesmente alegar, de forma genérica, que pretende receber dados pessoais para alcançar o interesse público, sem definir concretamente em que reside tal interesse. A finalidade do tratamento deve ser claramente demonstrada. Tal medida, aliás, é o que possibilita a avaliação com base no dever de proporcionalidade, uma vez que, como visto, a privacidade é um direito fundamental e, nessa condição, pode limitar o exercício do poder de polícia emanado pelo Estado. Se o poder público não especificar a finalidade que pretende dar ao tratamento de dados, não será possível avaliar sua necessidade, adequação e proporcionalidade em sentido estrito.

A segunda condição prevista na LGPD para o tratamento de dados pessoais por pessoas jurídicas de direito público é que estas indiquem um encarregado, que, nos termos da lei, é quem deve atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), órgão regulador criado pela LGPD (LEMOS et al., 2018). Da mesma forma, trata-se de equiparação com obrigação que é exigida de entes privados, basicamente equiparando agentes particulares e públicos a esse respeito.

O artigo 41 da LGPD prevê que o controlador, definido como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", deverá indicar encarregado pelo tratamento de dados pessoais. A identidade do encarregado e as suas informações de contato deverão ser públicas, estando disponíveis de forma clara e objetiva, de preferência no sítio eletrônico do controlador. Em princípio, qualquer operação que envolva tratamento de dados pessoais e que seja alcançada pela LGPD deverá contar com o

envolvimento de um encarregado. A ANPD, contudo, poderá estabelecer hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

A figura do encarregado, presente na LGPD, é inspirada no Data Protection Officer (DPO) previsto na regulamentação europeia, a General Data Protection Regulation – GDPR. Trata-se de um dos mecanismos criados pela União Europeia para garantir o cumprimento da norma regulamentadora por aqueles que estão a ela submetidos. De acordo com a GDPR, os responsáveis pelo tratamento e processamento de dados pessoais – tanto entes privados, quanto entes públicos – deverão possuir em seus quadros um DPO. Assim como na legislação brasileira, o DPO, entre outras atividades, é responsável pelo aconselhamento sobre as normas vigentes relativas à proteção de dados pessoais, o monitoramento do cumprimento das normas legais e regulatórias pela entidade a que está vinculado e a cooperação com as autoridades públicas supervisoras da norma.

Além das duas condições estabelecidas inicialmente pela LGPD (mais especificamente, as obrigações de justificativa do interesse público que motiva o pedido e de indicação de um encarregado pelo tratamento e armazenamento dos dados), existe um outro ponto, desta vez menos explícito, que pode representar um limite ao poder público para a solicitação de dados pessoais, incluindo-se aí *big data*: a demonstração de capacidade dos órgãos públicos de realizarem o tratamento adequado dos dados pessoais.

A literatura internacional já sustenta que pode haver governos que não possuem nem sequer capacidade de analisar os dados que pretendem receber, havendo o risco de incorporar conhecimento científico de forma ineficiente dentro do processo de tomada de decisão (GIEST, 2017). De fato, a LGPD prevê, em seu art. 18, IV, que o titular tem o direito à eliminação dos dados pessoais desnecessários ou excessivos. Se o órgão público não tem condições técnicas de realizar o tratamento, parece razoável supor que ele não poderá requerer a posse ou manutenção dos dados, inclusive porque, pelo princípio da necessidade (LGPD, art. 6º, III), qualquer operação de tratamento de dados pessoais deve se limitar ao mínimo necessário para a realização de suas finalidades. Nenhum ente particular deve ser obrigado a atender requisições de dados pessoais se a autoridade solicitante não dispuser dos conhecimentos e das ferramentas necessárias para garantir que o tratamento ocorra com segurança, requisito esse que se soma à presença de um encarregado.

