



Brasilizada da proteção de dados



No dia 17 de abril, o governo editou a Medida Provisória

nº 954, que determinou o compartilhamento de dados não anonimizados de telefonia fixa e móvel e o endereço de todos os brasileiros com o IBGE.

Imediatamente, foram propostas perante o Supremo Tribunal Federal cinco ações de inconstitucionalidade (ADIs) por PSB, PSDB, PSOL, PCdoB e pela Ordem dos Advogados do Brasil (OAB). As entidades defendem que o referido compartilhamento traz graves riscos para a privacidade dos cidadãos e para a própria democracia brasileira, violando o artigo 5º, incisos X, XII e LXXII da Constituição Federal.

A partir daí, deu-se um embate entre as visões, que defendiam, por um lado, a necessidade de acesso aos dados para a realização de pesquisas pelo IBGE durante a pandemia e, por outro, as fragilidades da norma passíveis de expor os dados de milhões de brasileiros a medidas de vigilância. Em defesa da Medida Provisória manifestaram-se os ex-presidentes do IBGE, no sentido de que “esta preocupação (com os dados) não se justifica, porque os dados não incluem informações pessoais e serão usados unicamente para fins estatísticos”(1). Mencionaram até mesmo um suposto “apagão estatístico, que tornaria muito mais difícil o controle da epidemia”(2).

Ocorre que no Estado Democrático de Direito as intenções dos entes públicos se manifestam por meio de atos normativos e a Medida Provisória não especifica para quais finalidades os dados serão utilizados para além do abstrato termo “produção estatística oficial”, não estabelece a relação entre as pesquisas estatísticas do IBGE e o combate à pandemia, e muito menos determina qualquer medida de segurança para que o compartilhamento possa se dar sem risco de acessos indevidos.

Mais grave ainda é a desproporcionalidade entre os dados necessários para uma pesquisa amostral e os dados requisitados: determina-se a disponibilização dos dados de todos os brasileiros que tem acesso a telefonia móvel e fixa (mais de 200 milhões), quando a própria Fundação informa na PNAD que “70 mil domicílios por mês fazem parte da amostra pesquisa”3.

Coloca-se em xeque a necessidade desse altíssimo número para alcançar o (incerto) objetivo da norma, o que aliás contraria o Regulamento Sanitário Internacional da OMS, incorporado no ordenamento pátrio pelo Decreto n. 10.212/ 2020, que determina que não devem existir “processamentos [de dados]



desnecessários e incompatíveis”, com o propósito de “avaliação e manejo de um risco para a saúde pública” (art. 45, 2, “a”).

Não há qualquer justificativa também para os exíguos prazos trazidos na MP, a explicar porque de forma tão urgente esses dados devem ser repassados ao IBGE (três dias para a regulamentação pelo IBGE e sete dias para a disponibilização dos dados), antes mesmo da publicação de um relatório de impacto à privacidade, que pudesse demonstrar de forma transparente aos cidadãos os riscos e meios de mitigação.

Ao contrário, a Medida Provisória prevê paradoxalmente a realização de um relatório depois que os dados já tiverem sido repassados!

Espanta ainda mais a lacônica Instrução Normativa nº 2 do IBGE (4), datada do mesmo dia da Medida Provisória, que ao invés de preencher algumas dessas omissões, prevê que a forma de compartilhamento poderá ser escolhida pelas operadoras de telefonia, desde que aceito pelo IBGE.

Assim, a norma do IBGE ignorou as importantes condições recomendadas pela Anatel (5) para a legitimidade do pretendido compartilhamento: (a) “sólida instrumentalização da relação jurídica que será estabelecida entre o IBGE e cada uma das” empresas de telecomunicações; (b) “a delimitação específica da finalidade do uso dos dados solicitados”; (c) “a limitação das solicitações ao universo de dados estritamente necessários para o atingimento da finalidade”; (d) “a delimitação do período de uso e da forma de descarte dos dados”; (e) “a aplicação de boas práticas de segurança, de transparência e de controle”. A despeito da MP expressamente determinar que a Anatel fosse ouvida antes da regulamentação expedida pelo IBGE, é de se estranhar porque nenhuma das medidas sugeridas pela Agência foi implementada na instrução normativa.

Assim, a discussão acerca da constitucionalidade da Medida Provisória é não apenas necessária, como urgente, vez que já nos próximos dias o governo terá em mãos um banco de dados unificado com nome, endereço e telefone fixo e móvel de mais de 200 milhões de brasileiros, sem que a sociedade tenha sido minimamente informada porque esse volume de dados deve ser coletado e quais são as medidas de segurança que serão adotadas para a sua proteção.

