LAPIN
LABORATÓRIO DE POLÍTICAS PUBLICAS E INTERNET

EXCELENTÍSSIMO SENHOR MINISTRO DO SUPREMO TRIBUNAL FEDERAL GILMAR MENDES

Ação Direta de Inconstitucionalidade nº 6.649/DF

O **LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET – LAPIN**, doravante também denominado "**LAPIN**", já qualificado nos autos do processo em epígrafe, em parceria com a **COALIZÃO DIREITOS NA REDE - CDR**, vem, respeitosamente, perante Vossa Excelência, na qualidade de *AMICUS CURIAE*, apresentar

MANIFESTAÇÃO

nos termos do artigo 138, *caput*, do Código de Processo Civil (Lei nº 13.105/2015), c/c o artigo 323, §3º, do Regimento Interno do Supremo Tribunal Federal, pelos fatos e fundamentos a seguir.

LAPIN
LABORATÓRIO DE POLÍTICAS PUBLICAS E INTERNET

SUMÁRIO

I. BREVE SÍNTESE

a. Da Demanda

Trata-se de Ação Direta de Inconstitucionalidade (ADI) com pedido cautelar ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) em face da integralidade dos dispositivos estabelecidos pelo Decreto nº 10.046/2019 (Decreto). O Decreto trata do compartilhamento de dados no âmbito da Administração Pública federal, institui o Cadastro Base do Cidadão (CBC) e cria o Comitê Central de Governança de Dados (CCGD). A ADI defende a inconstitucionalidade do Decreto por violação do artigo 84, incisos IV e VI, 'a', da Constituição Federal (CF), e violação direta dos artigos 1º, *caput*, inciso II e 5º, *caput* e incisos X, XII e LXXII, da CF.

O requerente alega que o Decreto inova no ordenamento jurídico, extrapolando a competência regulamentar do Presidente da República. Conforme a inicial, o preâmbulo do Decreto dá a entender que o diploma regulamenta a Lei de Acesso à Informação (LAI - Lei nº 12.527/2011), o art. 11 da Lei de Identificação Civil Nacional (ICN - Lei nº 13.444/2017) e o Capítulo IV da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), que dispõe sobre o tratamento de dados pessoais pelo Poder Público. Porém, o requerente aduz que o Decreto na realidade contraria frontalmente diversos dispositivos das leis federais que alega regulamentar.

No mérito, o CFOAB expõe que o Decreto desrespeita os direitos humanos e o direito à proteção de dados ao institucionalizar um cadastro unificado que será compartilhado de forma praticamente livre pela Administração Pública federal. O Decreto também não disporia sobre mecanismos adequados de segurança da informação, situação alarmante em se tratando de um mecanismo que permite o acesso a grande volume de dados, com riscos de vazamentos e incidentes que podem comprometer de forma irreversível os direitos à privacidade, à proteção de dados e à autodeterminação informativa de todos os cidadãos brasileiros.

O requerente defende, ainda, que o Decreto viola a LGPD com seus níveis de governança subjetivos e inova ao trazer a figura de gestor de dados e criar novos conceitos de dados pessoais alheios à LGPD. Ademais, argumenta que o Decreto cria poderoso instrumento estatal para a criação de perfis de indivíduos com base em dados e realização de atividades de vigilância, colocando em risco a democracia.

Por fim, o requerente rogou pela concessão de medida cautelar determinando a suspensão imediata da eficácia do Decreto nº 10.046/2019 e do CBC, para, no mérito, julgar procedente a ADI de forma a declarar a inconstitucionalidade do Decreto.

Diante disto, o **Laboratório de Políticas Públicas e Internet - LAPIN vem, perante este Supremo Tribunal Federal, apresentar sua manifestação a respeito do tema**, visando contribuir por meio de subsídios técnicos a respeito da governança de dados pessoais na Administração Pública federal brasileira que assegure estrito respeito aos direitos fundamentais dos cidadãos brasileiros.

b. Desta Manifestação

Tendo em vista a relevância da matéria e a repercussão social que a controvérsia exerce sobre toda a população brasileira, esta manifestação explora:

1. a aplicação da LGPD no tratamento de dados pelo Poder Público (**Seção II**);
2. os níveis de compartilhamento previstos no Decreto nº 10.046/2019 (**Seção III**);
3. a experiência estrangeira no compartilhamento irrestrito de dados a nível nacional (**Seção IV**);
4. a segurança da informação no Estado Brasileiro (**Seção V**); e
5. as conclusões (**Seção VI**) dessa análise.

II. DA APLICAÇÃO DA LGPD NO TRATAMENTO DE DADOS PELO PODER PÚBLICO

a. Introdução aos Aspectos Legais e Técnico-operacionais do CBC

O Decreto nº 10.046/2019 busca guiar o compartilhamento de dados entre os órgãos e entidades da Administração Pública Federal, com a finalidade de

> "I - simplificar a oferta de serviços públicos; II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas; III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais; IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e V - aumentar a qualidade e a eficiência das operações internas da administração pública federal."[1]

Para tanto, o Decreto institui o Cadastro Base do Cidadão - CBC, uma base integradora[2] composta de componentes de interoperabilidade necessários para o intercâmbio de dados entre a base do CBC com as bases temáticas[3], com o objetivo de servir como base de referência de informações sobre os cidadãos para os órgãos e entidades do Poder Executivo Federal (art. 17 do Decreto nº 10.046/2019).

Para guiar seus utilizadores a respeito de como definir as permissões de acesso a bases de dados que cada servidor tem, foram definidos os chamados "níveis de compartilhamento de dados", detalhados nos Capítulos II e III do Decreto.

Com isso, vale se ter em mente que o CBC não se trata de uma base única, centralizada, de dados, mas de um ponto a partir do qual é possível ter acesso a uma série de bases geridas pela Administração Pública federal. Tal noção é importante para as considerações que virão a seguir ao longo desta peça.

---

[1] Decreto nº 10;046/2019, artigo 6º.
[2] Uma base integradora é definida pelo art. 2º, VI, do Decreto nº 10.046/2019 como uma "base de dados que integra os atributos biográficos ou biométricos das bases temáticas".
[3] Uma base temática é definida pelo art. 2º, VII, do Decreto nº 10.046/2019 como uma "base de dados de determinada política pública que contenha dados biográficos ou biométricos que possam compor a base integradora".

b. O Direito Fundamental à Proteção de Dados

A disciplina da proteção de dados surgiu na Europa e nos Estados Unidos da América (EUA) na década de 1960.[4] Tal como aprofundado na Seção IV desta manifestação, nessa época discutia-se a criação de bases de dados nacionais centralizadas com a finalidade genérica de execução de políticas públicas. No Brasil, esse debate se intensificou nos últimos anos, principalmente com o andamento dos diálogos referentes à LGPD.

O tratamento de dados pessoais pelo Poder Público é indispensável para o cumprimento das funções delegadas ao Estado pela Constituição. Dele decorrem todas as políticas públicas que o Estado desenvolve, implementa e avalia, além da prestação de serviços públicos essenciais e execução de competências legais. Pelo fato de dados pessoais serem imprescindíveis para a atividade estatal, as diretrizes de proteção de dados incidem de forma diversa em entes públicos e em entes privados.

