EXCELENTÍSSIMO **MINISTRO DIAS TOFFOLI**, PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL

PARTIDO SOCIALISTA BRASILEIRO – PSB, partido político devidamente registrado perante o Tribunal Superior Eleitoral e com representação no Congresso Nacional, inscrito no CNPJ sob o n. 01.421.697/0001-37, com sede nacional no SCLN 304, Bloco A, Sobreloja 01, Entrada 63, Asa Norte, Brasília/DF, CEP n. 70.736-510 (Doc. 01), vem, por intermédio de seus advogados devidamente constituídos (Doc. 02), respeitosamente, à presença de Vossa Excelência, com fulcro no art. 102, inciso I, alínea *a*, da Constituição Federal, e na Lei n. 9.868/1999, ajuizar a presente

AÇÃO DIRETA DE INCONSTITUCIONALIDADE
(com pedido de medida cautelar)

para declarar a inconstitucionalidade dos artigos 2º, *caput* e §1º, e 3º **Medida Provisória n. 954, de 17 de abril de 2020**, que dispõe 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 (IBGE), para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública decorrente do novo coronavírus (SARS-CoV-2), de que trata a Lei n. 13.979/2020, pelas razões de fato e de direito a seguir expostas.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

I. DA NORMA IMPUGNADA.

A presente ação busca a declaração de inconstitucionalidade dos artigos 2º, *caput* e §1º a § 3º, e 3º da Medida Provisória n. 954, de 17 de abril de 2020, que assim dispõe:

> Art. 2º As 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.
> § 1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.
> § 2o Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o caput .
> § 3o Os dados deverão ser disponibilizados no prazo de:
> I - sete dias, contado da data de publicação do ato de que trata o § 2o; e
> II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes.
>
> Art. 3º Os dados compartilhados:
> I - terão caráter sigiloso;
> II - serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º; e
> III - não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial, nos termos do disposto na Lei nº 5.534, de 14 de novembro de 1968.
> § 1º É vedado à Fundação IBGE disponibilizar os dados a que se refere o caput do art. 2º a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos.
> § 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no caput do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Os dispositivos acima violam diretamente o direito constitucional à proteção de dados, amparado pela redação e pela interpretação sistemática dos artigos 1º, III, e 5º, X e LXXII, da Constituição Federal, referentes à dignidade da pessoa humana, à inviolabilidade da intimidade e da vida privada, e à garantia do *habeas data*.

A seguir, serão expostas com mais detalhes as inconstitucionalidades apontadas.

II. DA LEGITIMIDADE ATIVA UNIVERSAL DOS PARTIDOS POLÍTICOS.

Nos termos do art. 103, VIII, da Constituição Federal e do art. 2º, VIII, da Lei n. 9.868/99 os partidos políticos com representação no Congresso Nacional são dotados de legitimidade para propor ação direta de inconstitucionalidade, como é o caso do Partido Socialista Brasileira – PSB (Doc. 03).

Segundo o entendimento jurisprudencial deste Excelso Supremo Tribunal Federal, a legitimidade ativa de agremiação partidária com representação no Congresso Nacional "*não sofre as restrições decorrentes da exigência jurisprudencial relativa ao vínculo de pertinência temática nas ações diretas*" (ADI n. 1.407-MC, Rel. Min. Celso de Mello, Plenário, DJ 24.11.2000).

Destarte, os partidos políticos possuem a denominada legitimidade ativa universal para provocação do controle abstrato de constitucionalidade, razão pela qual está consolidada a legitimidade do Partido Socialista Brasileiro para o ajuizamento da presente ação.

III. DO CABIMENTO DA AÇÃO DIRETA DE INCONSTITUCIONALIDADE.

A Ação Direta de Inconstitucionalidade, prevista no art. 102, inciso I, alínea "a", da Constituição Federal, tem por objeto a declaração de inconstitucionalidade de lei ou ato normativo federal ou estadual que viole diretamente a Constituição.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

A Medida Provisória n. 954, de 17 de abril de 2020, constitui ato do Presidente da República dotado de força de lei pelo que dispõe o art. 62 da CF/1988[1]. A medida atende, portanto, ao pressuposto do art. 102, I, alínea "a", para fins de controle concentrado de constitucionalidade desse Supremo Tribunal Federal.

A violação constitucional provocada pela MPV n. 927 é **direta e não depende de anterior juízo de legalidade**, pois não há outra norma intermediando, em termos de fundamento e validade, a relação entre a lei questionada e a Constituição Federal. Portanto, a ação é perfeitamente cabível.

IV. DOS GRAVES RISCOS PARA O SISTEMA DEMOCRÁTICO

Em cenários de crise como o provocado pela pandemia desencadeada pelo coronavírus, os Estados contam com o poder-dever de tomar medidas extraordinárias para preservar o bem-estar e conferir segurança à coletividade.

Nessa direção, governos ao redor do globo têm se utilizado de poderes de emergência que, não raro, repercutem sobre direitos que consubstanciam premissas fundamentais para o regular funcionamento do sistema democrático.

A Medida Provisória impugnada consiste em um dos instrumentos legais de caráter emergencial de que se valeu o governo brasileiro nesse cenário. São contundentes, contudo, os fundamentos que ressaltam a elevada gravidade da disponibilização irrestrita de dados dos brasileiros vinculados a serviços de telecomunicações no país, o que, na realidade atual, representa quase a totalidade da população brasileira.

[1] Art. 62. Em caso de relevância e urgência, o Presidente da República poderá adotar medidas provisórias, com força de lei, devendo submetê-las de imediato ao Congresso Nacional.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Segundo dados da PNAD Contínua TIC 2017 do IBGE, o percentual de indivíduos com posse de telefone celular para uso pessoal, no ano de 2017, foi de 78,2% da população, o que corresponde a **141,6 milhões de brasileiros[2].**

Considerando os acontecimentos da história recente que denunciaram o elevado potencial de controle da opinião pública propiciado pelo acesso a informações de usuários de redes sociais, a disponibilização dos dados pessoais de tão grande número de brasileiros representa verdadeira ameaça ao sistema democrático do país.

O escândalo envolvendo as atividades da *Cambridge Analytica* e do *Facebook* demonstrou que o acesso aos dados pessoais dos usuários da rede social – cerca de 87 milhões de pessoas[3] – possibilitou a propagação de conteúdos políticos extremamente direcionados ao perfil dos eleitores nas eleições presidenciais dos Estados Unidos em 2018, bem como no referendo em que se debateu a saída do Reino Unido da União Europeia (Brexit)[4].

As implicações dessas atividades que se valem de elementos da vida privada dos cidadãos para influenciar sua participação no debate público são devastadoras ao pleno funcionamento da democracia. Isso porque a harmonia entre a autonomia privada e a autonomia pública de cada indivíduo – esta última compreendida na sua participação no debate realizado na esfera pública, livre de manipulações orientadas por interesses utilitaristas –, se apresenta como elemento justificador do Estado Democrático de Direito[5].

2https://agenciadenoticias.ibge.gov.br/media/com_mediaibge/arquivos/9e88a636785c573625be2c5632bd3087.pdf, pg. 44. Acesso em 19/04/2020.

3https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html. Acesso em 19/04/2020.

4 Para maiores informações, consultar: CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. *The Guardian.* 7 mai. 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>.

5 HABERMAS, Jürgen**. Between facts and norms** – contributions to a discourse theory of law and democracy. Translated by Willian Rehg. Massachusetts: The MIT press, 1996, p.104.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Vale ressaltar, ademais, que a possibilidade de vazamento de dados pessoais por bancos de dados públicos, longe de ser distante ou especulativo, é uma realidade. A título de exemplo, cita-se que no fim de 2019, o Estado de São Paulo admitiu o vazamento de dados pessoais de mais de 28 mil candidatos do Programa de Ação Cultural do Estado de São Paulo, que permitiu o acesso a fotocópias de documentos como carteira de identidade, CPF, endereço e telefone desses cidadãos, em patente violação aos seus direitos de privacidade[6].

