EXCELENTÍSSIMA SENHORA MINISTRA DO SUPREMO TRIBUNAL FEDERAL ROSA WEBER

Ação Direta de Inconstitucionalidade n. 6387/DF

O **LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET – LAPIN**, doravante também denominado "LAPIN", pessoa jurídica de direito privado, associação sem fins lucrativos, inscrita no CNPJ n. 36.965.428/0001-16, com sede na SHIGS 715, Bloco G, Casa 111, Asa Sul, CEP 70.381-707, Brasília/DF, vem, por seus advogados subscritos, conforme procuração em anexo, à presença de Vossa Excelência, com fulcro nos artigos 138 e 937, IV, do Código de Processo Civil, art. 7º, §2º da Lei 9.868/99 e art. 124, pár. único, do Regimento Interno do STF, requerer admissão na presente Ação Direta de Inconstitucionalidade n. 6.387 na condição de **AMICUS CURIAE**, pelos fatos e fundamentos a seguir.

I. BREVE SÍNTESE DA DEMANDA

Trata-se de Ação Declaratória de Inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil - CFOAB a fim de que seja reconhecida a "inconstitucionalidade, na íntegra, da Medida Provisória 954/2020".

Em sede Liminar, o Requerente postulou pela concessão de medida liminar para suspender imediatamente a eficácia da integralidade da Medida Provisória 954/2020, bem como para reconhecer a presença no ordenamento constitucional brasileiro do direito fundamental à autodeterminação informativa.

O CFOAB argumenta que a Medida Provisória objeto da presente ação fere a Constituição Federal "(i) por afronta aos requisitos de relevância e urgência para a edição de medida provisória (art. 62, caput, da CF/1988), e (ii) por violação direta aos artigos 1º, inciso III e 5º, incisos X e XII da Constituição Federal, os quais asseguram, respectivamente, a dignidade da pessoa humana; a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas; e o sigilo dos dados".

Quanto mais, o requerente pleiteia o reconhecimento "no ordenamento constitucional brasileiro do direito fundamental à autodeterminação informativa, a ensejar tutela jurisdicional quando sua violação não for devidamente justificada por motivo suficiente, proporcional, necessário e adequado e com proteção efetiva do sigilo perante terceiros, com governança que inclua o Judiciário, o Ministério Público, a Advocacia e entidades da sociedade civil".

Em decisão publicada no Dje. em 27.04.2020, a Exma. Ministra Relatora Rosa Weber deferiu o pedido liminar "para suspender a eficácia da Medida Provisória n. 954/2020."

II. DO *AMICUS CURIAE*

O instituto do *amicus curiae*, positivado no art. 138 do CPC, possui como requisitos para admissão a **(a)** a relevância da matéria; **(b)** a repercussão social da controvérsia; e **(c)** a representatividade do postulante. Ademais, à luz da evolução

jurisprudencial do Supremo Tribunal Federal[1], devem também ser consideradas **(d)** a oportunidade[2]; e **(e)** a utilidade das informações prestadas.

a. Da relevância da matéria

No tocante à **relevância da matéria**, restou evidente, a partir da leitura da decisão que suspendeu a eficácia do ato normativo ora questionado no presente processo, que a presente controvérsia pode ferir direitos fundamentais previstos na constituição:

> "O **art. 2º da MP n. 954/2020** impõe às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, da relação de **nomes**, **números de telefone** e **endereços** de seus consumidores, pessoas físicas ou jurídicas.
> Tais informações, relacionadas à **identificação – efetiva ou potencial – de pessoa natural**, configuram **dados pessoais** e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual **(art. 5º, caput)**, da privacidade e do livre desenvolvimento da personalidade **(art. 5º, X e XII)**. Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.
> Decorrências dos direitos da personalidade, o respeito à **privacidade** e à **autodeterminação informativa** foram positivados, no **art. 2º, I e II, da Lei nº 13.709/2018** (Lei Geral de Proteção de Dados Pessoais), como **fundamentos** específicos da disciplina da **proteção de dados pessoais**." (MEDIDA CAUTELAR NA ADI nº 6.387/DF, Relatora: Ministra ROSA WEBER, Data de Julgamento: 24.04.2020, Data de Publicação: DJe 27.04.2020)

Vale ressaltar que a proteção de dados pessoais é matéria de ampla repercussão no âmbito internacional, tendo em vista o aumento crescente na capacidade de processamento de dados pelas organizações e nos reflexos disso à livre construção do pensamento por indivíduos. Governos ao redor de todo o mundo têm regulado a matéria, com destaque para a recente entrada em vigor do Regulamento Geral de Proteção de Dados na União Europeia e com a edição

[1] ADI 2321 MC, Rel. Min. Celso de Mello, DJ de 10/6/05.
[2] ADI 4071 AgR, Rel. Min. Menezes Direito, DJe de 16/10/09

da Lei Geral de Proteção de Dados no Brasil. Tais normas já têm tido profundo impacto nos âmbitos social e econômico, e têm sido vistas como garantidoras da intimidade das pessoas.

b. Repercussão social da controvérsia

A repercussão social da controvérsia resulta da eficácia *erga omnes* e do efeito vinculante da decisão definitiva de mérito a ser proferida nesta ação, nos termos do art. 102, §2º, da Constituição.