A Lei Geral de Proteção de Dados - LGPD, marco da disciplina da proteção de dados no Brasil, foi promulgada e sancionada em 2018 e está vigente desde setembro de 2020. Já o **direito fundamental autônomo à proteção de dados pessoais** foi reconhecido em decisão recente deste e. Supremo Tribunal Federal, no julgamento da Medida Cautelar nas ADIs nº 6.387, 6.388, 6.389, 6.393 e 6.390 (doravante referenciadas "ADI nº 6.387")[5].

De forma geral, o tratamento de dados pelo Poder Público só deve ser conduzido quando for **necessário** para a execução de suas competências e atribuições legais. Esses princípios coexistem com normas setoriais, as quais podem trazer previsões específicas não abarcadas pela construção geral da LGPD.

---

[4] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados, 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

[5] MENDES, Laura S. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais**. Jota, 10 mai. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em 20 fev. 2021.

De acordo com Ana Frazão[6], a LGPD deve servir como **fio condutor** a outras estratégias de regulação (*i.e.* autorregulação e corregulação) e controle (*i.e.* arquitetura tecnológica, competição e soluções de mercado, normas sociais). Estes mecanismos se somam aos princípios previstos na lei para combater imposições unilaterais de agentes de tratamento de dados, como o próprio Estado. Respeitando a ideia de uma norma geral, a LGPD busca garantir que o tratamento de dados pessoais pelas entidades públicas seja feito de forma interoperável, racional, e com a finalidade de fundamentar a realização de políticas públicas[7].

O art. 37 da Constituição Federal, ao estabelecer o **princípio da legalidade** como um dos princípios basilares da Administração Pública, **restringe a atuação do Estado àquilo que lhe é permitido por lei**[8]. Da leitura conjunta do princípio constitucional com o disposto na LGPD, conclui-se que as hipóteses para compartilhamento de dados pela Administração Pública devem estar embasadas em fundamentos normativos que estabeleçam finalidades específicas para esse tipo de tratamento.

Evidencia-se, portanto, uma sobreposição entre os princípios da finalidade e da legalidade no tratamento de dados pela Administração Pública. Nesse sentido, as finalidades que legitimam o Estado a compartilhar dados devem estar previstas em normas jurídicas de forma explícita.

Isso reforça o modelo *ex-ante* de proteção[9], ao estipular que **o tratamento de dados pelo Estado pode ser realizado desde que fundamentado em uma das hipóteses legais, que tenha o interesse público como objetivo e apresente**

---

[6] FRAZÃO, Ana. **Objetivos e alcances da Lei Geral de Proteção de Dados.** In: FRAZÃO, A. et. al. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 125-126.

[7] O art. 25 da LGPD dispõe sobre a interoperabilidade no tratamento de dados pelo Poder Público: "*Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.*"

[8] FILHO, José dos Santos Carvalho. Manual de Direito Administrativo. 32ª ed. São Paulo: Atlas. 2018. p. 73.

[9] BIONI, B. R. et. al. **Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência.** In: FRAZÃO, A. et. al. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 810-812.

informações claras a respeito da finalidade para qual os dados serão tratados (art. 23, I, LGPD). Vale ressaltar que a importância de o setor público cumprir com esses comandos se expressa principalmente ao se considerar o volume expressivo de dados que é tratado pelo Estado[10].

A necessidade de tratamento de dados pessoais pelo Poder Público é reconhecida pela LGPD, que não busca impedir essas atividades, mas estabelecer um sistema de salvaguardas que evite abusos e violações de direitos. Reforça-se, assim, a ideia de que a norma geral deve servir como guia para garantir uma política de proteção de dados forte. A existência de um regime homogêneo entre os diferentes órgãos do Poder Público mitiga os riscos inerentes ao tratamento de dados pessoais, ao passo que diferentes microssistemas, com mecanismos e classificações distintos, diminui a confiabilidade nas instituições públicas ao pulverizar diretrizes[11].

Esse regime homogêneo, no entanto, deve seguir as disposições previstas na LGPD, de modo que o tratamento por órgãos estatais, o que inclui o fluxo de dados na Administração Pública, garanta que os processamentos envolvendo dados pessoais sejam proporcionais às finalidades almejadas por esses agentes.

Por conseguinte, a fim de preservar o princípio da legalidade e assegurar um regime rígido de proteção de dados pessoais, **a aplicação e a interpretação do Decreto devem respeitar o sistema de proteção estabelecido pela LGPD**. Nesse sentido, destaca-se a decisão da relatora do e. Supremo Tribunal Federal, Exma. Ministra Rosa Weber, referendada pelo plenário, no julgamento da ADI nº 6.387, que decretou a inconstitucionalidade de medida provisória que não garantia grau de proteção compatível ao direito à autodeterminação informativa:

> Nessa ordem de ideias, não emerge da Medida Provisória n. 954/2020, nos moldes em que posta, interesse público legítimo no compartilhamento dos

[10] BLACK, Gillian; STEVENS, Leslie. **Enhancing Data Protection and Data Processing in the Public Sector**. The Critical Role of Proportionality and the Public Interest. Script Ed, Volume 10, Issue 1, Abril 2013. DOI: 10.2966/scrip.100113.93. p. 99-101. Disponível em: <https://www.research.ed.ac.uk/portal/files/8145321/Enhancing_data_protection.pdf>. Acesso em 20 fev. 2021.

[11] *Ibid*.

> dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade da medida. E tal dever competia ao Poder Executivo ao editá-la.
>
> Nessa linha, **ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.** Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva.
>
> (...)
>
> Essas considerações são corroboradas pela manifestação trazida aos autos pela Agência Nacional de Telecomunicações – ANATEL, que destacou necessária "a observância de extrema cautela no tratamento dos dados de usuários de serviços de telecomunicações". E recomendou a **adoção de medidas visando a adequar a medida à garantia dos princípios estabelecidos na Constituição Federal, na Lei Geral das Telecomunicações e na Lei Geral de Proteção de Dados,** de modo a assegurar a proteção da privacidade, da intimidade e dos dados pessoais de usuários de serviços de telecomunicações (...)(Grifos aditados).

Vale ressaltar que o Estado não deve ser considerado uma entidade única no que diz respeito ao tratamento de dados pessoais por entes públicos. Esse tratamento deve ser pautado na noção de **separação informacional de poderes**[12] (tema aprofundado nos **pontos 'c.' e 'd.' da Seção IV)**, segundo a qual órgãos estatais devem tratar dados somente no limite daquilo que é estritamente necessário para a consecução de seus objetivos institucionais. Nesse sentido, a transferência, o compartilhamento e a integração de bases de dados entre entes estatais consistem em atividades de tratamento que carecem de uma previsão legal bem definida, de modo a evitar que órgãos tenham acesso a dados que extrapolam suas prerrogativas e coloque em risco o controle de indivíduos sobre seus dados.[13]

Com isso em mente, vale adiantar que **não é possível identificar o cumprimento pelo governo federal das disposições do supracitado art. 23 da LGPD na**

---

[12] Aqui, o termo "poderes" não deve ser confundido com a divisão de poderes do Estado.