Nesse contexto, o advento da Lei Geral de Proteção de Dados se apresenta como novo paradigma para a proteção de dados, conferindo maior segurança e confiabilidade às atividades que envolvam o processamento de dados no território nacional. Todavia, como a norma ainda não entrou em vigência, atualmente inexiste qualquer outro dispositivo legal que discipline a proteção de dados no setor público, exacerbando a vulnerabilidade do cidadão diante do tratamento sempre mais frequente de seus dados pelo Poder Público.

Esse cenário se mostra especialmente preocupante quando se tem em conta que a Medida Provisória impugnada vai na contramão de todo o debate desenvolvido até o presente momento por estudiosos acerca do impacto da má-utilização de dados pessoais no contexto democrático, bem como da norma já aprovada pelo Congresso Nacional, ao permitir a disponibilização dos dados de mais de 70% da população brasileira.

Ao promover a disponibilização desregulamentada de dados pessoais, a MPV n. 954 possibilita a criação de uma estrutura contemporânea de vigilância da população por parte do Estado brasileiro[7], concedendo ao governo o acesso a informações relevantes dos cidadãos que, dadas as tecnologias atualmente disponíveis, poderiam viabilizar ilegítimas interferências sobre tais indivíduos.

---

[6] 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.

[7] A estrutura de vigilância se relaciona com o conceito de panóptico desenvolvido pelo filósofo e jurista inglês Jeremy Bentham que, como instrumento de governo, permite o controle da população a partir da observação do seu comportamento pelo Estado. Para maiores informações consultar: FOUCAULT, Michel. Vigiar e punir: nascimento da prisão. 27ª Edição. Trad. Raquel Ramalhete Petrópolis-RJ, Editora Vozes, 1987.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Premido por tais preocupações é que o Partido Socialista Brasileiro vem a esta c. Corte Suprema buscar o controle de constitucionalidade das disposições que revelam de forma mais crítica a abusividade do referido ato normativo.

V. DO DIREITO CONSTITUCIONAL À PROTEÇÃO DE DADOS

A fim de facilitar a compreensão precisa dos dispositivos e princípios constitucionais violados pela norma impugnada, faz-se necessário desenvolver breve construção argumentativa e doutrinária sobre o tema.

Para tanto, inicialmente será utilizada como referência decisão da Corte Constitucional Alemã de 1983, em que se discutiu controvérsia similar à presente. Em seguida, a análise se voltará à Constituição Federal de 1988 e à existência de um direito constitucional à proteção de dados.

Por fim, serão apresentados os princípios elementares para o uso de dados à luz do direito constitucional acima mencionado.

a) Do reconhecimento da autodeterminação informativa pela decisão da Corte Constitucional alemã de 1983 e por outras jurisdições.

Desde a década de 1970, a Alemanha já contava com um sistema de proteção de dados de caráter infraconstitucional, uma vez que diversos estados e a própria União detinham leis esparsas relativas ao tema. Até 1983, contudo, ainda não havia o reconhecimento de uma garantia constitucional ao resguardo de dados e à transmissão de informações.

Isso se alterou a partir de decisão da Corte Constitucional de 1983, que analisou a constitucionalidade de lei de recenseamento nacional da população editada no ano anterior. Esse diploma recebeu críticas de diversos setores da sociedade pelo fato de prever o amplo processamento e compartilhamento dos dados coletados sem os controles e salvaguardas necessários.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Ao analisar a questão, o Tribunal destacou os avanços tecnológicos que possibilitariam o processamento, a armazenagem e a transmissão de dados em proporção jamais vistas antes. De acordo com a Corte, essas novas possibilidades demandavam o desenvolvimento da interpretação conferida a determinados direitos fundamentais, em razão do surgimento de ameaças até então impensáveis.

Nesse contexto, os julgadores identificaram possíveis violações aos direitos da personalidade, de autodeterminação e à liberdade de comportamento. Sobre o tema, explica Laura Mendes:

> Assim declara o Tribunal que o processamento automático dos dados ameaçaria o poder do indivíduo em decidir por si mesmo se e como ele desejaria tornar públicos dados pessoais no sentido de que o processamento de dados possibilitaria a elaboração de um "quadro completo da personalidade" por meio de "sistemas integrados sem que o interessado possa controlar o suficiente sua correção e aplicação". [...] Uma sociedade, "na qual os cidadãos não mais são capazes de saber quem sabe o que sobre eles, quando e em que situação", seria contrária ao direito à autodeterminação informativa, o que prejudicaria tanto a personalidade quanto o bem comum de uma sociedade democrática.[8]

Trata-se, em suma, do reconhecimento da autodeterminação informativa[9] do indivíduo e da valorização de seu direito de personalidade sob perspectiva mais ampla. Supera-se a ideia de que apenas determinados dados mais relevantes devam ser protegidos, para se reconhecer o direito dos indivíduos de ter controle sobre "quem sabe o que sobre eles", veja-se:

> Quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social, e quem não consegue avaliar mais ou menos o conhecimento de possíveis parceiros na

[8] MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. P. 188.

[9] A noção de "autoderminação informativa" não era, em si, nova, tendo sido cunhada por Alan Westin em 1967. WESTIN, Alan. *Privacy and Freedom.* New York: Atheneum, 1967.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

> comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação.[10]

Essa abordagem se mostra extremamente acertada em especial diante do avanço tecnológico. Como reconheceu o tribunal alemão, as novas possibilidades de processamento, armazenagem e compartilhamento de qualquer tipo de dado, seja ele considerado mais relevante ou não, têm potencial de gerar enormes danos à intimidade e à vida privada do indivíduo.

Por isso, reconheceu-se a necessidade de dar ao cidadão o controle sobre suas informações e o que será feito com elas. Não se trata mais de proteger uma lista fixa de dados que sempre deverão ser considerados sigilosos ou inacessíveis, mas de verdadeiramente garantir a autodeterminação informativa do indivíduo, que tem o direito de controlar a amplitude da divulgação ou utilização de qualquer aspecto relacionado a sua personalidade. Nesse sentido, ensina Laura Mendes:

> [...] todavia, logrou formular o novo direito fundamental como uma expressão do direito geral da personalidade, ou seja, dentro do já existente quadro da proteção da personalidade. Daí decorre que a decisão referente ao recenseamento contribuiu não apenas para fundamentar o direito à autodeterminação informativa, mas também para consolidar o direito geral da personalidade como um projeto efetivo, flexível e de aplicação prática.[11]

Como ocorre com os demais direitos fundamentais, a Corte Constitucional reconheceu a possibilidade de limitações dessa nova acepção do direito à personalidade. Eventuais restrições, contudo, somente podem ser justificados em nome de um interesse geral

---

[10] SCHWABE, Jürgen; MARTINS, Leonardo. Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Konrad-Adenauer-Stiftung, 2005. BVERFGE 65, 1. P. 237.
Disponível 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. Acesso em 19/04/2020.

[11] MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. P. 191.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

preponderante e desde que observados princípios mínimos, como a transparência e a segurança, que serão objeto de análise mais detalhada em tópico posterior.