Não se trata aqui, por óbvio, de suspeita ou de desconhecer a grande relevância dos serviços prestados pela Fundação IBGE à sociedade brasileira. É dizer: trata-se de desconfiança pelos riscos inerentes que tal medida pode gerar para a liberdade e personalidade dos cidadãos brasileiros, lição civilizatória duramente aprendida com o uso de informações pessoais por regimes autoritários e com os escândalos recentes de vazamento e uso indevido de dados pessoais.(6)

Como afirmou a Corte Constitucional alemã, no famoso julgamento de 1983 que deu origem ao direito à autodeterminação informativa, “não existem mais dados insignificantes no contexto do processamento eletrônico de dados”.

É que um dado sozinho, aparentemente insignificante, pode adquirir um novo valor quando cruzado com outras informações, compartilhado com pessoas ou entidades distintas e, de forma ainda mais sensível, utilizado para formar perfis pessoais, sem participação ou conhecimento do titular desses dados.



Curiosamente, a controvérsia do julgamento alemão tratava da lei do censo de 1982 e era análoga ao presente caso, ao debater o risco da ampla coleta estatal de dados e a possibilidade de cruzamento com outras informações que o Estado já possui. (7)

Na sua formulação de um direito à autodeterminação informativa, a Corte alemã criou verdadeiro marco teórico no campo da proteção de dados pessoais, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo à protagonista no processo de tratamento de seus dados. Esse reconhecimento representa uma limitação ao Poder Legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação informativa, do qual se extraem inúmeros pressupostos procedimentais e limites materiais cujo cumprimento irá determinar se o tratamento de dados é legítimo ou não.

Mais do que isso, os efeitos coletivos que o Tribunal extrai da violação dos dados pessoais são fundamentais, ao afirmar que uma sociedade na qual os cidadãos não detém controle sobre as suas próprias informações coloca em risco o seu próprio sistema democrático, em razão do estado de vigilância permanente trazido por essa situação (8).

Há muito se discute se um direito fundamental à proteção de dados também existe no ordenamento brasileiro. Uma leitura acurada do seu texto permite ver, com clareza, que a Constituição Federal traz normas e princípios aptos a realizar a tutela constitucional dos dados pessoais, como se percebe a partir da interpretação conjunta da garantia da inviolabilidade da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III, CF/88,) e da garantia processual do habeas data (art. 5o, LXXII).

Em acórdão de 2017, o Supremo Tribunal Federal (STF) inovou ao reconhecer em um Recurso Extraordinário em Habeas Data (RE no 673.707) o direito de acesso do contribuinte a um sistema da Receita Federal, o Sistema de Conta Corrente da Secretaria (SINCOR).(9) Essa jurisprudência representa um passo fundamental na consolidação da tutela constitucional dos dados pessoais no Brasil e traz elementos relevantes para a compreensão de um direito material à proteção de dados, decorrente lógico e necessário da garantia processual do habeas data. (10)

Os vícios de inconstitucionalidade, omissões e contradições da MP se mostram ainda mais preocupantes em razão do déficit institucional da proteção de dados no Brasil: afinal, se não há autoridade de proteção de dados no país, quem irá fiscalizar o cumprimento das obrigações estabelecidas pela própria MP, tais como a eliminação das informações obtidas após a sua utilização (art. 4º, caput, da MP)?

Ou quem irá examinar as conclusões e a metodologia desse deficiente relatório de impacto à proteção de dados pessoais elaborado pelo IBGE (art. 3º, §2º, da MP)?

O pano de fundo desse conflito é, em verdade, a enorme fragilidade institucional da proteção de dados no Brasil.

Afinal, o país não tem uma lei geral de proteção de dados em vigor, não conta com o reconhecimento expresso de um direito fundamental à proteção de dados e, de forma ainda mais grave, tampouco possui uma autoridade independente que possa supervisionar o tratamento de dados mencionado pela Medida



Provisória.

Esses requisitos, que formam um relevante tripé institucional da proteção de dados em grandes economias do mundo, são justamente o grande vácuo do ordenamento jurídico-político brasileiro em pleno século XXI. Sem eles, há uma enorme insegurança jurídica no país sobre a coleta, o uso e a transferência de dados, o que explica a intensa judicialização da medida ora proposta relativa ao compartilhamento de dados com o IBGE.

E é exatamente o momento atual de grave crise epidêmica, social e econômica que escancara a debilidade de nosso sistema institucional de proteção de dados.

Surpreende nesse contexto a prorrogação da LGPD pelo Senado Federal, justamente no momento em que mais precisamos da coleta e do uso de dados com base em parâmetros legais, que forneçam segurança jurídica para o Estado e para as empresas.

É fácil perceber que o Brasil se encontra diante de uma verdadeira encruzilhada institucional: quando mais precisamos coletar e processar dados pessoais relacionados à saúde pública dos cidadãos a fim de formular políticas públicas aptas a protegê-los, não temos balizas jurídicas para garantir segurança desse processamento, cenário no qual se destaca a omissão do Poder Executivo em constituir uma autoridade nacional de proteção de dados de dados.