[13] FRAGOSO, Nathalie; MASSARO, Heloisa. **Cadastro Base e amplo compartilhamento de dados pessoais: a que se destina?** Jota, 19 dez. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/cadastro-base-e-amplo-compartilhamento-de-dados-pessoais-a-que-se-destina-19122019>. Acesso em: 20 fev. 2021.

implementação do CBC. Como será demonstrado na Seção III, os níveis de compartilhamento de dados propostos pelo Decreto 10.046/2019 trazem direcionamentos que impedem juízos suficientemente cuidadosos da finalidade de cada tipo de compartilhamento. Em um contexto em que se propõe, pelo Decreto, a operacionalização de maior fluxo de dados na administração pública a partir da interligação de bases temáticas (como do CPF, da CNH, por exemplo), isso gera ainda mais preocupações a respeito do aumento da opacidade do tratamento de dados pelo Estado e da transparência do indivíduo à máquina pública.

Exemplo disso está no fato de que, ao buscar informações nos sites da Secretaria de Governo Digital, responsável pela elaboração do Decreto, não se localiza, por exemplo, informações claras, atualizadas e de fácil acesso acerca das hipóteses em que o tratamento de dados pessoais ocorrem, muito menos sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em evidente confronto ao inciso I do referido artigo[14]. Essa obscuridade sobre a operacionalização do disposto no Decreto é dissonante com o direito à proteção de dados conforme regulamentado pela LGPD, principalmente levando em conta a aura de garantia de controle pelo titular de seus dados pessoais que a lei institui.

c. O Decreto n° 10.046/2019 e a Lei Geral de Proteção de Dados

O presente item analisará a congruência do Decreto face à LGPD concernentes (i) aos seus princípios, (ii) às bases legais para o tratamento e (iii) à sistemática de proteção de dados pessoais.

[14] "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos".

i. Os Dez Princípios da LGPD

Como já exposto, a leitura do Decreto nº 10.046/2019 deve ser balizada pelas regras estabelecidas na LGPD, diploma de hierarquia superior que toca elementos essenciais do Decreto. Nesse sentido, as hipóteses de compartilhamento de dados trazidas pelo Decreto devem ser lidas como a explicitação das finalidades que o Estado elencou como legítimas para a realização do compartilhamento de dados pessoais entre órgãos da Administração Pública Federal. Isso indica que **não deve a Administração Pública contrapor ou ir além do que dispõem as hipóteses legais da LGPD, sob o risco de violar o princípio da legalidade**, como já mencionado no item anterior**.**

O Decreto nº 10.046/2019, como instrumento normativo infralegal, teria o condão de meramente regulamentar as hipóteses em que o compartilhamento é possível, desde que restrito às limitações da lei sobre a qual se baseia, no caso, a LGPD. Uma leitura diversa importaria entender que a Administração Pública não está adstrita aos termos das normas a que está submetida, situação na qual o Decreto serviria como verdadeira carta em branco para o compartilhamento de dados sem qualquer controle ou *accountability*. Tal postura, imbuída na infraestrutura que ronda o CBC, cria brechas para violação de direitos fundamentais e riscos incalculáveis decorrentes do potencial desvirtuamento do uso de dados.

O art. 6º da LGPD determina dez princípios que devem ser observados em toda e qualquer atividade de tratamento de dados pessoais. Tais princípios incorporam o espírito da Lei e determinam as lentes sob as quais as atividades de tratamento devem ser analisadas para que haja *compliance* com a LGPD. Dessa forma, o respeito aos princípios elencados é um alicerce fundamental para que as atividades de tratamento ocorram em conformidade com a lei.

Chamam atenção as incompatibilidades do Decreto com os princípios da finalidade, adequação e necessidade. Quando lidos em conjunto, determinam que

qualquer tratamento de dados só pode ser feito desde que necessário e adequado à finalidade legítima, específica e explícita informada ao titular. Seguir esses princípios consiste no primeiro passo a ser tomado antes de se realizar qualquer tratamento de dados legítimo.

Abaixo, trazemos uma **tabela para explicitar como o Decreto nº 10.046/2019 e o Cadastro Base do Cidadão não estão em conformidade com esses e os sete demais princípios norteadores da proteção de dados pessoais impostos pela LGPD**:

Princípio	Definição na LGPD	Análise do Decreto nº 10.046/2019
Finalidade	Art. 6º, I: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.	Os objetivos do art. 1º e do art. 16 do Decreto não são considerados finalidades no âmbito da LGPD por serem excessivamente amplos, discricionários e não individualizados. O previsto no Decreto pode levar a tratamentos excessivos, ilegais e abusivos por parte do Estado. Ademais, o Decreto permite que o Estado realize tratamento de dados com finalidades distintas para as quais eles foram inicialmente coletados, como segurança pública e atividade de inteligência, em desrespeito à LGPD.
Adequação	Art. 6º, II: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.	
Necessidade	Art. 6º, III: 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 pode ser interpretado sob uma dupla ótica: **(i)** o tratamento de dados deve se ater ao mínimo necessário e **(ii)** os dados devem ser retidos pelo menor tempo necessário para as finalidades do tratamento. No entanto, o Decreto e o CBC fomentam a coleta e uso excessivo de dados pessoais, sem nenhuma previsão de fim de seu ciclo de vida, em flagrante violação deste princípio. O próprio art. 11, §2º, do Decreto, ao excluir qualquer forma de controle de acesso a dados, comprova que o CBC admite solicitação de dados desproporcionais e não previstos (podendo até ser condicionada a pagamento de custos adicionais).
Livre acesso	Art. 6º, IV: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus	O Decreto não respeita o princípio do livre acesso pelo titular e de qualidade dos dados da LGPD, pois não há nenhuma previsão de exercício de direitos dos titulares para acesso, conferência e

	dados pessoais.	retificação de dados pessoais que podem estar incorretos ou desatualizados.
Qualidade dos dados	Art. 6º, V: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.	
Transparência	Art. 6º, VI: 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 Decreto peca em questões de transparência, do ponto de vista da proteção de dados pessoais e da segurança da informação. Também não há objetividade quanto à categorização de compartilhamento de dados. Não há previsão de mecanismos de fornecimento de informação ao titular sobre quais dados estão sendo tratados, por quais órgãos, e de que maneira.
Segurança	Art. 6º, VII: 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.	O Decreto pretende facilitar o acesso a uma imensa quantidade de dados detidos pela Administração Pública ao conectar várias bases de dados governamentais sem especificar medidas de segurança da informação e prevenção necessárias para proteger os dados retidos e em transição. Rememora-se o histórico recente de incidentes de segurança massivos ocorridos no Poder Público. Apenas em 2020, foram notificados 24.303 incidentes de segurança em toda a Administração Pública federal[15]. Isso demonstra como a grande maioria dos órgãos públicos não possui sistemas de gestão de segurança da informação robustos. Isso leva a existirem vários pontos de vulnerabilidade que poderão ser explorados por sujeitos mal intencionados para acessar os dados disponíveis na base integradora. Afinal, caso se encontre uma falha de segurança no sistema de um único órgão, é possível que, a partir desse acesso facilitado proposto pelo Decreto 10.046/2019, se acesse informações em bases de muitos outros órgãos.
Prevenção	Art. 6º, VIII: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	
Não discriminação	Art. 6º, XI: impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.	Ao permitir alto grau de discricionariedade no tratamento de dados realizado por cada ente público, o Decreto não oferece qualquer tipo de salvaguarda contra tratamento discriminatório,

[15] CTIRGov. **CTIRGov em Números**. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 20 fev. 2021.

		ilícito ou abusivo pela Administração Pública.
Responsabilização e prestação de contas	Art. 6º, X: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.	O Decreto não traz qualquer medida de *accountability* por parte dos entes que vierem a tratar dados pessoais. Ainda, dispensa a obrigatoriedade de instrumentos jurídicos formalizando o compartilhamento de dados e responsabilidades dos controladores envolvidos. Isso prejudica a transparência e a responsabilização por tratamentos ilegais.