Diversas outras jurisdições já reconhecem o direito fundamental à proteção de dados. O primeiro país a incorporar previsões específicas acerca do tratamento automatizado de dados pessoais foi Portugal, no artigo 35 da Constituição da República Portuguesa[12] de 1976, relativo à utilização da informática no contexto dos dados pessoais. Inspirado parcialmente no exemplo português, a Constituição Espanhola de 1978 apresenta previsão específica que limita o uso da informática com o fim de garantir a honra e intimidade[13].

Nas décadas seguintes verificou-se a consolidação do reconhecimento de um direito fundamental relacionado à proteção de dados pessoais no espaço jurídico europeu, com, entre outros marcos, a

---

[12] Artigo 35. Utilização da informática 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acesso em 19/04/2020.

[13] "Articulo 18.
1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podra hacerse en el sin consentimiento del titular o resolucion judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegraficas y telefonicas, salvo resolucion judicial.
4. La ley limitara el uso de la informatica para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf Acesso em 19/04/2020

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

promulgação da primeira legislação comunitária sobre o tema, a Diretiva 95/46/CE[14], que identificava como seu objetivo que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais".

Em 2000, a Carta dos Direitos Fundamentais da União Europeia[15], tratou especificamente da proteção de dados pessoais em seu artigo 8, proporcionando o tratamento deste direito fundamental pela Corte de Justiça da União Europeia[16].

b) Da Constituição Federal de 1988 e a existência de um direito à proteção de dados.

Conforme se infere a partir da experiência do Tribunal alemão, naquele país o direito à proteção de dados foi identificado no texto da Constituição com base principalmente nos direitos de personalidade.

Em suma, a partir do reconhecimento do núcleo desse direito fundamental, a Corte verificou a existência de nova acepção protetiva relativa aos dados pessoais.

[14] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046 Acesso em 19/04/2020

[15] Artigo 8º. Proteção de dados pessoais 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 aceder 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.
Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 19/04/2020.

[16] Uma descrição da casuística mais relevante sobre o tema na Corte está em GONZALES FUSTER, Gloria. *The emergence of personal data protection as a fundamental right of the EU.* London: Springer, 2014, pp. 226 - segs.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Esse tipo de hermenêutica constitucional é parte integrante do desenvolvimento histórico dos direitos humanos, uma vez que possibilita a concessão de respostas jurídicas a situações novas, decorrentes da evolução de cada sociedade. A propósito, destacam-se os ensinamentos de Paulo Branco e Gilmar Mendes:

> A especificação leva à necessidade de serem explicitados novos direitos, adequando-se às particularidades dos seres humanos na vida social. Incrementa-se o quantitativo dos bens tidos como merecedores de proteção.
>
> A tendência de multiplicação se dá, por igual, no interior dos próprios direitos tradicionais, na medida em que a abrangência destes experimenta movimentos de dilatação. Assim, por exemplo, a liberdade religiosa que, em um primeiro momento, alcançava apenas certas confissões, passa a alcançar concepções religiosas mais variadas.[17]

Em face dessa possibilidade hermenêutica, é necessário analisar se a proteção de dados, de alguma forma, encontra guarida na Constituição brasileira, assim como ocorreu na experiência alemã.

Inicialmente, destaca-se que um dos fundamentos da República, listado já no artigo 1º, III, da CF/1988, é a dignidade da pessoa humana. A amplitude desse dispositivo é enorme, demonstrando que o constituinte pretendeu colocar os direitos humanos e sua garantia no cerne do sistema jurídico-constitucional pátrio, também com o intuito de proteger os indivíduos de intromissões injustificadas do próprio Estado.

Nesse sentido, destaca-se a proteção constitucional aos direitos de personalidade. O artigo 5º, X-XII, expressamente resguarda, entre outros elementos, a intimidade, a vida privada, as correspondências e as comunicações dos cidadãos, veja-se:

> [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em

[17] MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 7. ed. rev. e atual. – São Paulo: Saraiva, 2012. P. 177.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

> caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]

A leitura desses dispositivos demonstra que o constituinte se preocupou em assegurar que cada indivíduo tenha controle sobre os elementos constitutivos de sua personalidade e sua eventual divulgação, deixando claro que essa proteção também se direciona a atos do Estado, que somente em situações extremamente específicas podem se sobrepor aos direitos de personalidade.

Como se demonstrou em tópicos anteriores, a divulgação irrestrita de dados pessoais, que cada vez mais opera de forma massiva e sistemática, pode gerar efeitos nefastos não apenas ao indivíduo, mas também à sociedade, como observa Danilo Doneda:

> Frente aos novos desafios, é cada vez mais claro que o sentido do isolamento predominante na doutrina do direito à privacidade do tempo de Brandeis e Warren está superado. Neste novo panorama, a privacidade deixa de ser um meio de garantir o isolamento de alguns para cumprir também uma outra função, que é reagir contra políticas de discriminação baseadas em opiniões e opções religiosas, políticas e sexuais, bem como de toda sorte de informações privadas[18].

Diante dessa realidade – e tendo em vista que o Texto Constitucional utiliza conceitos extremamente amplos, como intimidade e vida privada –, é evidente que o resguardo de dados se inclui no escopo de proteção à personalidade da CF/1988. Nesse sentido, afirma Laura Mendes:

> Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos "tradicionais",

[18] DONEDA, Danilo. "Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade", in TEPEDINO, Gustavo (coord.). *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar: 2000, p. 119.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

> que ensejaram o nascimento desse direito, como a hipótese de ser flagrado por paparazzi ou de ser notícia de jornais sensacionalistas. Assim, se não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos.[19]

Além disso, destaca-se que a proteção de dados pode ser identificada na Constituição Federal a partir do artigo 5º, LXXII, referente à concessão de *habeas data* como meio de os cidadãos acessarem ou corrigirem dados referentes a si mesmos.

Ora, se o Texto Constitucional garante a efetividade processual de determinado direito fundamental, é lógico concluir que sua dimensão material está igualmente protegida, ainda que não haja previsão expressa nesse sentido, conforme observado por Sepúlveda Pertence:

> É preciso ver que o sentido da criação dessa consagração explícita do habeas data tem menos a utilidade de uma criação de instrumentos processuais, que a rigor seriam desnecessários, do que de dar ênfase ao direito substancial, assegurado o acesso de qualquer cidadão aos dados sobre a pessoa do impetrante, constates de registros ou bancos de dados de entidades governamentais ou de caráter público, ou direito à retificação compulsória dos dados inexatos

A propósito, vale ressaltar que há precedente do Supremo Tribunal Federal em que se reconheceu essa perspectiva mais ampla da concessão de *habeas data*. Trata-se do RE 673.707/MG, julgado em 17/06/2017 sob a relatoria do Exmo. Ministro Luiz Fux, em que se discutia a possibilidade de um contribuinte acessar ao Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil (SINCOR). Nessa oportunidade, o Ministro Relator ressaltou que:

[19] MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. P. 201.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

> [...] aos contribuintes foi assegurado o direito de conhecer as informações que lhes digam respeito em bancos de dados públicos ou de caráter público, em razão da necessidade de preservar o status de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente, dentre outras. Consectariamente, estas informações não são de uso privativo do órgão ou entidade produtora ou depositária das informações, a Receita Federal do Brasil, mas dizem respeito ao próprio contribuinte.

Ou seja, reconheceu-se que o *habeas data* poderia ser utilizado para garantir o direito à proteção de dados do indivíduo, haja vista seu necessário protagonismo no que diz respeito a seus próprios dados pessoais. Inclusive, essa tendência jurisprudencial protetiva foi mencionada expressamente pelo Ministro Gilmar Mendes em seu voto, veja-se:

> Ao lado disso, temos essa situação específica que diz respeito a um direito subjetivo material, à proteção de dados ou à proteção dessa autonomia. Daí, a importância, me parece, deste julgado, que pode ser, talvez, o marco inicial de uma vitalização do *habeas data*, numa percepção mais ampla, na medida em que hoje, para esse julgamento, eu tinha feito um levantamento de vários artigos sobre essa temática, já falando de um direito fundamental à autodeterminação informativa: Ana Maria Neves de Paiva Navarro, ou do próprio colega e amigo Ricardo Cueva, "Há um direito à autodeterminação informativa no Brasil?" Em suma, há já uma reflexão, não no campo procedimental processual, mas também no campo do direito material.