4 CONCLUSÕES

Em janeiro de 2014, o Office of Science and Technology Policy, órgão integrante do governo norte-americano, divulgou consulta pública por meio da qual solicitou informações sobre como o *big data* afetará como os americanos vivem e trabalham, além das implicações decorrentes da coleta, análise e uso dessas informações, à privacidade, economia e política pública (ALTMAN et al., 2014). A ideia dessa consulta pública consistiu em buscar informações para padronizar a forma de gerenciar *big data* tendo em vista as finalidades acima, viabilizando a antecipação de tendências, tanto para o setor público, como para o privado.

Embora não seja suficiente para fixar um marco temporal, parece claro que existiram diferentes ciclos de motivação para o acesso, pelo poder público, de dados pessoais (e a consulta pública acima marca o início do interesse governamental em *big data* para políticas públicas de uma maneira mais sistematizada): (*i*) num primeiro momento, o foco se centrou em informações que poderiam revelar possíveis indícios de atividades terroristas de grande porte; (*ii*) num segundo momento, os pedidos de dados pessoais, agora submetidos a decisões judiciais prévias, instrumentalizaram ações públicas mais direcionadas (como, por exemplo, a produção de provas para a condenação de um determinado indivíduo num caso concreto). Esse último ciclo, em vigor ainda hoje, levou a uma enorme proliferação de pedidos de dados pessoais, devidamente relatados pelas principais empresas de tecnologia em relatórios anuais e em páginas da internet.

Este artigo procurou demonstrar que a nova tendência governamental, marcada pela consulta pública acima mencionada, de procurar *big data* como fonte matricial de decisões de políticas públicas, o que também já se reflete, ainda que inicialmente, no Brasil, faz repensar a estrutura de proteção moldada para garantir direitos individuais, sobretudo em um mundo em que a tecnologia evolui de maneira bastante agressiva, inclusive para tornar a anonimização um empreendimento mais difícil e de resultado não necessariamente confiável, tendo em vista a possibilidade de cruzamento de bases de dados.

Dessa forma, a proteção de direitos fundamentais a partir das limitações tradicionais ao poder de polícia pode ser insuficiente para viabilizar os efeitos positivos da justificada utilização de *big data* por autoridades públicas, pois devem-se impedir (ou mitigar de forma satisfatória) os riscos que decorrem de vazamentos ou tratamentos inadequados para as bases de dados que passam a ser tratadas e armazenadas por agentes públicos, que incluem possíveis impactos para pessoas, relações comerciais e mesmo para questões políticas, como o equilíbrio democrático das instituições.

Com essa finalidade, duas legislações entraram em vigor, de forma a dar tratamento mais específico ao acesso a dados pessoais, o que inclui uma série de limites endereçados a agentes públicos que requerem *big data* para empresas privadas de tecnologia que coletam, usam e armazenam dados que possuem natureza sensível. Além de obrigações associadas à transparência, envolvendo funções ativas de justificação de finalidades e uso dos dados, essas legislações impõem regimes de governança rígidos para permitir que uma autoridade governamental possa ter acesso a *big data* produzidos por agentes privados, sendo necessário inclusive demonstrar a capacidade de processar a informação solicitada: o poder público não está autorizado a solicitar dados pessoais se não tiver capacidade técnica de realizar o tratamento dos dados recebidos e armazená-los com segurança, garantindo-lhes confidencialidade. Dessa forma, a simples alegação de busca por interesse público não irá legitimar o poder de polícia do poder público, que deverá ter uma governança ativa suficiente a proteger e processar de maneira pertinente à finalidade pública os dados pessoais requeridos, sob pena de ter o seu pedido devidamente negado.

Em particular, é interessante ver que a LGDP equiparou agentes públicos a privados na obrigação constante da indicação de um encarregado, este responsável por diversas funções, entre as quais: (*i*) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, (*ii*) receber comunicações da autoridade nacional e adotar providências, (*iii*) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, e (*iv*) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. É recomendável a inclusão de dever de sigilo ao encarregado pelo tratamento e a todos aqueles que tenham acesso aos dados pessoais tratados.