A partir desta análise, conclui-se que o processo de elaboração do Decreto não considerou os ideais fundacionais e norteadores da proteção de dados no Brasil. Ao ignorar os princípios que equilibram os interesses subjacentes das regras concretas da LGPD, o Decreto também viola o direito autônomo à proteção de dados.

ii. As Bases Legais da LGPD

De acordo com a LGPD, o tratamento de dados pessoais pela Administração Pública se baseia majoritariamente em duas bases legais principais: **(i)** execução de políticas públicas e **(ii)** cumprimento de obrigação legal ou regulatória.

No que diz respeito a **(i)**, o art. 7º, III, LGPD, autoriza o tratamento quando necessário à "**execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres". Se a atividade englobar tratamento de dados sensíveis, esta deverá ser prevista somente em leis e regulamentos (art. 11, II, 'b').

Quanto a **(ii),** os art. 7º, II, c/c 11, II, 'a', LGPD autorizam o tratamento realizado para o **cumprimento de obrigação legal ou regulatória** pelo controlador de dados.

Ressalta-se que a adoção da primeira base legal mencionada deve ocorrer à luz do já mencionado **art. 23, *caput*.** Este dita que todo tratamento realizado pela

Administração Pública deve ser feito "para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público".

Essa leitura sistemática da base legal do art. 7º, II, pode ser interpretada como uma aplicação do princípio da legalidade à referida base legal, tornando claro que **o Estado só poderá realizar tratamentos dentro do âmbito de competência determinado pela legislação vigente e pelos princípios que regem a Administração Pública.** Ao adentrar especificamente em como deve se dar a interpretação do art. 7º, II, c/c o art. 23, *caput*, o Capítulo IV da LGPD traz regras específicas que devem ser observadas pelo Poder Público ao realizar o compartilhamento de dados pessoais.

Enquanto o art. 23 limita o rol de bases legais para o tratamento de dados, **o *caput* do art. 26 deixa claro que o compartilhamento de dados entre a Administração Pública deve se ater às finalidades específicas de execução de políticas públicas e de cumprimento de obrigações legais[16],** restringindo o campo de hipóteses legais aplicáveis neste contexto.

Das bases legais da LGPD aplicáveis ao Poder Público infere-se que **a lei não autoriza a integração e compartilhamento irrestrito de bases de dados de forma *a priori*, sem levar em conta a finalidade e o contexto em que se insere o tratamento.** Pelo contrário, para cada novo tratamento de dados, o que inclui atividades de compartilhamento, uma análise casuística deve ser feita a respeito das finalidades do tratamento, bem como da necessidade e adequação dos dados ao propósito definido. Como se verá na Seção III, o CBC vai de encontro a essa noção ao estipular níveis de compartilhamento de dados que ignoram juízos de finalidade e contexto caso a caso dos tratamentos pretendidos pela Administração Federal

A razão para isso é que a base legal de execução de políticas públicas exige a correlação dos tratamentos com políticas públicas já existentes e em processo de

[16] "Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei."

execução, com previsões expressas em leis ou regulamentos. Com isso, o regime da LGPD **impede o tratamento de dados pessoais para as finalidades alargadas e genéricas pretendidas com o Decreto, que não preveem cuidados para determinar se tratamentos de dados são de fato necessários e adequados às finalidades específicas pretendidas**.

iii. Sistemática de Proteção de Dados

Como já destacado anteriormente, *accountability* e transparência são princípios dos quais dependem o próprio exercício de direitos pelos titulares de dados, bem como a possibilidade de aferir se a postura de controladores está de acordo com a lei.[17] Daí porque a documentação íntegra da atividade de tratamento é elemento indispensável na sistemática da LGPD.

Diante disso, ao prever no art. 5º a dispensa de celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados, o Decreto fere a sistemática imposta pela LGPD. **Sob o pretexto vago de agilidade, desburocratização e eficiência da Administração Pública, o Decreto dispensa instrumentos pelos quais poderia fixar-se informações objetivas sobre a atividade de tratamento dos dados solicitados, tal como seu escopo, finalidade e, inclusive, a responsabilidade de cada controlador.** Assim, prejudica-se a transparência e *accountability* estatal.

Além disso, é uma máxima tão antiga quanto a própria regra jurídica de que, onde há um direito, há um remédio (*ubi ius, ibi remedium*). Em que pese a LGPD atribuir uma série de direitos ao titular, tais quais os de informação e oposição ao tratamento e acesso, correção e eliminação dos dados, **não há previsão no Decreto, nas resoluções do CCGD ou nos sites do Governo Federal relativos ao CBC sobre como exercê-los**.

---

[17] ARTICLE 29 WORKING PARTY. Guidelines on transparency under Regulation 2016/679. Bélgica, Bruxelas, 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227>. Acesso em 26 abr. 2021.

Nota-se, por fim, que legislações de dados pessoais estabelecem um microssistema de proteção no qual uma peça do maquinário é condição para o funcionamento de outra. Os deveres de transparência e *accountability* são necessários para supervisão independente pela Autoridade Nacional e para o exercício do direito dos titulares. Estes, por vez, asseguram a aplicação apropriada dos princípios e bases legais e vice-versa. Portanto, ao não compreendê-los, o Decreto impossibilita o funcionamento de mecanismos co-dependentes e, por conseguinte, desvirtua a essência da LGPD.

III. NÍVEIS DE COMPARTILHAMENTO DE DADOS PESSOAIS NO DECRETO Nº 10.046/2019

O Decreto determina, nos incisos I, II e III, do art. 4º, que o compartilhamento de dados entre os órgãos da administração pública ocorrerá de acordo com três níveis de compartilhamento, quais sejam:

I. compartilhamento amplo, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;

II. compartilhamento restrito, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e

III. compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.

Analisar esses níveis de compartilhamento é fundamental para compreender de que forma são delimitadas restrições ao fluxo de dados pessoais na Administração Pública federal. Para essa avaliação, também tomaremos como parâmetro o conteúdo de documentos emitidos pelo CCGD, como as Regras para Compartilhamento de Dados[18] (doravante referenciado "Regras") e a Apresentação das Regras de Compartilhamento[19] (doravante referenciado "Apresentação").