No presente caso, o que será decidido por esta Corte transcende os limites subjetivos deste processo, uma vez que a norma questionada impacta diretamente a privacidade e a proteção de dados de milhões de brasileiros que possuem contas de telefone.

A decisão de mérito contribuirá para suprir parte da lacuna legal existente hoje pela ausência de regulamentação de mecanismos de proteção de dados no país, materializada pela *vacatio legis* da Lei Geral de Proteção de Dados - LGPD.

Vale ressaltar que a LGPD é instrumento essencial para a observância de direitos fundamentais previstos nos artigos **1º e 5º, X e XII, da Constituição Federal,** que prevêem a dignidade humana, a inviolabilidade da intimidade e da vida privada e a proteção do sigilo dos dados das pessoas.

Nesse sentido, conclui-se que **toda a sociedade brasileira será impactada por esta decisão**, que alcançará milhões de brasileiros, clientes ou não de empresas de telefonia, o que indica a ampla repercussão social desta controvérsia.

c. Representatividade

O Laboratório de Políticas Públicas e Internet - LAPIN é um centro de pesquisa e ente da sociedade civil fundado em 2016, na Universidade de Brasília. Sua atuação engloba estudos que focam a intersecção entre direito, tecnologia e sociedade para apoiar a elaboração de políticas públicas sobre a regulação de tecnologias.

O LAPIN já atuou perante esta egrégia Corte em diferentes momentos. Destacam-se a participação como expositor na audiência pública convocada no

escopo da **Ação Direta de Constitucionalidade n. 51**[3], que discute medidas para transferência internacional de dados em contextos de investigação criminal.

A instituição também atuou na **Arguição de Descumprimento de Preceito Fundamental n. 403**[4], que versava sobre a criptografia de aplicativos de mensagens instantâneas e que analisou a suspensão do Whatsapp em âmbito nacional. O LAPIN foi o primeiro ente da sociedade civil aceito como *amicus curiae* no referido processo.

Além disso, o LAPIN tem atuação constante no Poder Legislativo, onde seus representantes foram expositores na **Comissão Especial da Câmara dos Deputados para discutir a Proposta de Emenda à Constituição n. 17/2020**, que pretende incluir a proteção de dados no rol de direitos fundamentais da Constituição.

Também tem veiculado notas técnicas para instruir parlamentares envolvidos na redação de projetos de lei sobre regulação de tecnologia. Além disso, contribuiu com a **Estratégia Brasileira de Inteligência Artificial** junto ao Ministério da Ciência, Tecnologia, Inovação e Comunicações.

Assim, resta evidente a pertinência temática do objeto desta Ação Direta de Inconstitucionalidade com os estudos e as demais ações desenvolvidas pelo LAPIN.

d. Oportunidade

O requisito da **oportunidade** diz respeito ao momento do pedido de intervenção formulado pelo *amicus curiae*, que deve ocorrer, segundo precedentes dessa E. Corte, "até a data em que o Relator liberar o processo para pauta".[5] Como a presente Ação Direta de Inconstitucionalidade ainda não entrou nesse estágio, a exigência ora tratada resta cumprida.

---

[3] SUPREMO TRIBUNAL FEDERAL (BRASIL). **Segurança jurídica foi a ênfase do último grupo de expositores a participar da audiência sobre controles de dados na internet**. 10 fev. 2020. Disponível em https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=436677&ori=1. Acesso em 29 abr. 2020.

[4] SUPREMO TRIBUNAL FEDERAL (BRASIL). **Definidos participantes e cronograma da audiência pública sobre WhatsApp e Marco Civil da Internet.** Brasília, DF, 10 fev. 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=341437. Acesso em: 27 abr. 2020.

[5] AgRg na AD nº 4.071-5. Relator: Ministro Carlos Alberto Menezes Direito. DjE. 22.04.2009.

e. Utilidade das Informações

Por fim, acerca do critério da **utilidade das informações**, o LAPIN recentemente publicou Nota Técnica[6] a partir de um trabalho coletivo de pesquisa que esmiuçou aspectos concernentes à proteção de dados contidos na MP nº 954. O documento foi direcionado a parlamentares a fim de subsidiar futuras emendas legislativas na medida provisória em questão, tendo em vista a complexidade do tema.