Despiciendo ilustrar a importância que os dados pessoais possuem na sociedade atual. Ao passo que os cidadãos são constantemente identificados, avaliados, monitorados por meio de seus dados pessoais, e quando um sem-número de serviços públicos e privados dependem ou mesmo são baseados no tratamento destes dados, cabe ao intérprete ler o conjunto de garantias constitucionais à luz destas práticas afim que as atualize e não acabe por propiciar o surgimento de uma espécie de "zona cinzenta", na qual garantias seriam arrefecidas por conta de uma mudança no cenário tecnológico que não teria sido acompanhada com atenção pelo jurista.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Um importante exemplo desta atualização da interpretação de garantias à luz do desenvolvimento tecnológico é dado por Lawrence Lessig, ao comentar um célebre voto do Juiz Louis Brandeis no caso *Olmstead v. United States*, em 1928. Lessig afirma que Brandeis "traduziu" a quarta emenda à Constituição norte-americana, cunhada em um ambiente anterior, para um novo panorama, ao qual novas possibilidades e ferramentas foram tornadas possíveis pelo desenvolvimento tecnológico - e que é obrigação do direito levar em conta estas mudanças:

> Brandeis reconheceu que a Quarta Emenda, conforme fora originalmente escrita, somente se aplicaria à invasão de propriedade (*trespass*). Porém, arguiu Brandeis, a emenda dispunha desta forma por que era somente assim, à época da sua redação, que a privacidade poderia ser invadida. Aqueles estes os pressupostos, porém estes pressupostos tinham mudado. Com esta mudança, prosseguia Brandeis, passava a ser responsabilidade da Corte interpretar a Emenda de forma que seu significado fosse preservado, consideradas as mudanças nas circunstâncias. Era necessário *traduzir* as proteções originais para um novo contexto, no qual as tecnologias para invasão da privacidade mudaram. Isto deveria ser feito, para Brandeis, aplicando-se a Quarta Emenda em situações que não eram literalmente de invasão de propriedade[20].

No caso da decisão da Corte Constitucional alemã, o seu ponto de partida é justamente o processamento eletrônico de dados que, em virtude do moderno desenvolvimento tecnológico, possibilitou o processamento ilimitado, a armazenagem e transmissão de dados pessoais em proporções até então desconhecidas. De acordo com o Tribunal, as condições tecnológicas e sociais modificadas requerem o desenvolvimento continuado da interpretação da proteção pelos direitos fundamentais para que as novas ameaças possam ser superadas. (BVerfGE 65,1 (45), Recenseamento (Volkszählung).

Por fim, a centralidade do direito fundamental à proteção de dados dentre as garantias individuais hoje deixou de ser um efeito da proteção da privacidade para ser uma garantia mais ampla e

[20] LESSIG, Lawrence. *Code and other laws of cyberspace.* New York: Basic Books, 1999, p. 115. (trad. livre).

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

instrumental para a fruição de diversos outros direitos, confirme observa o professor Stefano Rodotà:

> A proteção de dados pessoais constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea. Relembrar isto a cada momento não é mera retórica, pois toda mudança que afeta a proteção de dados tem impacto sobre o grau de democracia que nós podemos experimentar[21].

O mesmo Rodotà especifica que:

> Sem uma forte tutela das suas informações pessoais, as pessoas correm cada vez mais risco de serem discriminadas por suas opiniões, crenças religiosas, condição de saúde, etc. A privacidade, neste sentido, apresenta-se como um elemento fundamental para a "sociedade da igualdade". Sem uma tutela forte dos seus dados a respeito de suas relações com instituições, com partidos políticos, sindicatos, associações, movimentos, os cidadãos correm o risco de serem excluídos dos processos democráticos: e, assim, a privacidade se torna uma condição essencial para se estar incluído em uma "sociedade da participação". Sem uma tutela forte do "corpo eletrônico", do conjunto de informações que se pode reunir a nosso respeito, a própria liberdade pessoal está em perigo e nos aproximamos perigosamente de uma sociedade da vigilância, da classificação, da seleção social: e, assim, fica evidente que a privacidade é um instrumento necessário para salvaguardarmos a "sociedade da liberdade". E, sem uma resistência contínua às micro violações, aos controles contínuos, capilares, opressivos e invisíveis que invadem a nossa vida cotidiana, encontraremo-nos nus e fracos diante de poderes públicos e privados: a privacidade, desta forma, se específica como componente inafastável da "sociedade da dignidade[22].

Portanto, a partir de uma interpretação sistemática da Constituição Federal de 1988, bem como com a devida consideração de que as tecnologias para tratamento de dados pessoais fazem destes a verdadeira nova fronteira na qual os contornos da privacidade e da

[21] RODOTÀ, Stefano. *A vida na sociedade da vigilância. A privacidade hoje.* Trad. Danilo Doneda e Luciana Cabral. Rio de Janeiro: Renovar, 2008, p.21.
[22] RODOTÀ, Stefano. *Intervista su privacy e libertà.* Bari: Laterza, 2005, pp. 148-149. (trad. livre).

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

própria personalidade são delineados, é possível identificar de maneira clara a existência de direito fundamental à proteção de dados, inserido no contexto de valorização da dignidade da pessoa humana e dos direitos de personalidade, bem como na condição de direito material decorrente da garantia processual ao *habeas data*.

c) Dos princípios que decorrem do direito constitucional à proteção de dados.

Feita a verificação de que o direito à proteção dos dados pessoais encontra amparo imediato na Constituição Federal, incumbe agora perquirir quais são os princípios que decorrem da aplicação desse direito.

Nessa direção, vale ressaltar que concomitantemente ao desenvolvimento do conceito do direito à proteção de dados pessoais, estabeleceu-se uma convergência internacional em torno dos princípios que devem nortear as atividades de tratamento de dados.

Como aponta Colin Bennett, esse quadro comum de princípios é conhecido como "*Fair Information Principles*" e teve origem na década de 1970[23]. A análise da legislação infraconstitucional brasileira, notadamente a Lei n. 12.965/2014 (Marco Civil da Internet) e da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados), revela de forma inequívoca que tais princípios foram albergados também pelo ordenamento jurídico pátrio.

Pode-se apresentar como primeiro princípio que rege as atividades de tratamento de dados[24] o **princípio da finalidade,** o qual prevê que essa atividade deverá ser realizada para propósitos legítimos, específicos, explícitos e informados ao titular, bem como veda a sua

[23] BENNETT, Colin. *Regulating Privacy:* data protections and public policy in Europe and the United States. Cornell University Press, 2018, p. 111.

[24] Importante esclarecer que o termo "tratamento de dados" é aqui utilizado no sentido que lhe é conferido pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018) em seu art. 5º, X: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

utilização para atividades posteriores incompatíveis com as finalidades informadas no momento da coleta dos dados:

> Esse princípio busca assegurar que os titulares de dados terão alguma forma de controle sobre os usos atribuídos aos seus dados, ao mesmo tempo em que permite aos controladores alguma flexibilidade em relação aos usos futuros - é autorizada a utilização para novas finalidades, desde que sejam legítimas e compatíveis com as finalidades originalmente informadas ao titular de dados.[25]

Os contornos do princípio da finalidade já haviam sido albergados pelo Marco Civil da Internet, nos seguintes termos:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> (...)
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> (...)
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; [...].