Não obstante, embora tenha significado avanços em obrigações estruturais, diversos órgãos da administração pública vêm descumprindo determinação do Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet, quanto à publicação de relatórios estatísticos de requisição de dados cadastrais, determinação essa estabelecida para viabilizar a transparência e possibilitar o controle sobre os pedidos de dados, o que naturalmente inclui pedidos de acesso a *big data*.

REFERÊNCIAS

ABREU, Jacqueline de Souza; MASSARO, Heloisa. Marco Civil da Internet e transparência: resultados de pedidos de acesso à informação sobre quebras de sigilo de dados cadastrais.

Internetlab, [*s. l.*], Privacidade e Vigilância, 4 jun. 2018. Disponível em: https://bit.ly/2QZP7Tl. Acesso em: 16 mar. 2019.

AIRBNB e Santa Catarina assinam acordo para promover turismo responsável. Airbnb, [*s. l.*], News, Política, 21 jun. 2018. Disponível em: https://bit.ly/3uq7iiF. Acesso em: 1 maio 2019.

ALTMAN, Micah *et al*. **Big Data Study; Request for Information** [reply]. Destinatário: The White House Office of Science and Technology Policy (OSTP). [*S. l.*], 31 mar. 2014. 1 mensagem eletrônica. Disponível em: https://bit.ly/3oZP46G. Acesso em: 24 fev. 2019.

AMITAI, Ziv. Israel's 'Anonymous' Statistics Surveys Aren't So Anonymous. **Haaretz**, [*s. l.*], Home, 7 jan. 2013. Disponível em: https://bit.ly/3yL1kMQ. Acesso em: 13 mar. 2019.

ARAGÃO, Alexandre Santos de. **Direito dos serviços públicos**. Rio de Janeiro: Forense, 2007.

BAUMAN, Zygmunt *et al*. After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology**, [*s. l.*], v. 8, n. 2, p. 121-144, 2014.

BECK, Ulrich. **Sociedade de risco**: Rumo a uma Outra Modernidade. Tradução Sebastião Nascimento. São Paulo: Editora 34, 2011.

BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação**. Belo Horizonte: Fórum, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Diário Oficial da União, 5 out. 1988. Disponível em: https://bit.ly/3paUUlX. Acesso em: 25 abr. 2021.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, […]. Brasília, DF: Diário Oficial da União, 11 maio 2016 – Edição extra. Disponível em: https://bit.ly/3wFth6N. Acesso em: 25 abr. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Diário Oficial da União, 24 abr. 2014a. Disponível em: https://bit.ly/3wF3RGn. Acesso em: 24 abr. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Brasília, DF: Diário Oficial da União, 15 ago. 2018, republicado parcialmente em 15 ago. 2018 – Edição extra. Disponível em: https://bit.ly/3oXF4e2. Acesso em: 25 abr. 2021.

BRASIL. **Lei nº 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília, DF: Diário Oficial da União, 27 out. 1966, retificado em 31 out. 1966. Disponível em: https://bit.ly/3fwquY5. Acesso em: 24 abr. 2021.

BRASIL. Superior Tribunal de Justiça (Terceira Turma). **REsp nº 1417641/RJ**. Civil e consumidor. Internet. Provedor de conteúdo. Usuários. Identificação. Dever. Guarda dos dados. Obrigação. Prazo. Terceira Turma. Relatora: Ministra Nancy Andrighi. Decisão: 25/02/2014. DJe 10/03/2014b. Disponível em: https://bit.ly/3fwtvYs. Acesso em: 24 abr. 2021.

COOPERATION or Resistance?: The Role of Tech Companies in Government Surveillance. Harvard Law Review, [*s. l.*], v. 131, p. 1.722-1.741, 2018. Disponível em: https://bit.ly/3c2q0GN. Acesso em: 8 mar. 2019.