Diante disso, restam cumpridos os requisitos previstos no artigo 7º, §2º, da Lei no 9.868/99, e no artigo 138, do Código de Processo Civil, devendo o LAPIN ser admitido como *Amicus Curiae* da presente ação constitucional.

III. DA PROTEÇÃO DE DADOS PESSOAIS

Tendo em vista a urgência da matéria, o LAPIN aproveita para já trazer, perante esta Suprema Corte, uma prévia de sua argumentação a respeito da conformidade ao direito de proteção de dados da Medida Provisória n. 954 e aos direitos estipulados nos artigos **1º e 5º, X e XII, da Constituição Federal,** que prevêem a dignidade humana, a inviolabilidade da intimidade e da vida privada e a proteção do sigilo dos dados das pessoas.

a. Dos dados coletados

A Medida Provisória n. 954 dispõe, como descreve sua epígrafe, sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística. De acordo com seu art. 2º, esses dados consistiriam nos **nomes**, **números de telefone** e **endereço** de todos os consumidores de serviços de telefonia no Brasil.

Para que se possa compreender a repercussão desse tipo de coleta de dados, é imprescindível analisar a natureza dessas informações para classificá-las

[6] LAPIN. **Nota Técnica MP 954**: Recomendações para o Compartilhamento de Dados Entre Empresas de Telecomunicação e o IBGE. Brasília, DF, 2020. Disponível em: https://9977a902-e455-46d9-8a7b-0ac71f155f93.filesusr.com/ugd/77388c_6d4ef26c4f6248b1a8317b055e501486.pdf. Acesso em: 27 abr. 2020.

como dados pessoais. Caso sejam assim consideradas, os princípios e direitos previstos na Lei Geral de Proteção de Dados Pessoais (LGPD) devem ser seguidos.

A tabela abaixo descreve o **conceito** e traz exemplos:

<table>
<tr><th colspan="3">Por que endereço e telefone são dados pessoais?</th></tr>
<tr><td colspan="3">Conforme a LGPD, art. 5º, I, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Este conceito é composto por quatro elementos:[7]</td></tr>
<tr><td rowspan="3">Elementos do dado pessoal</td><td>Informação</td><td>Pode ter natureza objetiva (ex. idade) ou subjetiva (ex. o devedor X é confiável).</td></tr>
<tr><td>Relacionada a</td><td>Um dado pode ser considerado relacionado a um indivíduo se ele diz respeito a um dos seguintes critérios:
(i) se relaciona a um conteúdo sobre o indivíduo;
(ii) tem a finalidade de avaliar um indivíduo ou seu comportamento; ou
(iii) tem um impacto sobre interesses ou direitos do indivíduo.</td></tr>
<tr><td>Pessoa Natural</td><td>Para ser pessoal, a informação deve estar relacionada a um indivíduo humano.</td></tr>
</table>

[7] Esses elementos são apresentados a partir do conceito legal da LGPD e as referências do Grupo de Trabalho do Artigo 29, Comitê Europeu que regulou matérias de proteção de dados. Para mais informações, checar: Article 29 Working Party, Opinion 4/2007 on the concept of personal data Brussels, 2007. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acesso em: 23 abr. 2020.

	Identificada ou identificável	"Identificada" significa que a ligação ao indivíduo é feita de forma direta, como pelo tratamento de seu nome completo ou sua foto. Como "identificável", a ligação é indireta, e um processo de cruzamento de dados pode ser necessário para a identificação. Isto contudo não elimina a caracterização do dado como dado pessoal. É o caso de identificadores como o RG, CPF, o **endereço** e o **telefone** de uma pessoa natural.

Por consistirem em "informaç[ões] relacionada[s] a pessoa natural identificada ou identificável", nome, endereço e telefone são sim considerados dados pessoais de acordo com a LGPD. Por isso, seu tratamento deve seguir os parâmetros ditados pela referida lei.

Para melhor compreensão do que será descrito ao longo desta peça, cabe conceituar também o que é um **dado pessoal sensível.**

Previsto no art. 5º, inciso II, da LGPD, dado sensível consiste em um dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

É vedado realizar o tratamento de dados sensíveis, salvo com base nas exceções previstas no art. 11, da LGPD. Essa abordagem diferenciada da lei ocorre por se tratarem de dados que, a depender da forma como são utilizados, são capazes de causar ainda maior impacto à privacidade ou ao exercício de liberdades de seu titular. Isso faz com que sejam exigidas mais condições de

segurança para seu tratamento do que seria o caso para dados pessoais sem categoria específica[8] .