O preceito foi também conceituado pelo art. 6º, I da Lei Geral de Proteção de Dados como a "*realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com tais finalidades*".

A partir dessas construções, verifica-se que o princípio da finalidade impõe ao responsável pelo tratamento de dados a exposição, de forma expressa e específica, dos propósitos de tal atividade[26], eis que o tratamento realizado com base na comunicação de finalidades amplas e genéricas pode dar azo a vulnerações ao direito à proteção de dados.

---

[25] ADAMI, Mateus Piva et al. Tratamento de dados pessoais pela administração pública: análise do Serpro. Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018. Belo Horizonte: Fórum, 2019, p. 193-224.

[26] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 71

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Nessa direção, importa ressaltar que, em se tratando do processamento de dados pelo setor público, o princípio resta, ainda, atrelado à finalidade que lhe é dada por lei:

> O uso dos dados está restrito **à finalidade prevista em lei.** Já tendo em vista os perigos do processamento eletrônico de dados, é necessária uma proteção (...) contra o afastamento do propósito inicial de levantamento de dados, mediante proibição de transmissão e de utilização[27].

No ordenamento jurídico pátrio, essa conclusão deriva com clareza ainda maior do art. 37 da Constituição Federal, que submete toda a atuação da Administração Pública ao princípio da legalidade.

Com efeito, tendo em vista o risco inerente ao tratamento de dados pessoais, que pode afetar diretamente direitos de personalidade do cidadão, a sua realização pelo poder público exige previsão em lei de sua finalidade específica.

Outra decorrência do princípio da finalidade é a limitação do acesso de terceiros ao banco de dados detido por determinada entidade, eis que, caso ele seja deferido, deve-se garantir que o uso a ser realizado por este terceiro não divirja da finalidade para a qual o dado foi originalmente coletado.

O **princípio da transparência,** por sua vez, apresenta a necessidade de sejam fornecidas informações "claras, precisas e facilmente acessíveis sobre as atividades de tratamento de dados pessoais realizadas"[28].

Desse princípio decorre, portanto, a obrigação de que a existência de sistemas de manutenção de registros ou bancos de dados seja de conhecimento público, com a especificação do conteúdo mantido

---

[27] SCHWABE, Jürgen; MARTINS, Leonardo. Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Konrad-Adenauer-Stiftung, 2005. BVERFGE 65, 1. P. 240.

[28] ADAMI, Mateus Piva et al.. Tratamento de dados pessoais pela administração pública: análise do Serpro. Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018. Belo Horizonte: Fórum, 2019, p. 193-224.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

e da forma como esses dados podem ser utilizados[29], fatores que denotam a sua essencialidade para o *accountability* dos bancos de dados.

O princípio também abarca a disponibilização de informações acerca de controles implementados para endereçar os riscos a que está sujeito o tratamento de dados, bem como as vias pelas quais o titular pode apresentar perguntas e requerimentos para exercer seus direitos à proteção de dados.

Como explica Bennett, subjacente a este princípio está a crença de que a as complexidades e riscos do ambiente de processamento de informações podem ser mitigados se a natureza e a finalidade dessas atividades estiverem submetidas à arena pública[30].

O referido princípio foi normatizado pelo já citado art. 7º, VIII, do Marco Civil da Internet e foi também expressamente albergado pela LGPD, no inciso VI, do art. 6º, que assim o descreveu: "*garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial*".

O **princípio da necessidade** expressa a máxima de que a coleta e manutenção de dados pessoais deve se limitar àqueles dados estritamente *relevantes* e *necessários* para os propósitos a que se dirige. O referido princípio dialoga diretamente com o princípio a finalidade, eis que alberga a exigência de que a coleta e tratamento de dados pessoais seja adequada, pertinente e não excessiva em relação à sua finalidade.

O conteúdo do princípio da necessidade e sua correlação com o princípio da finalidade foram muito bem expostos no já mencionado precedente da Corte Constitucional alemã, em que fixado o direito dos cidadãos à "autodeterminação informativa":

[29] BENNETT, Colin. *Regulating Privacy:* data protections and public policy in Europe and the United States. Cornell University Press, 2018, p. 101.

[30] BENNETT, Colin. *Regulating Privacy:* data protections and public policy in Europe and the United States. Cornell University Press, 2018, p. 103.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

> A obrigação de fornecer dados pessoais pressupõe que o legislador defina **a finalidade de uso por área e de forma precisa, e que os dados sejam adequados e necessários para essa finalidade**. Com isso não seria compatível a armazenagem de dados reunidos, não anônimos, para fins indeterminados ou ainda indetermináveis. **Todas as autoridades que reúnem dados pessoais para cumprir suas tarefas devem se restringir ao mínimo indispensável para alcançar seu objetivo definido.**[31]

O preceito foi descrito pela LGPD como a "*limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.*"

O princípio da necessidade volta-se a impedir a chamada "pesca de dados" (*fishing expeditions*), indicando que a coleta de dados pessoais deve ser realizada apenas na medida para atender os propósitos específicos de seu tratamento.

Outro relevante princípio da proteção de dados é o **princípio da qualidade de dados,** que se refere à exigência de que os dados objeto de tratamento sejam exatos, completos e atualizados.

Esse princípio impõe ao detentor de bases de dados cautela em sua formação e manutenção e dele decorre a necessidade de se garantir direitos de acesso, retificação e cancelamento de dados por seus titulares. Em consonância com esse princípio, a LGPD previu ao titular de dados pessoais o direito de obter do controlador do banco de dados "*correção de dados incompletos, inexatos ou desatualizados*" (art. 18, III).

Destaca-se ainda, dentre os princípios da proteção de dados o **princípio da segurança,** que reflete a necessidade de que qualquer banco de dados pessoais esteja guarnecido de ferramentas capazes de garantir segurança razoável aos dados ali mantidos.

---

[31] SCHWABE, Jürgen; MARTINS, Leonardo. Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Konrad-Adenauer-Stiftung, 2005. BVERFGE 65, 1. P. 240.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

O princípio encontrava-se expresso no Guia sobre Proteção da Privacidade e Fluxos de Informação Transfronteiriços de Dados Pessoais da OCDE editado pela OCDE ainda no ano de 1981, com a seguinte enunciação: "*dados pessoais devem ser protegidos por garantias razoáveis de segurança contra riscos como perda ou acesso não autorizado, destruição, uso, modificação ou divulgação de dados*"[32].

Também esse princípio foi expressamente tratado pela LGPD aprovada em 2018. Em seu art. 6º, VII, a Lei n. 13.709/2018, dispõe que dentre os princípios a serem observados no tratamento de dados estão o da segurança, compreendido como a "*utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão*".

Ressalte-se, ainda que alguns destes princípios relacionados à proteção de dados pessoais integram também outras normas específicas, como por exemplo a Lei n. 12.414/2011, conhecida como Lei do Cadastro Positivo, aplicável aos dados em bancos de dados com históricos de adimplemento. Nesta, são verificáveis os princípios da finalidade (art. 2º, I e 5º, VII), transparência (art. 5º, II), necessidade (art. 3º, § 1º), qualidade (art. 3º, § 2º, I a III) e segurança (art. 5º, II e 7º, parágrafo único).

Por fim, vale ressaltar que, a toda evidência, quanto maior a sensibilidade dos dados tratados, mais cuidadosas devem ser as medidas de segurança adotadas para resguardá-los.