Para tanto, o primeiro passo é compreender de que forma essas categorias são (in)compatíveis com a teoria da **privacidade contextual**.

a. Mudança Paradigmática: A Proteção Contextual dos Dados Pessoais

Da leitura dos incisos citados, observa-se que os níveis de compartilhamento trabalham com uma **categorização estanque dos dados pessoais**. Essa visão pressupõe que os dados observarão as mesmas regras de controle de acesso **independentemente do contexto** em que foram coletados ou em que serão aplicados.

É o que se conclui ao analisar que determinados dados serão abertos ao público (compartilhamento amplo), a qualquer órgão da Administração Pública federal (compartilhamento restrito) ou a órgãos específicos (compartilhamento específico), **independentemente da observância da finalidade** visada pelo órgão ou pessoa requerente dos dados. Para solidificar a situação, prevê-se que seja feita a revisão das categorizações apenas uma vez a cada cinco anos ou quando houver alteração nas diretrizes que as regulam, como determina o art. 4º, §6º do Decreto.

---

[18] COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Regras para Compartilhamento de Dados**. 4 mai. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/regras-de-compartilhamento_v1-0.pdf>. Acesso em 20 fev. 2021.

[19] COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Apresentação das Regras de Compartilhamento de Dados do Decreto nº 10.046/2019**. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/apresentacao_categorizacao_2020-abril-02.pdf>. Acesso em 20 fev. 2021.

A disciplina da proteção de dados pela LGPD se baseia em uma abordagem de risco para direcionar os esforços de controladores de dados a respeito de quais salvaguardas devem ser implementadas para garantir a proteção de dados e a privacidade. De forma contrária ao proposto pelo Decreto, isso demanda juízo sobre o grau de sensibilidade dos dados**.** Assim, **o nível de medidas de segurança a serem implementadas correlaciona-se diretamente com o risco do contexto da atividade de tratamento e as expectativas do titular em relação a como suas informações serão utilizadas**.

A teoria da **privacidade contextual** é um importante marco teórico para delimitar o escopo da proteção de dados nas atividades de tratamento de acordo com seu contexto. Um dos objetivos da teoria é de **superar a noção de que existem dados que *a priori* devem ou não ser protegidos**[20]. Este entendimento foi corroborado pelo voto do Exmo. Ministro Gilmar Mendes na ADI nº 6387.[21] A Profª. Helen Nissenbaum, cunhadora do termo, afirma que todos os espaços são dotados de regras para o fluxo de informações, as chamadas **normas de fluxos informacionais** (*norms of information flows*).[22]

Considerando que todas as esferas de nossa existência se articulam de acordo com determinados contextos, as informações transacionadas em diferentes momentos ocorrem com base nos aspectos políticos, sociais, econômicos, espirituais em que nos enquadramos em cada momento. Por isso, não há espaço para considerar que uma informação possa ser compartilhada independentemente de uma avaliação contextual.

---

[20] NISSENBAUM, Helen. **Privacy as Contextual Integrity**. Washington Law Review, v. 79, 2004. Disponível em: <https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf>. Acesso em 20 fev. 2021.
[21] "Como bem destacado pela professora Laura Schertel Mendes, é decisivo para a concepção do direito à autodeterminação "o princípio segundo o qual NÃO MAIS EXISTIRIAM DADOS INSIGNIFICANTES nas circunstâncias modernas do processamento automatizado dos danos", de modo que "o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato que quão sensíveis ou íntimos eles são)" (MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. No Prelo).". Voto do Exmo. Ministro Gilmar Mendes no julgamento do referendo da Medida Cautelar na ADI nº 6387/DF.
[22] *Idem*, p. 119.

Nesse sentido, as normas de fluxos informacionais seriam próprias para cada circunstância social. Elas se dividem em **normas de conveniência** (*appropriateness*), que revelam quais informações são apropriadas para serem reveladas sobre um indivíduo em uma situação específica[23], e **normas para distribuição de informação** (*distribution of information*), que se referem à distribuição de um dado pessoal de uma pessoa a outra[24].

A título ilustrativo, normas de conveniência estipulam que, em condições normais, uma pessoa expresse sua visão política para um amigo, mas não necessariamente para seu superior no trabalho.[25] Já uma norma de distribuição dispõe que um delicado segredo contado a uma amiga não deve ser compartilhado com outra pessoa.[26]

A privacidade é violada quando uma dessas categorias normativas é infringida.[27] Por exemplo, considera-se razoável que o Departamento Nacional de Trânsito tenha acesso aos dados da Carteira Nacional de Habilitação para aplicação da legislação de trânsito. No entanto, o compartilhamento desses dados, de forma individualizada, com entidades do Sistema Brasileiro de Inteligência para finalidades desconhecidas, pode vir a ser considerado irregular.

Nesse sentido, Helen Nissenbaum afirma que o mais preocupante para as pessoas não é a mera restrição do fluxo de seus dados pessoais, mas a garantia de que esse fluxo seja feito de forma apropriada.[28] Transpondo essa lógica à terminologia usada na LGPD, a análise do contexto da operação envolve a **delimitação de uma finalidade específica e um juízo de se os dados a serem tratados são de fato necessários e adequados para cumprí-la**. Daí porque a LGPD fixa tais elementos como seus princípios no art. 6°, I, II e III.

---

[23] *Idem,* p. 120.
[24] *Idem,* p. 122.
[25] *Idem,* p. 121.
[26] *Idem,* p. 123.
[27] *Idem,* p. 125.
[28] NISSENBAUM, Helen. **Privacy in context: technology, policy, and the integrity of social life**. Stanford University Press, Stanford, California. 2010, p. 2.

Isso mostra como o Decreto, bem como as Regras que pretendem instruir sua aplicação, se atêm a uma noção ultrapassada de privacidade, que foca estritamente na categorização *a priori* de dados de forma estanque. É essa característica que revela sua incompatibilidade com o regime de proteção de dados pessoais estipulado pela LGPD.

Uma vez realizada uma análise mais generalizante a respeito de como os níveis de compartilhamento descritos no Decreto se comportam face à LGPD, cabe proceder agora a uma exploração mais pormenorizada a respeito de cada nível.

b. Compartilhamento Amplo

A categoria de **compartilhamento amplo** inclui dados que serão disponibilizados para que qualquer pessoa, seja ela servidora pública ou não, tenha acesso irrestrito. As Regras trazem ainda mais um elemento: cairão nessa categoria todos os "dados não protegidos por norma, portanto públicos".[29]

Esses dados dispensarão autorização prévia pelo gestor de dados e seu compartilhamento será realizado pelos canais para dados abertos e transparência ativa (art. 11 do Decreto nº 10.046/2019). Para a categoria ampla, a única restrição apresentada pelas Regras é o mascaramento do CPF[30]. Porém, não há exposição dos motivos para tal decisão, tampouco análise quanto à efetividade dessa técnica para impedir a identificação do titular ou mitigar danos de incidentes de segurança.

Exemplo de informação que consta como dentro da categoria ampla são informações de **beneficiários de programas sociais do Governo**, conforme documento *Formulário de Categorização* disponibilizado pela Secretaria de Governo

[29] COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Regras**, Op. Cit., p. 6.
[30] *Idem*, p. 8.