Como se verá mais à frente, no escopo da MP está o compartilhamento de informações e o cruzamento de dados para realização de "estatísticas oficiais" do IBGE, as quais são declaradas de maneira genérica. Contudo, um dos extratos possíveis de um compartilhamento indiscriminado é a criação de perfis de pessoas baseados em informações como ideologia, hábitos de consumo e situação de saúde Com essas informações em mãos, agentes têm a capacidade de influenciar hábitos de consumo, discriminar pessoas com base em sua raça, ideologia ou orientação sexual, recusar crédito e inclusive manipular eleições, como ocorreu com o caso Cambridge Analytica.[9]

A partir disso, qual a diferença entre a coleta de dados pessoais como nome, número e telefone da forma massificada e digital, como propõe a MP 954, e as páginas amarelas? A resposta reside na facilidade de extração de inferências a partir desses dados e a facilidade de pareá-los com os resultados das entrevistas conduzidas pelo IBGE que as tecnologias atuais permitem.

Logo, da forma como foi disciplinada a MP 954, **os dados que serão disponibilizados para o IBGE são dados pessoais e podem facilitar o acesso a dados sensíveis de maneira ampla.** A partir dessa conclusão, o próximo passo é compreender a finalidade à qual o tratamento de dados se disciplina. Posteriormente, será possível compreender se tais dados são necessários e adequados para o propósito visado pela medida.

Vale chamar aqui atenção de que a preocupação com dados pessoais nesse contexto se dá pelo potencial de violação da intimidade dos indivíduos que

---

[8] FINCK, Michèle; PALLAS, Frank. **They who must not be identified—distinguishing personal from non-personal data under the GDPR**. International Data Privacy Law, Oxford, p. 25, 10 mar. 2020. Disponível em: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. Acesso em: 9 abr. 2020.

[9] THE GUARDIAN. **What is the Cambridge Analytica scandal?** - video explainer. 19 mar 2018. https://www.theguardian.com/news/video/2018/mar/19/everything-you-need-to-know-about-the-cambridge-analytica-expose-video-explainer. Acesso em 24 abr 2020.

pode ocorrer caso haja o abuso na utilização dos dados ou mesmo por seu vazamento.

O Brasil já conta com diversos exemplos de vazamentos pela administração pública. Casos como o vazamento recente de dados do Programa de Ação Cultural pelo Governo de São Paulo[10] e o ocorrido pelo DETRAN do Rio Grande do Norte[11].

Considerando que nenhuma organização, pública ou privada, é completamente isenta de falhas de segurança, a preocupação com a proteção dessas informações é necessária para garantir o exercício regular de liberdades individuais pelos cidadãos brasileiros.

b. Da finalidade dos dados coletados

O texto da Medida Provisória estabelece a "*produção de estatística oficial*" como a finalidade do tratamento de dados que será realizado pelo IBGE. No entanto, **não há especificação de qual estatística específica será produzida**, dentre as tantas realizadas pela fundação.

Essa imprecisão na descrição do propósito do tratamento vai contra o art. 6º, Inciso I, da Lei nº 13.709, a Lei Geral de Proteção de Dados (LGPD), que estabelece que a finalidade para o tratamento de dados pessoais deve ser específica.[12] Para que cumpra esse requisito, **é necessário que a MP 954 determine quais estudos estatísticos serão realizados e quais os resultados**

[10] Folha de São Paulo. **Governo paulista confirma exposição de dados de pessoas físicas**. 24 out. 2019. Disponível em https://www1.folha.uol.com.br/tec/2019/10/governo-paulista-confirma-vazamento-de-dados-de-pessoas-fisicas.shtml. Acesso em 19/04/2020.

[11] Tecmundo. **Falha no Detran vaza dados de 70 milhões de brasileiros com CNH**. Disponível em: https://www.tecmundo.com.br/seguranca/146780-falha-detran-vaza-dados-70-milhoes-brasileiros-cnh.htm

[12] 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;

esperados, ainda mais levando em conta que se tratam de dados pessoais com potencial para dar acesso a dados sensíveis sobre indivíduos.

Não há motivo para não se realizar essa especificação. Tal medida daria mais segurança para os indivíduos consentirem na disponibilização dos seus dados pessoais, ainda mais caso haja garantias de que eles serão utilizados apenas para pesquisas estatísticas que já eram feitas anteriormente.

Apesar de não estar expressa na MP, informações da mídia indicam que estes dados serão utilizados para a Pesquisa Nacional por Amostra de Domicílios Contínua (PNADC)[13]. Pelo fato de essa pesquisa, como se verá adiante, historicamente coletar dados sobre a **raça** dos entrevistados,[14] a importância da especificação da finalidade se faz ainda mais urgente. Afinal, informações sobre a raça do indivíduo configuram **dado sensível,** de acordo com o art. 11, da LGPD, o que obriga o controlador a tomar medidas de segurança ainda mais elaboradas ao tratá-los.