Apresentados, portanto, os princípios cunhados transnacionalmente, que fixam as balizas para o tratamento de dados em consonância com a dignidade da pessoa humana e a garantia da autodeterminação informativa, passa-se a analisar o ato normativo ora impugnado à luz dos referidos princípios, o que permitirá demonstrar que a norma vulnera, de maneira escancarada e inaceitável, o direito constitucional à proteção de dados de milhões de cidadãos brasileiros.

[32] OCDE. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris, 1981. Tradução livre.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

VI. DOS VÍCIOS DE INCONSTITUCIONALIDADE DA MPV n. 954. INOBSERVÂNCIA AOS PRINCÍPIOS ELEMENTARES DA PROTEÇÃO DE DADOS.

a) Enorme amplitude das finalidades previstas pelo art. 2º, §1º. Impossibilidade aferição dos propósitos específicos da transferência de dados imposta pela norma.

Como ressaltado, a observância ao princípio da **finalidade** consubstancia sustentáculo do exercício da autodeterminação informada de dados pessoais, na medida em que permite ao titular ter acesso a informações essenciais para exercer juízo de conveniência e oportunidade acerca dos propósitos para os quais os seus dados serão utilizados.

Ao analisar a MPV n. 954 de 17 de abril de 2020, contudo, verifica-se que a norma foi extremamente **inespecífica** ao tratar das finalidades para as quais serão empregados os dados cuja transferência é requerida. Veja-se:

> Art. 2º As 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.
> § 1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE **para a produção estatística oficial,** com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

O caráter vago e inespecífico do dispositivo acerca dos propósitos da operação por ele determinada carece de maior explanação!

Como já ressaltado, o IBGE é responsável pela produção de **diversas estatísticas oficiais,** seja a partir da Pesquisa Nacional por Amostra de Domicílios (PNAD), do Sistema Nacional de índices de Preços ao Consumidor (SNIPC) ou pesquisas econômicas de indústria, comércio e serviços (PIM, PMC, PMS, IPP, SINAPI). E, se o Governo Federal chegou ao ponto de editar ato normativo para obter **nome, telefone e endereço de centenas de milhões de brasileiros,** é de se esperar que tenha clareza acerca dos propósitos capazes de justificar medida tão intrusiva.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Esta maior clareza, além de permitir o atendimento ao princípio da finalidade, proporcionaria também que o princípio da necessidade fosse atendido, já que, sabendo-se os objetivos almejados, torna-se possível prescrever o *quantum* de informação é necessária para o atingimento do objetivo, evitando-se o risco de repasse de informações excessivas

Tais propósitos, entretanto, não restaram minimamente espelhados nas disposições da MPV n. 954.

Diante do cenário ora colocado, não é apenas razoável, mas imprescindível que haja clara delimitação e explicitação das finalidades pretendidas com essa massiva transferência de dados à entidade governamental.

A corroborar tal entendimento, vale invocar mais uma vez os termos da decisão proferida pela Corte Constitucional alemã no precedente de 1983:

> Só quando existe clareza sobre a finalidade para a qual os dados são solicitados e quais são as possibilidades de uso e ligação [destes com outros] que existem, pode-se saber se a restrição do direito de autodeterminação da informação (no caso) é admissível[33].

A atemporalidade do referido precedente evidencia-se ainda quando se tem em conta que, em recente estudo elaborado pelo *Centre for Information Policy Leadership* (CIPL)[34] – para analisar as providências básicas de *accountability* a serem empregadas para possibilitar a coleta, uso e compartilhamento **responsável** de dados pessoais na luta contra o COVID-19, apresentou-se como **primeira medida** a seguinte:

[33] SCHWABE, Jürgen; MARTINS, Leonardo. Cinqüenta anos de jurisprudência do Tribunal Constitutional Federal Alemão. Konrad-Adenauer-Stiftung, 2005. BVERFGE 65, 1. P. 239.

[34] O Centre for *Information Policy Leadership* é uma entidade reconhecida globalmente no desenvolvimento de soluções e melhores práticas para o direito à privacidade e proteção de dados.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

> **Propósitos claramente definidos e documentados para a utilização de dados**
> Cada projeto proposto deve definir claramente objetivos para ajustar os limites do que pode e deve ser feito com os dados e para que fins. As finalidades propostas para os dados devem ser apoiados por evidência de que o uso de dados realmente trata uma necessidade particular[35].

Em sentido totalmente contrário a tal orientação, a norma ora impugnada confere verdadeiro "cheque em branco" para a utilização dos referidos dados pela Fundação Instituto Brasileiro de Geografia Estatística, limitando-os unicamente propósito genérico de "produção de estatística oficial".

Incumbe salientar que a vagueza da disposição normativa impede, inclusive, a realização de um juízo efetivo acerca da imprescindibilidade da coleta massiva de dados pessoais dos cidadãos brasileiros pela agência governamental.

De fato, diante do caráter genérico da finalidade prevista pela MPV n. 954, resta absolutamente inviabilizada qualquer ponderação acerca da proporcionalidade entre os dados requeridos e os propósitos pretendidos com sua utilização, o que não se pode admitir.

Assim, diante da evidente vulneração ao princípio da finalidade, o qual decorre diretamente do direito constitucional à proteção de dados, resta patente a incompatibilidade do art. 2º, §1º da MPV n. 954, de 17 de abril de 2020, com a Constituição Federal.

[35] BELLAMY, Bojana. Covid-19 meets privacy: a case study for accountability. CIPL. Disponível em: <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/04/covid-19_meets_privacy_a_case_study_for_accountability_-_centre_for_information_policy_leadership__april_2020_.pdf>. Acesso em 19 abr. 2020. Tradução livre.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

b) Da ausência de indicação de necessidade a justificar a requisição de tão grande quantidade de dados com tamanho detalhamento e em prazo tremendamente exíguo. Patente desproporcionalidade da medida.

Não bastasse a ausência de delimitação de finalidade que, como exposto, seria imprescindível para o processamento de dados de forma legítima pelo poder público, o *caput* do art. 2º, da MPV n. 954, ao prever o compartilhamento de nome, telefone e endereço de milhões de brasileiros vulnera o princípio da necessidade, reforçando a inconstitucionalidade que eiva o referido ato normativo, conforme se passa a demonstrar.

O dispositivo em questão possui a seguinte redação:

> Art. 2º As 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.

Na esteira do que exposto na seção anterior, o princípio da especificidade exige que a quantidade e a forma de realização do processamento de dados sejam **relevantes, necessárias e proporcionais** aos objetivos visados.

Diante disso, a salvaguarda ao direito constitucional à proteção de dados impõe que o seu processamento seja precedido de questionamentos como: *(i)* é possível alcançar esse mesmo objetivo com menor quantidade de dados, ou, alternativamente, por meio da utilização de dados agregados ou complemente anônimos? *(ii)* o processamento de dados proposto é uma resposta proporcional para o objetivo que estamos buscando atingir?

Como já ressaltado no tópico anterior, a ausência de indicação da finalidade específica visada com o compartilhamento na MPV n. 954 impede a realização de qualquer juízo efetivo de proporcionalidade, o que, por si só, já denota a violação às salvaguardas constitucionais conferidas à privacidade e à autodeterminação informativa.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Todavia, ainda que se realize um esforço para sopesar a necessidade de tais insumos para o desenvolvimento de atividades estatísticas pelo IBGE e a sensibilidade dos dados requisitados das *telecons,* resta notória a desproporcionalidade da medida em tela.

Com efeito, é imperioso ressaltar que a determinação de compartilhamento realizada pela Medida Provisória diz respeito a **dados não anônimos** e que permitem a verificação do **local de residência** de seus titulares, configurando-se inequivocamente como dados **altamente relevantes** e, portanto, merecedores da mais elevada proteção.