Digital[31], que assim descreve:

> Beneficiários de programas sociais do governo. Relação de beneficiários diretos de programa social do governo. Informações devem conter no mínimo o nome, CPF mascarado e valor.

Por mais que seja compreensível uma busca por maior transparência a respeito de como o Governo investe em programas sociais e se busque combater fraudes que recaiam sobre eles, questiona-se aqui o fato de que **os dados dessas pessoas são acessíveis por absolutamente toda a população brasileira**. Beneficiárias de programas como o Bolsa Família são muitas vezes pessoas em situação de profunda vulnerabilidade, amplamente suscetíveis a fraudes por parte de indivíduos que utilizam seus dados de forma maliciosa. Essas beneficiárias são também frequentemente miradas por campanhas políticas que acabam por varrer essas bases de dados para incidir sobre sua fragilidade para tentar influenciar seu voto ou qualquer outra esfera de expressão política.

Outro problema que torna clara a incompatibilidade do Decreto com a Lei Geral de Proteção de Dados Pessoais é que a categoria ampla também possibilita o compartilhamento sem autorização prévia de dados de regularidade fiscal de pessoas jurídicas. O CNPJ pode se configurar como um dado pessoal, como no caso de microempreendedores individuais (MEI). Tal como aludido acima, esses indivíduos também são potenciais alvos de tentativas de fraude, ainda mais em um contexto comercial.

Identifica-se, pois, **incongruências entre o estipulado pelo CCGD e as regras da LGPD e da LAI**. Há uma confusão quanto a que dados qualificam-se como pessoais e sobre como protegê-los. Isso é especialmente evidenciado no Decreto e nas Regras pelo uso do conceito opaco de "dados públicos" e subsequente previsão de que estes são disponibilizados sem qualquer discrição.

---

[31] Disponível em https://www.gov.br/governodigital/pt-br/governanca-de-dados/formulario_regras-de-compartilhamento_modelo-v1-0.pdf.

Ainda, o Decreto atrela o conceito de "dados públicos" à definição de "dados amplos" (art. 4°, I, c/c 31, § 2º, Decreto 10.046/2019) e, subsequentemente, delega sua conceituação às Regras do CCGD (art. 31, *caput*, Decreto 10.046/2019). Este, por sua vez, os define como "dados que deveriam estar na em **transparência ativa**, ou que são cedidos sempre que solicitados pelo SIC – Serviço de Informações ao Cidadão. Trocá-los entre órgãos não é um problema, geralmente" (Regras, p. 5).

No entanto, a ideia de "transparência ativa" decorre da prática acerca da aplicação da LAI, e versa sobre dados de interesse público que a Administração deve publicar ativamente, isto é, sem que lhe seja solicitada. Ocorre que, sob a LAI, informações pessoais (art. 4°, IV, LAI e art. 5°, I, LGPD)[32] são protegidas (art. 31, LAI) e, atualmente, não deveriam constituir a transparência ativa, dado serem de acesso restrito e poderem ser publicizadas somente mediante consentimento do titular, salvo exceções previstas no §3º do art.31 da LAI[33].

As incongruências também se refletem na incompatibilidade do Decreto com o §1º do mesmo art. 31. De acordo com ele,

> Art. 31. (...)
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão

[32] Note-se que, tanto a LGPD, quanto a LAI definem dado pessoal ou informação pessoal (respectivamente) como "aquela relacionada à pessoa natural identificada ou identificável". Portanto, há sinergia entre ambos conceitos.

[33] § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
III - ao cumprimento de ordem judicial;
IV - à defesa de direitos humanos; ou
V - à proteção do interesse público e geral preponderante.

legal ou consentimento expresso da pessoa a que elas se referirem.

O texto da LAI reforça a importância de garantir a proteção de dados pessoais, inclusive garantindo a restrição a seu acesso, o que faz cair por terra a exagerada abertura trazida pelo Decreto em seu nível de categoria ampla. Além disso, vale ressaltar ser incompatível com o inciso II o fato de o Decreto autorizar a divulgação de dados pessoais sem que tenha natureza de lei. Essas incongruências ressaltam a contradição do Decreto com a LGPD e a LAI, leis que pretende regulamentar.

Há dois problemas com a prática instaurada pelo Decreto. Em primeiro lugar, a norma delega a conceituação de "dados públicos" a instrumento que não possui caráter normativo e, portanto, não pode servir como base legal para tratamento de dados. Dois, em que pese ser possível o alinhamento com a LGPD a partir da aplicação do conceito de transparência ativa, derivado da LAI, o CCGD se pauta em prática desatualizada, de um tempo no qual o direito à proteção de dados pessoais ainda não havia tido sua autonomia reconhecida por esta e. Corte.

Note-se que, seja qual for o significado atribuído ao conceito de "dados públicos", a LGPD traz, em seu art. 7º, § 4º, que **até mesmo aos dados tornados manifestamente públicos por seus titulares assegura-se a aplicação de direitos e princípios fixados no diploma**. Logo, ainda que a atividade de tratamento esteja associada a dados pessoais publicizados há que se fazer análise contextual por meio dos princípios de adequação, finalidade e necessidade.

Isto é dizer que dados pessoais, até quando tornados públicos, o são assim tratados para determinado fim e não se isentam de proteção. Não poderia o Estado desvirtuar tal finalidade devido à publicidade dos dados em determinado contexto. Portanto, é impreterível que, constituindo-se uma nova finalidade, há de se realizar outra análise de adequação e necessidade, fundamentada em nova base legal com todas informações e salvaguardas indispensáveis ao tratamento.

Desta forma, dados pessoais, sejam sensíveis, sejam públicos, devem ser protegidos conforme os parâmetros previstos na LGPD, tal como determina a jurisprudência deste e. STF no julgamento da ADI nº 6.387. Portanto, os **requisitos especificados na categoria ampla deverão ser revistos,** de modo que um nível adequado de proteção de dados seja garantido na Administração Pública federal.

c. Compartilhamento Restrito

O art. 4º, II, do Decreto nº 10.046/2019 estabelece que, quando se tratar de dados protegidos por sigilo, será concedido acesso "a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas". Para o documento de Regras, "são dados restritos aqueles que o órgão entende que podem ser acessados por todos os órgãos e entidades da Administração Pública federal, sem a necessidade de analisar pedidos e emitir permissões para cada caso".[34]

Tal explicação se contradiz. Segundo o glossário de segurança da Internet do Internet Engineering Task Force (IETF)[35] o **controle de acesso** é a "proteção dos recursos de um sistema contra acesso não autorizado"[36]. As boas práticas recomendam que o controle de acesso seja orientado pelo princípio "*need to know*", isto é, o uso e acesso a dados protegidos devem ocorrer apenas quando estritamente necessário para atividades legítimas.[37] Portanto, não há controle de acesso quando

---

[34] COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Regras**, Op. Cit., p. 9.

[35] O IETF é uma comunidade internacional e aberta composta de designers de rede, operadoras e pesquisadores preocupados com a evolução da arquitetura e o bom funcionamento da Internet. Para executar tal missão, a organização produz documentos técnicos de alta qualidade, pautando-se em princípios tais quais processo aberto, competência técnica, núcleo voluntário e consenso. Internet Engineering Task Force. A Mission Statement for the IETF. Out. 2004. Disponível em: <https://datatracker.ietf.org/doc/rfc3935/> Acesso em 18 abr. 2021.