Esse é mais um motivo pelo qual a especificação do tratamento é necessária, especialmente para dar segurança para os indivíduos consentirem na disponibilização dos seus dados pessoais, ainda mais caso haja garantias que serão feitas apenas para pesquisas estatísticas que já eram feitas anteriormente pelo IBGE.

c. Da minimização dos dados

Para atender ao art. 6º, II c/c III, da LGPD, os dados a serem coletados devem ser necessários e adequados à finalidade de seu tratamento. Desses dois princípios, se subsume a ideia de minimização, que determina que a coleta de

[13] SENADO FEDERAL (Brasil). **Operadoras deverão repassar dados de clientes a IBGE para pesquisa por telefone**. [*S. l.*], 20 abr. 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/04/20/operadoras-deverao-repassar-dados-de-clientes-a-ibge-para-pesquisa-por-telefone. Acesso em: 21 abr. 2020.
[14] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Manual Básico da Entrevista. Pesquisa Nacional por Amostra de Domicílios Contínua**. Coordenação de Trabalho e Rendimento. Rio de Janeiro: IBGE, 2016. p. 53.

dados pessoais deve se restringir ao mínimo possível para alcançar o propósito pretendido pelo tratamento.[15]

Pela falta de informações oficiais sobre qual será a "estatística oficial" que será de fato a finalidade para a coleta dos dados, partiremos aqui do pressuposto de que será para a PNADC. Analisaremos tanto a **quantidade de pessoas** entrevistadas que formam a amostragem necessária para sua realização, quanto a **natureza dos dados** coletados de cada uma para informar a pesquisa.

De acordo com as normas regulamentadoras da PNADC, os domicílios selecionados para integrar seu Plano Amostral e participar da pesquisa são retirados do Cadastro Nacional de Endereços para Fins Estatísticos (CNEFE),[16] uma base de dados pública composta de 78 milhões de endereços urbanos e rurais em todo Brasil.

O plano amostral é feito a partir de uma seleção aleatória de domicílios a serem entrevistados[17] dentro de um certo espaço territorial pré-definido pelo IBGE, de modo a garantir a representatividade de cada região. As pesquisas do PNADC são divulgadas com periodicidade mensal, trimestral e anual.[18]

De acordo com o IBGE, a cada trimestre são entrevistados 211.344 domicílios.[19] **Esse número é muito abaixo da quantidade de indivíduos que serão afetados pela Medida Provisória**, que pode alcançar o total de 230 milhões de linhas telefônicas em uso no Brasil, considerando somente as de celular.[20]

---

[15] Information Commissioner's Office. **Principle (c): Data minimisation.** Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/. Acesso em 23 abr. 2020.
[16] FREITAS, Marcos Paulo Soares de. **Sistema integrado de pesquisas domiciliares**: amostra mestra 2010 e amostra da PNAD contínua. Rio de Janeiro : IBGE, Coordenação de Métodos e Qualidade, 2014. p. 14.
[17] FREITAS, Marcos Paulo Soares de. **Sistema integrado de pesquisas domiciliares**: amostra mestra 2010 e amostra da PNAD contínua. Rio de Janeiro : IBGE, Coordenação de Métodos e Qualidade, 2014. p. 22.
[18] ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (org.). **Censo Demográfico, Pesquisa Nacional por Amostra de Domicílios (PNAD) e PNAD Contínua**. Brasília, 26 nov. 2019. Disponível em: https://repositorio.enap.gov.br/bitstream/1/4643/6/2019-11-26%20-%20PNAD%2C%20Censo%20Demográfico%2C%20PNADC%20e%20PNS.pdf. Acesso em: 24 abr. 2020.
[19] IBGE, op. cit., p. 17.
[20] ÉPOCA NEGÓCIOS. **Brasil tem 230 milhões de smartphones em uso**. 26 abr 2019. Disponível em

Isso mostra como é desproporcional a ideia de o IBGE ter acesso aos dados de todos os clientes das empresas de telefonia, sendo que normalmente consegue conduzir suas pesquisas com qualidade utilizando somente os de cerca de 211 mil, em um claro desrespeito ao princípio da minimização de dados.

Por isso é que **a coleta desses dados deve ser feita de modo amostral e aleatório.** Uma solução viável para isso é que as empresas de telefonia já passem os dados de clientes na quantidade razoável e selecionada de forma aleatória para realização da pesquisa, nos parâmetros usados nas pesquisas anteriores.

Ultrapassada a questão da quantidade de clientes cujos dados serão compartilhados, **cabe agora analisar quais dados de cada indivíduo são primordiais para a realização da pesquisa** de modo a cumprir com os princípios da necessidade e adequação.

Em condições normais, como visto, os agentes do IBGE conduzem a PNADC de forma presencial. Dotados apenas do endereço das pessoas, os contatos são feitos diretamente nas residências, momento em que as demais informações úteis para a pesquisa são coletadas.