De outro lado, a necessidade de tais dados pelo IBGE resta de todo controvertida quando se tem em vista que o referido Instituto, antes mesmo da edição da malfadada medida provisória, já havia publicado em sua página na internet comunicado no qual informava que as investigações referentes às suas principais pesquisas passariam a ser realizadas de maneira remota[36]:

(i) PNAD contínua: visando manter a produção de estatísticas relacionadas ao mercado de trabalho, o IBGE optou por manter a coleta de informações da pesquisa através de telefone. Segundo o instituto, *"cerca de 2 mil entrevistadores estão trabalhando em suas residências,* ***telefonando para os domicílios selecionados que fazem parte da amostra da pesquisa****. Aproximadamente 70 mil domicílios (mês) fazem parte da amostra pesquisa"*.

(ii) INPC: no que tange à a coleta de preços referente ao Sistema Nacional de Índices de Preços ao Consumidor, o IBGE decidiu que esses passariam a ser coletados manualmente pela internet ou pelo telefone. O instituto informa que *"a coleta é atualmente realizada em mais de 33.000 locais de compra nas 16 áreas de abrangência do índice, com cerca de 590.000 preços coletados por mês.* ***Os entrevistadores seguem trabalhando remotamente e inserindo os preços coletados online nos equipamentos de coleta****"* e *"adicionalmente,* ***mantém-se a coleta online de preços por robô****, implementada a partir de janeiro deste ano"*.

[36] Disponível em https://respondendo.ibge.gov.br/coleta-por-telefone.html. Acesso em 19/04/2020.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

(iii) Pesquisas econômicas de indústria, comércio e serviços: o IBGE nos comunicou que *"as pesquisas econômicas anuais de indústria, comércio e serviços feitas em empresas,* ***permanecem utilizando os questionários eletrônicos auto preenchidos*** *como a principal forma de coleta de dados junto aos informantes. Para uma parcela pequena, que solicitava responder presencialmente, serão intensificados os pedidos de resposta por telefone"*. Para viabilizar essa coleta, *"os funcionários do IBGE, nas 27 Unidades da Federação, estão executando as atividades operacionais descentralizadas* ***pelo telefone e por e-mail****."*

Ora, pelo que se pode depreender do referido informativo, o IBGE **já possuía meios de continuar conduzindo as duas principais pesquisas estatísticas** com os dados de que dispunha previamente.

Chama a atenção ainda o fato de que as pesquisas estatísticas efetivadas pelo IBGE são realizadas de forma amostral. Nessa esteira, o Instituto informa no comunicado supratranscrito que para a realização do PNAD, por exemplo, são entrevistadas cerca de 70 mil pessoas por mês. Diante desse quadro, colocam-se fundadas dúvidas acerca da efetiva necessidade de obtenção dos dados de quase de **260 milhões** de contas de telefonia fixa e móvel.

Além disso, há diversas pesquisas do IBGE que, mesmo antes da pandemia, já eram realizadas de forma remota através do Centro de Entrevista Telefônica Assistida por Computador (CETAC), o que também corrobora a capacidade do Instituto de manter suas atividades de pesquisa nesse cenário.

Ressalte-se, ainda, para a extrema exiguidade dos prazos para a elaboração dos procedimentos necessários para a disponibilização dos dados e para sua efetiva disponibilização, nos parágrafos 2º e 3_ do artigo 2º:

> § 2o Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o caput .
> § 3o Os dados deverão ser disponibilizados no prazo de:

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

> I - sete dias, contado da data de publicação do ato de que trata o § 2o; e
> II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes.

A exiguidade dos referidos prazos, além de não encontrar justificativa específica, atenta gravemente aos direitos dos titulares dos dados no sentido em que, potencialmente, os efeitos da disponibilização dos dados podem se produzir ainda que a Medida Provisória não seja convertida em Lei ou, o sendo, sofra modificação. Neste caso, ainda que se proceda à eliminação dos dados disponibilizados, persiste o risco de que tenham sido alvos de falha de segurança ou outra modalidade de má utilização pela ausência de salvaguardas específicas. Este ponto, em particular, implica na extrema sensibilidade do fator tempo para o presente pedido.

Em suma, a partir de todas essas circunstâncias é inevitável a conclusão de que a determinação do compartilhamento de dados altamente relevantes em tão vasta quantidade **não se justifica minimamente** na hipótese em apreço.

Evidenciada a desproporcionalidade entre o processamento de dados imposto pela MPV n. 954 e a sua finalidade, há se reconhecer a inconstitucionalidade da referida medida, por frontal violação ao direito constitucional à proteção de dados.

c) Da ausência de adoção de medidas de segurança minimamente razoáveis para o tratamento de dados tão relevantes.

Por fim, é necessário expor também a absoluta ausência de especificação, pela medida de provisória, de qualquer providência voltada a garantir níveis adequados de segurança ao processamento massivo de dados pessoais totalmente identificados por ela determinado.

Com efeito, a Medida Provisória se limita a afirmar que os dados deverão ser disponibilizados por meio eletrônico e delega ao Presidente da Fundação IBGE, após ouvida a Agência Nacional de Telecomunicações, a regulamentação dos procedimentos para a disponibilização dos dados, **sem lhe imputar qualquer ônus no sentido**

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

de apresentar evidências de que a metodologia escolhida possui salvaguardas compatíveis com a dimensão dos dados a serem processados.

A ausência de observância mínima ao princípio da segurança resta ainda mais evidente quando, em uma frustrada tentativa de dar ares de cautela à medida adotada, o ato normativo aduz que a Fundação IBGE irá divulgar relatório de impacto à proteção de dados pessoais, nos termos em que previsto pela LGPD:

> Art. 3º
> (...)
> § 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no *caput* do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.

Com o devido acatamento, mas na situação concreta, de que adiantaria a divulgação de relatório de impacto quando já ultimada a transferência de dados para a entidade governamental?

É notório que a segurança e higidez do processamento dos dados deve ser objeto de estudo devidamente evidenciado e publicizado, que permita a contraposição de riscos identificados e benefícios a serem alcançados **antes** da efetivação da transferência dos dados requerida pela MP.

Esta inversão, na prática, relega o referido relatório a uma função essencialmente ornamental, visto que os efeitos cujos riscos o relatório visaria identificar e auxiliar a mitigar, já teriam todos sido concretizados, fazendo com que se tenha fundada desconfiança da seriedade com que a segurança e os direitos do titular dos dados seriam levados em consideração.

É preciso dar garantia à sociedade brasileira de que a Fundação receptora possui meios adequados para manter a segurança dos dados a ela endereçados, para que só então alguma medida de compartilhamento possa ser efetivada.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

d) da situação de vulnerabilidade a que são relegados os cidadãos titulares dos dados pessoais ante à inexistência de instrumentos e instituições capazes de supervisionar o tratamento dos dados

Uma das características específicas dos tratamentos de dados pessoais que justificaram e fundamentaram a edição de normativas específicas para a proteção de dados pessoais é a sua opacidade.

A imaterialidade dos dados pessoais e a crescente disponibilidade de meios para sua coleta, armazenamento e tratamento sugerem fortemente que a tarefa de evitar abusos na sua utilização não podem ser confiadas apenas ao cidadão em relação aos seus próprios dados, porém deve ser robustecida com instrumentos jurídicos específicos, na forma das normas de proteção de dados, com como com estruturas capazes de realizar a supervisão e monitoramento dos tratamentos de dados.

Estas estruturas são essenciais por serem a única forma de suprir uma vulnerabilidade que é, no caso, conjuntural ao cidadão pela crescente impossibilidade de acompanhar tecnicamente e mesmo quanto ao volume, as características dos tratamentos de seus dados pessoais, bem como de perceber os efeitos que poderiam ter em sua vida.