DAAS, Piet; LOO, Mark van der. Big Data (and official statistics). United Nations Economic Commission for Europe (ECE). Conference of European Statisticians. **Meeting on the Management of Statistical Information Systems (MSIS 2013)**. (Paris, France, and Bangkok, Thailand, 23-25 April 2013). Working Paper, 11 April 2013. Disponível em: https://bit.ly/3uEKex3. Acesso em: 1 maio 2019.

DE MONTJOYE, Yves-Alexandre *et al*. Unique in the Crowd: The privacy boundsof human mobility. **Nature**, [*s. l.*], Scientific Reports, v. 3, Article number 1.376, 2013. DOI: 10.1038/srep0137. Disponível em: https://go.nature.com/3p08U1z. Acesso em: 13 mar. 2019.

DUBUQUE, Iowa and IBM Combine Analytics, Cloud Computing and Community Engagement to Conserve Water. IBM, [*s. l.*], IBM News Room, 20 maio 2011. Disponível em: https://ibm.co/3p1vyH6. Acesso em: 25 abr. 2021.

GIEST, Sarah. Big data for policymaking: fad or fasttrack? **Policy Sciences**, [*s. l.*], v. 50, p. 367-382, 2017. DOI 10.1007/s11077-017-9293-1. Disponível em: https://bit.ly/2RRDSgh. Acesso em: 25 fev. 2019.

GOVERNMENT Requests for User Data. Facebook, [*s. l.*]. Transparency Center. Home. Data. Government Requests for User Data. Brazil. 2019. Disponível em: https://bit.ly/34sFyQa. Acesso em: 9 mar. 2019.

JAEGER, Paul T.; BERTOT, John Carlo; MCCLURE, Charles R. The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. **Government Information Quarterly**, [*s. l.*], v. 20, p. 295-314, 2003. Disponível em: https://bit.ly/3c0Npsg. Acesso em: 9 mar. 2019.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **PNAS**, [*s. l.*], v. 110, n. 15, p. 5.802-5.805, 2013. Disponível em: https://bit.ly/3fUaZrS. Acesso em: 13 mar. 2019.

LAZZARINI, Álvaro. Limites do poder de polícia. **Revista de Direito Administrativo**, [*s. l.*], v. 198, p. 69-83, 1994.

LEMOS, Ronaldo *et al*. A criação da Autoridade Nacional de Proteção de Dados pela MP nº 869/2018. **JOTA**, [*s. l.*], Opinião & Análise, 29 dez. 2018, atualizado em 30 dez. 2018. Disponível em: https://bit.ly/2RKysUr. Acesso em: 26 jan. 2019.

MEGAVAZAMENTO de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. G1, [*s. l.*], Economia, Tecnologia, 28 jan. 2021. Disponível em: https://glo.bo/3vyrS1L. Acesso em: 24 abr. 2021.

MOREIRA, Marli. Prefeitura de SP faz parceria com aplicativo Waze para melhorar o trânsito. **Agência Brasil**, [*s. l.*], Geral, 20 set. 2017. Disponível em: https://bit.ly/34rh0a1. Acesso em: 3 maio 2019.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Sparse Datasets. **2008 IEEE Symposium on Security and Privacy (sp 2008)**, [*s. l.*], p. 111-125, 2008. DOI: 10.1109/SP.2008.33. Disponível em: https://bit.ly/2R1kg8Z. Acesso em: 13 mar. 2019.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

POELA, Martijn *et al*. **Data for Policy**: A study of big data and other innovative data-driven approaches for evidence-informed policymaking. Draft report about the State-of-the-Art: invitation for reflection. Centre for European Policy Studies. Oxford Internet Institute. University of Oxford. Technopolis [group]. 11 May 2015. Disponível em: https://bit.ly/2RKPAtd. Acesso em: 20 fev. 2019.

POLONETSKY, Jules; TENE, Omer. Privacy and Big Data: Making Ends Meet. **Stanford Law Review Online**, [*s. l.*], v. 66, p. 25-33, 2013.