Isto posto, **um procedimento a ser seguido pelo IBGE deveria consistir em coletar somente amostragem aleatória do número de telefone dos clientes** com as empresas de telefonia, separados conforme a sua unidade territorial definida pelas normas da PNADC.

Uma vez realizado o contato com cada indivíduo, aí sim a fundação terá a oportunidade de recolher outros dados, tais como nome e endereço do indivíduo. Vale ressaltar que a PNADC é feita de forma voluntária.

Esse procedimento é essencial para garantir maior segurança da informação. Menos dados estarão expostos a vazamentos ou ataques durante sua transferência entre as empresas de telefonia e o IBGE. Além disso, passarão a ser respeitados os princípios da **necessidade** e **adequação** de dados, previstos na LGPD.

---

https://epocanegocios.globo.com/Tecnologia/noticia/2019/04/brasil-tem-230-milhoes-de-smartphones-em-uso.html. Acesso em 22 abr 2020.

Já no que diz respeito aos dados coletados sobre cada entrevistado, ou seja, às informações requeridas pelo IBGE, a PNADC, como ressaltado anteriormente, envolve a coleta de dados sobre a **raça** dos entrevistados,[21] o que configura **dado sensível,** de acordo com o art. 11, da LGPD.

Esse tipo de tratamento de dados exige ainda mais condições de segurança do que um tratamento de dados pessoais sem categoria específica. A respeito disso, mais à frente trataremos de técnicas de segurança como anonimização e pseudonimização, que podem garantir menor exposição a usos indevidos dos dados pessoais.

Outra questão diz respeito ao recente **convênio firmado entre IBGE e Ministério da Saúde** para usar a PNADC para monitorar a incidência do COVID-19 no Brasil.[22] Da forma como está redigida, a MP 954 pode permitir a coleta de dados para fundamentar essa pesquisa, o que deve ser proibido caso não haja regulação específica para tratar a matéria.

Afinal, sob a PNADC-Covid, os dados coletados dos brasileiros, tais como seus nomes, telefones e endereços, serviriam para criar correlações com **dados de saúde**, o que também caracterizaria um tratamento de dados sensíveis. Isso porque dados extraem sua característica de serem sensíveis ou não a partir também do contexto em que são tratados.[23]

Pelo exposto, conclui-se que a coleta de dados pretendida pela MP 954 não atende aos princípios da necessidade e da adequação, por não se firmar como proporcional aos supostos fins pretendidos.

---

[21] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Manual Básico da Entrevista. Pesquisa Nacional por Amostra de Domicílios Contínua**. Coordenação de Trabalho e Rendimento. Rio de Janeiro: IBGE, 2016. p. 53.

[22] Agência de Notícias IBGE. **IBGE faz parceria com Ministério da Saúde para monitorar casos de Covid-19**, 2 abr 2020. Disponível em https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/27302-ibge-faz-parceria-com-ministerio-da-saude-para-monitorar-casos-de-covid-19. Acesso em 23 abr 2020.

[23] ARTICLE 29 WORKING PARTY. **Health data in apps and devices**. Bruxelas, 2 maio 2015. Disponível em: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf. Acesso em: 24 abr. 2020.

d. Da eliminação dos dados pessoais

Também desproporcional é a previsão do art. 4º da Medida Provisória 954, que dita que os dados compartilhados pelas empresas serão deletados após a superação da pandemia. Prevê ainda que o ato poderá ser postergado por mais 30 dias, caso haja comprovada necessidade de uso dos dados para a conclusão de produção estatística oficial pelo IBGE.

Essa redação abre margem para que haja abusos na utilização dos dados, o que viola os princípios da segurança e da finalidade. Afinal, o descarte dos dados não está vinculado ao encerramento do estudo estatístico que deveria ser indicado pela medida provisória, mas sim ao fim da pandemia. Tal previsão permite que os dados coletados continuem armazenados por período indeterminado, que pode superar em muito o tempo de duração da pesquisa.

Uma vez que a finalidade precípua do IBGE seja a produção de estudos estatísticos, que, por sua natureza, apresentam dados agregados, tão logo esses resultados sejam produzidos e o estudo concluído, os dados pessoais coletados devem ser eliminados. Por isso, **uma data precisa deve ser estipulada, e não atrelada a uma ordem do poder público que não tem prazo definido,** que é o fim da situação de calamidade pública do COVID-19. Até lá, caso a crise ainda não tenha sido superada, o prazo poderá ser renovado, mas sempre por períodos definidos.

Os dados coletados pelo IBGE deverão ser mantidos apenas durante o período que serão utilizados para fins de divulgação de cada pesquisa. Logo, se os dados de uma divulgação mensal não forem necessários para a divulgação trimestral ou anual, deverão ser eliminados. A coleta desses dados, da forma como prevê a MP, não pode de forma alguma perdurar caso seja decretado o fim da calamidade pública.