Nesse sentido, para além de prevenir os possíveis riscos gerados pela Medida Provisória, as ADIs se mostram também como uma oportunidade de instituir os parâmetros constitucionais da proteção de dados no Brasil, que poderiam ser aproveitados para os casos de processamento e uso de dados relacionados durante e depois da pandemia. Assim, o reconhecimento expresso de um direito fundamental à proteção de dados pelo STF, por exemplo, seria de grande contribuição. Dessa tutela constitucional poder-se-iam extrair não somente os procedimentos de segurança, transparência e proporcionalidade/necessidade para tratamento de dados, como também a necessidade da supervisão por uma autoridade independente, como previsto expressamente no direito fundamental à proteção de dados europeu. (11)

No atual contexto de processamento automatizado de dados, não existem dados pessoais insignificantes, tampouco há entidades a quem se pode dar um cheque em branco para o amplo processamento de dados pessoais dos cidadãos brasileiros.

Os vícios da Medida Provisória são ainda mais graves diante de um quadro de carências do sistema institucional brasileiro da proteção de dados.

Tais carências ficarão mais evidentes nos debates relativos ao uso de dados pessoais para monitorar e controlar a pandemia no país e controvérsias semelhantes deverão se repetir nas arenas estaduais e federal.

Por todas as razões expostas, é flagrante a inconstitucionalidade da Medida Provisória nº 954 e os seus danos são irreparáveis. Tal Medida subtraiu do Congresso Nacional a oportunidade de debater o tema, ao determinar que os dados sejam repassados ao IBGE no exíguo prazo de uma semana, período no qual



não é possível sequer aprovar emendas legislativas ao seu texto.

É fundamental, em primeiro lugar, que esses vícios sejam reconhecidos e anulados e, em uma perspectiva mais ampla, que um verdadeiro tripé institucional da proteção de dados seja construído no país, calcado em: (i) um direito fundamental à proteção de dados pessoais, (ii) na entrada em vigor da Lei Geral de Proteção de Dados em agosto deste ano, bem como (iii) na instituição de uma autoridade de proteção de dados autônoma, técnica e atuante.

1 <http://www.schwartzman.org.br/sitesimon/?p=6488>. Há um equívoco na frase, pois não há dúvida de que se trata de dados pessoais à luz da Lei Geral de Proteção de Dados, vez que os dados requisitados são identificados (não anonimizados), conforme disposto expressamente no art. 2º da Medida Provisória: “empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.”

2 Idem.

3 <https://respondendo.ibge.gov.br/coleta-por-telefone.html>

4 <http://www.in.gov.br/web/dou/-/instrucao-normativa-n-2-de-17-de-abril-de-2020-253341223>

5 Anatel VOTO Nº 30/2020/PR Processo nº 53500.017367/2020-40

6 Os escândalos relativos à espionagem da Internet e dos meios de comunicação, que atingiram a Agência Nacional de Segurança dos EUA em 2013, expuseram de forma inédita os riscos a que os cidadãos estão submetidos na era da informação. Retorna, assim, o temor do Estado como o “Big Brother”, que tudo vê e tudo controla, ameaçando direitos já há muito consolidados e colocando em risco a confiança dos indivíduos na infraestrutura da comunicação e informação, componente vital da sociedade da informação. Cf.: <http://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat>; <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>; <http://www.theguardian.com/commentisfree/series/glenn-greenwald-security-liberty>. Ainda, o escândalo da Cambridge Analytica revelou como dados de um teste de personalidade podem ser usados em contexto completamente diverso daquele em que foram coletados, como no caso, para o microtargeting eleitoral do Partido Republicano.

7 BVERFGE 65, 1. p. 239 e 240. Na reclamação ajuizada perante a Corte Constitucional, contestava-se a “Lei do Recenseamento de População, Profissão, Moradia e Trabalho”. O Tribunal conheceu da reclamação e, no mérito, confirmou a constitucionalidade da lei em geral, declarando nulos os dispositivos que determinavam a comparação dos dados coletados, bem como a sua transferência para outros órgãos da administração. Cf: MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

8 BVERFGE 65, 1. p. 239 e 240. SCHWABE, Jürgen; MARTINS, Leonardo. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Konrad-Adenauer-Stiftung, 2005. Acessível em <http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs->



[jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf/view](#)

9 RE n. 673.707, Minas Gerais, relatado pelo Min. Luiz Fux em 17.06.2017.

10 A análise dessa decisão, bem como o delineamento da estrutura de um direito fundamental à proteção de dados pode ser encontrada no texto: MENDES, Laura. Habeas Data e Autodeterminação informativa: dois lados da mesma moeda. In: Direitos Fundamentais & Justiça, ano 12, n. 39, p. 185-216, jul./dez. 2018.

11 Esse direito está previsto no art. 8o. da Carta de Direitos Fundamentais e tem a seguinte redação: Art. 8o. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de acessar aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”

Date Created

24/04/2020