[36] *"Access control: 1. (I) Protection of system resources against unauthorized access. 2. (I) A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy." In* Internet Engineering Task Force (IETF). **Internet Security Glossary, Version 2**. 2007. Disponível em: <https://tools.ietf.org/html/rfc4949 >. Acesso em 20 fev. 2021.

[37] Berkeley Information Security Office. **Need to Know Access Control Guideline.** Disponível em

entende-se que dados são acessíveis por toda Administração Pública.

A restrição dos dados deve estar atrelada a um controle de acesso que inclua um **mecanismo de autorização** para acesso aos dados, não podendo se resumir a uma mera rastreabilidade. A ferramenta de controle de acesso também tem uma faceta organizacional de política de controle pela entidade gestora do banco. Nada impede que esse mecanismo seja automatizado pelo uso de *hashes* criptográficos que autentiquem o acesso a dados quando a necessidade for previamente comprovada (por exemplo, ao se firmar um convênio entre o órgão requerente e o responsável pela base central de dados). Contudo, esses mecanismos de segurança (manuais ou automatizados) não parecem estar sendo adotados no CBC.

O art. 6º, VII, da LGPD, obriga aos controladores 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". Apesar de o acesso a dados na categoria restrita não englobar qualquer pessoa, mas todos os funcionários da Administração Pública (milhares de indivíduos), **o Decreto e o CCGD não estipulam salvaguardas suficientes e tampouco asseguram os princípios da LGPD, em especial, os de finalidade, prevenção e responsabilização e prestação de contas (*accountability*).**

Isso porque, uma vez que seja fixada finalidade para uma específica atividade de tratamento por determinado órgão, o princípio da necessidade dita que apenas os funcionários que trabalham para tal fim devem ter acesso aos dados. Do contrário, há acesso ilícito. Logo, caso o acesso não seja registrado e controlado, há falha na prevenção ao acesso ilegal, e, mesmo que este não ocorra, o controlador deve ser capaz de provar sua inocorrência.

Aplicação prática da categoria restrita também se encontra no supracitado *Formulário de Categorização*[38]. Estão sob esse nível, dentre outros dados:

---

https://security.berkeley.edu/need-know-access-control-guideline. Acesso em 5 mai 2021.

[38] Disponível em

Categoria de Compartilhamento Restrita		
Dados cadastrais. Inclui nome, identificadores (CPF, NIS, título eleitoral, etc), data de nascimento, situação civil, endereço, contatos (telefone, e-mail, etc.), filiação, nome social.	Situação de regularidade com a APF de Pessoas FISICAS. Exemplo: CPF, dívida ativa, certificados, certidões, alvarás, etc. Deverá incluir tipo de regularidade (qual alvará, permissão, etc.), situação (regular, irregular), validade (início e fim, se houver), nome e CPF.	Beneficiários de programas sociais do governo. Informações completas sobre beneficiários de programa social do governo.

Tais dados são **acessíveis por absolutamente todos os servidores da Administração Pública Federal.** Isso é extremamente preocupante devido aos dados que se encontram dentro dessa categoria. As três categorias de dados trazidas acima são dados pessoais de grande relevância, como a vida fiscal da pessoa e, em alguns casos, dados pessoais sensíveis como raça, e eles transitam dentro da Administração Pública Federal sem qualquer tipo de controle. Dados esses que possibilitam uma série de atividades danosas aos titulares desses dados, como propaganda indevida, roubos de identidade, fraudes, golpes, tratamentos discriminatórios, entre outros.

Além disso, essa possibilidade de amplo acesso a dados por uma grande quantidade de servidores gera preocupações, considerando o histórico de vazamentos massivos de dados no Brasil. Afinal, caso se encontre uma falha de segurança no sistema de um único órgão, é possível que, a partir desse acesso facilitado proposto pelo Decreto 10.046/2019, se acesse informações em bases de muitos outros órgãos.

---

https://www.gov.br/governodigital/pt-br/governanca-de-dados/formulario_regras-de-compartilhamento_modelo-v1-0.pdf.

Nesse sentido, em 2021, já ocorreram dois grandes incidentes de segurança com bases de dados que reuniam diferentes informações pessoais. O caso de maior repercussão foi o vazamento de dados de mais de 220 milhões de brasileiros com a exposição de dados pessoais variados, como CPF, salário, endereço, entre outros, e que, conforme indicam especialistas, é o resultado de uma compilação de vários vazamentos menores que ocorreram ao longo dos anos por vulnerabilidades de sistemas de órgão públicos e empresas.[39] Ainda, instituições governamentais como Serpro e a base Infoseg, responsáveis por gerir dados de milhões de brasileiros, já foram vítimas de vazamentos no setor público brasileiro.[40] Diante disso, soma-se preocupações que advêm da histórica **ausência de salvaguardas suficientes para proteger os dados pessoais dos cidadãos que constam no CBC**.

Essas disposições do Decreto poderão representar uma abertura para possíveis violações em massa dos princípios da finalidade, necessidade e adequação e, com eles, da proteção de dados de milhões de cidadãos brasileiros.

d. Compartilhamento Específico

A última categoria de compartilhamento prevista no Decreto é o nível de compartilhamento específico, que promete maior controle de acesso por parte da Administração Pública. É a única que demanda permissão do gestor de dados para autorização de acesso. De acordo com as Regras, "critérios para aprovar ou recusar

---

[39] VENTURA, Felipe. **Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava**. 2020. Disponível em: <https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/>. Acesso em 25 fev. 2021. V. também ITForum. **Tudo o que você precisa saber sobre o megavazamento de dados.** 3 fev 2021. Disponível em https://itforum.com.br/noticias/tudo-o-que-voce-precisa-saber-sobre-o-megavazamento-de-dados/. Acesso em 5 mai. 2021.

[40] SOUZA, Renato. **Dados pessoais de brasileiros são negociados livremente na internet**. Correio Braziliense. 18 jul 2018. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/brasil/2018/07/16/interna-brasil,695136/dados-pessoais-de-milhares-de-brasileiros-sao-negociados-na-internet.shtml>. Acesso em 20 fev. 2021.

acesso, bem como detalhes do processo, são de total responsabilidade do gestor dos dados".[41]

Ocorre que, em que pese o maior nível de controle, a sistemática não endereça a natureza dinâmica da proteção de dados e viola os princípios da adequação, finalidade, necessidade, responsabilidade e prestação de contas (*accountability*) e transparência dado seu enfoque exclusivo na classificação de sigilo.

Tal como destacado na **Seção III (a)**, os princípios da adequação e necessidade norteiam-se pela finalidade do tratamento. O Decreto fixa que o gestor de dados decidirá sobre acesso quando os dados estiverem protegidos por sigilo. Assim, utiliza-se de conceito estanque e binário (sigiloso ou não) que não contempla juízo de proporcionalidade, a dimensionalidade da proteção de dados e os referidos princípios.