IV. APLICAÇÃO DE SALVAGUARDAS DURANTE O TRATAMENTO DOS DADOS

A MP 954 já traz, em seu escopo, alguns parâmetros de proteção de dados a serem seguidos pelo IBGE no tratamento dos dados pessoais, como data para eliminação, vedação de compartilhamento e obrigatoriedade de seguir a finalidade designada, que, como dito acima, deve ser melhor descrita.

A medida também prevê a realização de um relatório de impacto de proteção, o que é louvável, e faz expressa referência à LGPD, em seu art. 3º, §2º, o que demonstra intenção em seguir as diretrizes da lei.

Apesar disso, salvaguardas adicionais devem ser adotadas, conforme será descrito a seguir.

a. Nomeação de encarregado de proteção de dados

A primeira delas é a designação de um encarregado de proteção de dados. O ocupante do cargo será indicado pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e uma auditoria independente, na ausência da Autoridade Nacional de Proteção de Dados (ANPD).

Seu objetivo é garantir que os tratamentos de dados realizados por uma organização sejam feitos de acordo com princípios e regras de proteção de dados. No Brasil, apesar de ainda não estar em pleno vigor, a LGPD traz esses parâmetros, e dispõe sobre a figura do encarregado em seus art. 5º, VIII; art. 23, III; e art. 41.

O encarregado deve ser um especialista na área e estar posicionado na estrutura hierárquica da organização de modo a poder trabalhar com independência e não receber ordens sobre seu trabalho.[24] Além disso, o art. 23, III, da LGPD, estipula que o órgão público deve indicar um encarregado como condição para tratar dados pessoais.

[24] European Data Protection Supervisor. **Data Protection Officer (DPO)**. Disponível em https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en. Acesso em 22 abr. 2020.

b. Realização de auditoria externa

Sem a ANPD em funcionamento para trabalhar na fiscalização de atividades de tratamento de dados, é essencial que haja um colegiado de especialistas em proteção de dados sem vínculos com o IBGE para auditar a atuação do órgão. A auditoria externa também pode ser responsável por receber solicitações de titulares de dados que envolvam, por exemplo, seu direito de acesso ou de correção de suas informações.

A presença de uma auditoria será fundamental para aumentar o nível de confiança da sociedade[25] tanto em relação ao IBGE quanto às próprias empresas de telecomunicações. Além disso, irá assegurar **maior transparência** a respeito de como os dados estão sendo tratados. Especialmente em uma época em que desinformação tem sido disseminada indiscriminadamente, ter informações precisas de como o governo usa nossos dados é essencial.

c. Estabelecer parâmetros de controle de acesso e de segurança dos dados

A MP 954 também deve prever que o IBGE aponte parâmetros de segurança da informação a serem seguidos durante a realização do tratamento de dados especificado. O órgão deve delimitar com clareza quem terá acesso aos dados, bem como quais as medidas de autenticação e de autorização necessárias para acessá-los. O IBGE também deve apontar quem será responsabilizado por eventuais abusos realizados com os dados ou vazamentos.[26]

Mecanismos de segurança dos dados também devem ser previstos nas normas, especialmente pelo fato de o tratamento de dados, como explicitado acima, incluir dados sensíveis. O IBGE deve ser transparente com a forma como

[25] European Data Portal. **Analytical Report 12: Business-to-Government Data Sharing**, p. 21. Mar. 2019. Disponível em https://www.europeandataportal.eu/sites/default/files/analytical_report_12_business_government_data_sharing.pdf. Acesso em 22 abr. 2020.
[26] *Idem*.

protege dados contra invasões e vazamentos, considerando o fato de pertencerem a uma categoria especial.

d. Anonimização e pseudonimização

Uma salvaguarda a ser priorizada é a utilização de mecanismos de anonimização e pseudonimização durante o processo de realização das estatísticas.

O conceito de anonimização de dados se refere, nos termos da LGPD, à "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". Ao serem anonimizados, dados deixam de ser pessoais, e não estão mais sujeitos às regras da LGPD.

A esse respeito, vale ressaltar que o processo de anonimização de dados pessoais nunca é perfeito. Conforme descrito por Finck e Pallas,[27] a anonimização deve ser entendida como um meio de **reduzir o risco** de identificação de titulares de dados. Embora nunca seja absoluta, a anonimização apenas ocorrerá se puder garantir que, em um determinado período, os recursos técnicos e financeiros então existentes tornariam o processo de re-identificação impraticável ou excessivamente dispendioso.