PORCHE, Isaac R. *et al*. **Data Flood**. Helping the Navy Address the Rising Tide of Sensor Information. [*S. l.*]: RAND Corporation, 2014. Disponível em: https://bit.ly/34pVPoG. Acesso em: 12 mar. 2019.

PREFEITURA de São Paulo anuncia parceria com Waze. Cidade de São Paulo, [São Paulo], Secretaria Especial de Comunicação, Notícias, 20 set. 2017. Disponível em: https://bit.ly/3fQscSU. Acesso em: 9 mar. 2019.

PREFEITURA do Rio de Janeiro usa Waze para monitorar o trânsito na cidade. Canaltech, [*s. l.*], Redação, 25 jul. 2013. Disponível em: https://bit.ly/3fwq8Ao. Acesso em: 9 mar. 2019.

RUBINSTEIN, Ira S. Big Data: The End of Privacy or a New Beginning? (October 5, 2012). **International Data Privacy Law (2013 Forthcoming)**, [*s. l.*], NYU School of Law, Public Law Research Paper No. 12-56.

SÃO PAULO (Município). Comitê Municipal de Uso do Viário. **Resolução nº 13, de 18 de novembro de 2016**. Regulamenta o parágrafo único do art. 35º do Decreto no 56.981, de 10 de maio de 2016, em relação à gestão […]. São Paulo: Diário Oficial da Cidade de São Paulo, 25 nov. 2016. Disponível em: https://bit.ly/2QZT5eK. Acesso em: 24 abr. 2021.

SÃO PAULO (Município). Comitê Municipal de Uso do Viário. **Resolução nº 16, de 07 de julho de 2017**. Regulamenta os requisitos mínimos exigidos para cadastramento de condutores nas Operadoras de Tecnologia de Transporte Credenciadas […]. São Paulo: Diário Oficial da Cidade de São Paulo, 12 jul. 2017, republicação em 13 jul. 2017. Disponível em: https://bit.ly/3vvLofx. Acesso em: 24 abr. 2021.

SWEENEY, Latanya. **Privacy Technologies for Homeland Security**. Statement of Latanya Sweeney, PhD (Associate Professor of Computer Science, Technology and Policy; Director, Data Privacy Laboratory; Carnegie Mellon University), before the Privacy and Integrity Advisory Committee of the Department of Homeland Security ("DHS"). 15 jun. 2005. Disponível em: https://bit.ly/2RMzeAi. Acesso em: 13 mar. 2019.

SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely. **Carnegie Mellon University**, Pittsburgh, Data Privacy Working Paper 3, 2000. Disponível em: https://bit.ly/3uvjtLh. Acesso em: 13 mar. 2019.

TENE, Omer; POLONETSKY, Jules. Privacy in the Age of Big Data. A Time for Big Decisions. **Stanford Law Review**, [*s. l.*], v. 64, 2012.

TORRA, Vicenç; NAVARRO-ARRIBAS, Guillermo. Big Data Privacy and Anonymization. *In*: LEHMANN, Anja *et al*. (ed.). **Privacy and Identity Management**. Facing up to Next Steps. Karlstad: Springer, 2016. p. 15-26. Disponível em: https://bit.ly/2R6zolG. Acesso em: 25 fev. 2019.

TU, Zhen *et al*. A New Privacy Breach: User Trajectory Recovery From Aggregated Mobility Data. **IEEE/ACM Transactions on Networking**, [*s. l.*], v. 26, n. 3, p. 1.446-1.459, 2018. DOI: 10.1109/TNET.2018.2829173. Disponível em: https://bit.ly/3ft2WmI. Acesso em: 28 abr. 2019.

WAZE for cities. **Waze**, [*s. l.*], 7 jan. 2019. Disponível em: https://bit.ly/2R6BVwc. Acesso em: 3 maio 2019.