Para compensar esta vulnerabilidade, a LGPD, no rastro das legislações mais modernas na área, procura introduzir tanto mecanismos que obriguem as organizações que tratem dados pessoais a documentar, avaliar riscos e ser transparente sobre seu uso, quando institui um órgão cuja função é especificamente fiscalizar o cumprimento da lei, a Autoridade Nacional de Proteção de Dados (ANPD).

A MPV 957/2020, apesar de que, paradoxalmente, se referir à LGPD em seu art. 2º, § 2º, tem sua entrada em vigor antes da referida norma (que somente entrará em vigor em agosto de 2020), portanto os tratamentos de dados pessoais que proporcionaria não estariam sujeitos à supervisão e monitoramento de ente especializado, proporcionando risco desproporcional que só vem a agravar a vulnerabilidade dos cidadãos titulares dos dados pessoais .

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Ressalte-se, por fim, que não se desconhece a enorme relevância dos serviços prestados pelo Instituto de Geografia Estatística à sociedade brasileira, nem tampouco o papel central que a referida entidade pode desempenhar nas medidas de combate ao Covid-19.

Entretanto, essas circunstâncias não são capazes de afastar a necessidade de que eventual compartilhamento de dados a ser realizado com o órgão governamental esteja estritamente aderente aos princípios que norteiam o direito fundamento à proteção de dados.

Por tudo o que se expôs acima, no caso específico da MPV n. 954, restam patentes e inequívocas as graves violações perpetradas pela norma contra os princípios da finalidade, da necessidade e da segurança.

Tais vulnerações, ao violar o direito constitucional à proteção de dados, resulta em inequívoca afronta à inviolabilidade da intimidade e da vida privada (art. 5º, X, CF), à dignidade da pessoa humana (art. 1º, III, CF) e à garantia do *habeas data* (art. 5º, LXXII), preceitos especialmente resguardados pela Constituição Federal.

Por essas razões é que se requer a declaração de inconstitucionalidade do art. 2º, *caput* e §1º - § 3º, bem como art. 3º da Medida Provisória n. 954, de 17 de abril de 1917, de modo a impedir que se consumem os deletérios impactos que o abusivo ato normativo editado pelo Poder Executivo Federal tem potencial de causar aos usuários das 226,6 milhões de linhas de telefonia móvel e aos 32,8 milhões de portadores de linhas de telefonia fixa[37]

VII. DA MEDIDA CAUTELAR.

Na hipótese em apreço, faz-se imperioso o deferimento de medida cautelar para **suspender liminarmente a eficácia** dos dispositivos ora impgunados da Medida Provisória n. 954, de 17 de abril de 2020.

[37] Segundo dados da Agência Nacional de Telecomunicações, disponível em https://www.anatel.gov.br/paineis/acessos/telefonia-movel e https://www.anatel.gov.br/paineis/acessos/telefonia-fixa. Acesso em 19 abr. 2020

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Primeiramente, verifica-se o atendimento ao requisito do ***fumus boni iuris***, como se demonstrou acima, pela flagrante violação ao direito constitucional à proteção de dados, amparado pela redação e pela interpretação sistemática dos artigos 1º, III, e 5º, X e LXXII, da Constituição Federal.

Com efeito, restou sobejamente demonstrada a violação às salvaguardas constitucionais conferidas à privacidade e à autodeterminação informativa em decorrência do caráter vago e inespecífico das finalidades que ensejam a operação determinada pela MP n. 954, de 17 de abril de 2020.

Além disso, evidenciou-se a desproporcionalidade da medida, ante a ausência de adequação e pertinência para o compartilhamento de dados pessoais tão relevantes e em tamanha quantidade, bem como a absoluta ausência de especificação de qualquer providência voltada a garantir níveis adequados de segurança ao processamento destes.

O ***periculum in mora***, por sua vez, revela-se patente eis que os efeitos da Medida Provisória impugnada se exaurem no exato momento em que ocorre a liberação dos dados pessoais sobre os quais ela dispõe, de maneira que, após efetivada a previsão constante na medida, impossível o retorno ao *status quo ante*.

Agravando esse cenário, tem-se que a MPV n. 954 surge em um contexto no qual inexiste qualquer dispositivo legal que discipline a proteção de dados no setor público – vez que a Lei Geral de Proteção de Dados ainda aguarda o início de sua vigência –, bem como suprime a participação do Congresso Nacional em debate sobre tema já desenvolvido pelo Poder Legislativo.

Destarte, os prazos extremamente exíguos previstos pela Medida Provisória (3 dias para a regulamentação do procedimento de disponibilização dos dados pelo Presidente da Fundação IBGE e 7 dias para a disponibilização dos dados) impediria a deliberação do ato pelo Congresso Nacional.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Esse fato fica patente quando se tem em vista que o prazo para a apresentação de emendas à MPV é de 6 (seis) dias e que, em seguida, prevê-se prazo de até 14 dias para que a Comissão Mista do Congresso possa emitir parecer sobre o ato normativo e, só então, ele passará a ser apreciado pelo Plenário da Câmara dos Deputados.

Portanto, ainda que imprimisse um ritmo extremamente célere à apreciação da Medida Provisória, o Congresso Nacional dificilmente teria a possibilidade de se manifestar sobre o ato antes da consumação irreversível de seus efeitos.

Ante tais circunstâncias, é possível verificar, mesmo em sede de cognição sumária, que a manutenção dos dispositivos em vigência implica graves danos à população brasileira como um todo, razão pela qual requer-se a imediata concessão da medida cautelar ora pleiteada.

VIII. DOS PEDIDOS.

Diante do exposto, requer-se seja conhecida a presente Ação para que, em razão das graves violações perpetradas pela Medida Provisória objeto desta Ação Direta:

a. liminarmente, nos termos do art. 10, da Lei n. 9.868/1999, seja concedida **medida cautelar** para a suspensão da vigência dos artigos 2º, *caput* e §1º a § 3º , e 3º da Medida Provisória n. 954, de 17 de abril de 2020;

b. no mérito, seja declarada a **inconstitucionalidade** dos artigos 2º, *caput* e §1ºa §3º, e 3º da Medida Provisória n. 954, de 17 de abril de 2020.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

Requer-se ainda que todas as intimações referentes ao presente feito sejam realizadas em nome do advogado **Rafael de Alencar Araripe Carneiro**, inscrito na OAB/DF sob o número 25.120, sob pena de nulidade.

Atribui-se à causa, para meros efeitos contábeis, o valor de R$ 100,00 (cem reais).

Nestes termos, pede deferimento.
Brasília, 20 de abril de 2020.

Rafael de Alencar Araripe Carneiro
OAB/DF 25.120

Danilo Doneda
OAB/RJ 156.590

Mariana Albuquerque Rabelo
OAB/DF 44.918

Arthur Vieira Duarte
OAB/DF 46.693

Gabriella Souza Cruz
OAB/DF 57.564

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002

CARNEIROS
ADVOGADOS

LISTA DE DOCUMENTOS

Doc. 01 – Comprovante de Inscrição e de Situação Cadastral perante a Receita Federal e Estatuto do Partido;

Doc. 02 – Procuração;

Doc. 03 - Lista de Deputados Federais e Senadores do PSB;

Doc. 04 – Medida Provisória n. 954, de 17 de abril de 2020.

SGAN Quadra 601, Bloco H, L2 Norte, Edifício ION - Sala 1035 | Brasília/DF - CEP: 70.830-018
Alameda Santos, nº 700, Conj. 131, 13º andar - Cerqueira César | São Paulo - CEP: 01.418-002