Ou seja, **a anonimização só existe se o risco de re-identificar um indivíduo for residual e irrelevante.** Baseado nessa abordagem, a agregação é apenas mais uma técnica (embora bastante relevante neste contexto) para garantir a anonimização dos dados. Nesse sentido, o emprego de métodos de agregação, como *k-anonimity, l-diversity e t-closeness* devem ser incentivados mesmo em compartilhamentos dentro do próprio órgão.

[27] FINCK, Michèle; PALLAS, Frank. **They who must not be identified—distinguishing personal from non-personal data under the GDPR**. International Data Privacy Law, Oxford, pp. 1-26, 10 mar. 2020. Disponível em: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. Acesso em: 9 abr. 2020.

Por outro lado, para dados que não poderão ser anonimizados antes de serem eliminados ao fim da pesquisa, técnicas de **pseudonimização** podem ser aplicadas.

De acordo com o art. 13, §4º, da LGPD, pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Trata-se de um método de tratamento protetivo para dados. Apesar de não perderem o caráter pessoal, a pseudonimização garante maiores obstáculos para re-identificar indivíduos. Exemplos de aplicação são o emprego de recursos de criptografia e do estabelecimento de *hashes*, por exemplo.

A adoção de tais técnicas pelo IBGE é recomendada considerando tanto o alto volume de dados coletados quanto sua natureza sensível. Caso mecanismos adequados para impedir sua re-identificação não sejam postos em prática, aumenta o risco de cruzamento dessa base de dados com outras a fim de descobrir a identidade de indivíduos afetados pela Medida Provisória.

Isso pode dar margem tanto para uma violação à finalidade previamente estabelecida de tratamento desses dados, como também a possibilidade de levar indivíduos a serem discriminados com base em sua raça, orientação sexual ou sobre suas informações de saúde.

Nesse sentido, o risco de se ter uma base de dados que permita uma violação em massa da privacidade das pessoas é muito alto para que não se adote técnicas preventivas, em respeito ao princípio da segurança e da prevenção previstos no art. 6, incisos VII e VIII da Lei Geral de Proteção de Dados.

e. Adoção de código de conduta

Na ausência da LGPD, um código de conduta deveria ser adotado pelo IBGE, de modo a tornar transparente o fato de que tem seguido princípios claros de proteção de dados. Um exemplo de código a ser seguido é o descrito pela Comissão Europeia para transferências de dados entre organizações, que inclui,

entre outros princípios, os de proporcionalidade, finalidade e transparência.[28]

f. Garantia do exercício dos direitos do titular de dados

Além dos princípios estabelecidos no art. 6º da LGPD, o IBGE deve garantir o pleno exercício dos direitos do titular, previstos no art. 18 da mesma lei, como o direito de **livre acesso** aos dados e de **retificação**.

Outro direito importante de ser garantido é o de **revogação** do consentimento, caso a entrevista seja realizada de forma voluntária. O titular de dados entrevistado tem o direito de manifestar sua desistência do interesse em participar da pesquisa.

Para tanto, conforme descrito acima, a criação de um canal aberto de comunicação, que pode ser exercido pela auditoria externa, para lidar com o caso específico das pesquisas realizadas durante COVID-19 deveria ser prevista no procedimento de tratamento de dados. Cumprir com o princípio da **transparência**, nesse sentido, é fundamental.

Pelo canal, o titular de dados poderia encaminhar suas solicitações, que deveriam ser cumpridas em tempo hábil, preferencialmente dentro de 15 dias, de modo a garantir ao indivíduo controle sobre suas informações. Esse prazo está de acordo com o estipulado no art. 19, II, da LGPD.

V. PEDIDOS

Face ao exposto, o Laboratório de Políticas Públicas e Internet - LAPIN requer:

1. A admissão do Laboratório de Políticas Públicas e Internet - LAPIN na presente demanda, na qualidade de Amicus Curiae, nos termos do art. 138, do Código de Processo Civil, artigo 7º, §2º, da Lei no 9.868/1999 e no art. 21, XVIII, do

[28] European Commission. **Guidance on sharing private sector data in the European data economy.** Disponível em https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data- european-data-economy. Acesso em 22 abr. 2020.

Regimento Interno do Supremo Tribunal Federal, para que venha a apresentar manifestação escrita quanto ao mérito e a realizar sustentação oral durante o julgamento da demanda;

2. O Laboratório de Políticas Públicas e Internet - LAPIN requer a Vossa Excelência, desde já, que seja **autorizada sua sustentação oral durante julgamento da matéria.**

3. Seja a postulante intimada, por meio de seus procuradores, de todos os atos do processo.

Termos em que,

Pede deferimento.

Brasília, 1º de maio de 2020.

Henrique Bawden Silverio de Castro
OAB/DF n. 58.680

José Renato Laranjeira de Pereira
OAB/DF n. 59.985

Paulo Henrique Atta Sarmento
OAB/DF n. 63.259

Thiago Guimarães Moraes
CPF n. 014.667.361-19