Como se vê de uma análise sistêmica do disposto na LGPD, ao dispor sobre princípios, bases legais e direitos do titular, ela não menciona em nenhum momento a ideia de sigilo. Isso indica que **o sigilo não está no cerne da disciplina da proteção de dados conforme regulamentada no Brasil**. Em direção distinta, está na disciplina de que tratamentos de dados pessoais sejam feitos tão somente quando **(i)** estritamente necessários e adequados a uma finalidade e seguindo os demais princípios previstos em seu art. 6º, **(ii)** baseados em uma fundamentação prevista em lei (arts. 7º e 11) e **(iii)** com a condição de que sejam assegurados os direitos do titular de dados (art. 18 ss).

Por isso é que o critério binário de decretação de sigilo para o nível de compartilhamento específico é insuficiente para garantir a conformidade do Decreto à LGPD e ao exercício da autodeterminação informativa. Além disso, mais uma vez, demonstra-se sua incompatibilidade com a teoria da privacidade contextual, já que não permite qualquer juízo de contexto a respeito de se determinado dado, consideradas as finalidades e circunstâncias do tratamento, pode ou não ser compartilhado. Afinal, ao decretar se determinado dado é ou não sigiloso de forma *a priori*, mais uma vez não se permite um juízo caso a caso sobre a adequação e

[41] *Idem*, p. 12.

necessidade do tratamento à finalidade pretendida.

IV. DA EXPERIÊNCIA ESTRANGEIRA NO COMPARTILHAMENTO IRRESTRITO DE DADOS PESSOAIS A NÍVEL NACIONAL

Entre os anos de 1960 e 1970, nos EUA e na Europa, o desenvolvimento tecnológico e a disseminação de dispositivos informáticos, como computadores com capacidade de armazenamento jamais vista até então, impactaram a forma de organização de informações dos Estados e de entidades privadas. Esse período histórico é marcado pela **elaboração de projetos pela burocracia estatal a fim de criar políticas públicas que se desenvolviam especialmente por meio do tratamento de dados pessoais de cidadãos, em linha com o paradigma de Estado Social que era predominante nessa época.**[42]

Assim, a burocracia estatal percebeu o **uso da tecnologia como uma oportunidade de tornar mais eficiente** a realização de suas atividades rotineiras diante da possibilidade de manipulação de um volume expressivo de dados, inclusive aqueles considerados pessoais.

Como resultado, bases de dados com dados pessoais detalhados se proliferaram em diferentes países para fundamentar a elaboração de políticas públicas. Ao longo dessa expansão tecnológica, exemplos ao redor do mundo evidenciaram os primeiros questionamentos sobre as interferências da tecnologia no funcionamento do Estado, nas relações da vida e no âmbito dos direitos fundamentais humanos.[43]

---

[42] SCHERTEL, Laura. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade de Brasília. Brasília, p. 34. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso em 20 fev. 2021.

[43] Sobre essas mudanças, Danilo Doneda destaca que esse processo de disseminação do uso de ferramentas inovadoras "teve a participação ativa de diversos setores representativos da sociedade e foram importantes a ponto de determinar consideráveis mudanças nas relações de poder, na vida cotidiana e na esfera de direitos fundamentais". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados, 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 159.

Desde o início, notou-se uma constante **tensão entre a imprescindibilidade e a relevância do tratamento de dados pessoais para o bom funcionamento do aparato estatal e a proteção de direitos fundamentais** - em especial, a livre manifestação da personalidade e o direito à privacidade.

Segundo Miriam Wimmer, "ao mesmo tempo que o tratamento de dados pessoais pelo Estado é pré-requisito para o exercício da cidadania, a expansão da quantidade e da variedade de dados pessoais custodiados pelo Estado suscita riscos de violações de direitos".[44] Logo, o processamento de dados amplo e irrestrito por órgãos estatais sem efetivos mecanismos de controle de acesso, levanta questionamentos relevantes sobre o impacto em direitos fundamentais. Isso porque esse contexto permite um compartilhamento excessivo de informações sob controle estatal entre os órgãos públicos, mesmo que não haja finalidade ou motivação específica para o acesso. Essa característica abre margem para atividades vigilantistas que podem infringir direitos humanos.

Com isso, o debate sobre a proporcionalidade entre a eficiência estatal e os riscos para direitos fundamentais no tratamento de dados determinou o desenvolvimento da disciplina de proteção de dados pessoais no contexto mundial. Foi com esse pano de fundo que as **primeiras leis de proteção de dados** foram elaboradas, como é o caso da Lei do estado de Hesse (1970), na Alemanha, e o Privacy Act (1974), nos EUA. Isso mostra que as discussões sobre criação de bases de dados nacionais de compartilhamento amplo entre os órgãos do Estado resultaram na rejeição dessas bases e na implementação de mecanismos para promoção dos direitos à autodeterminação informativa e à proteção de dados pessoais.

Essas garantias não mais se relacionavam a um mero direito de ser deixado só[45] ou de uma defesa da vida privada, mas alçaram a outro nível a salvaguarda às

---

[44] WIMMER, Miriam. **O regime do tratamento de dados pessoais pelo Poder Público**. *In:* DONEDA, Danilo [et al], Tratado de proteção de dados. Rio de Janeiro: Forense, 2021. p. 284.

[45] WARREN, Samuel. BRANDEIS, Louis. The Right to Privacy. Harvard Law Review, Estados Unidos, Massachusetts, Vol. 4, No. 5, pp. 193-220, dez, 1890

informações de um indivíduo, agora reconhecidas como integrantes de sua personalidade e dignas por si só de proteção.[46]

A seguir **apresentaremos três casos internacionais em que discutiu-se a ampliação indiscriminada no acesso a dados e seu compartilhamento entre diferentes órgãos estatais sem mecanismos que garantissem o controle do titular sobre como seus dados estariam sendo utilizados.**

Os casos dispõem sobre bases de dados de abrangência nacional que permitiriam acesso a informações pessoais por órgãos públicos sem finalidade específica nos EUA, França e Alemanha, durante as décadas de 1960 e 1970. Em que pese o Decreto nº 10.046/2019 ser um facilitador do amplo acesso e compartilhamento de informações, especialmente enquanto integrador de bases e promotor de interoperabilidade com níveis de compartilhamento excessivamente permissivos, as lições das experiências a seguir auxiliam na identificação de **riscos decorrentes do acesso a dados com restrições frágeis por múltiplos entes estatais**.

a. Estados Unidos: o *National Data Center*

Em 1965, o Gabinete Orçamentário do Escritório Executivo da Presidência dos EUA[47] propôs a criação do ***National Data Center*** **(NDC)** – banco de dados único e revolucionário à época. Inicialmente, essa base armazenaria, de forma conjunta, informações de diferentes agências governamentais, tais quais dados populacionais, habitacionais, fiscais, previdenciários e empregatícios. Essa proposta objetivou diminuir custos e estudos estatísticos eficientes e altamente precisos.

A iniciativa recebeu apoio de algumas instituições, tal como o Princeton Institute for Advanced Study. Estas a defenderam com o argumento de que a

[46] Agência dos Direitos Fundamentais da União Europeia. Conselho da Europa. Handbook on European Data Protection Law. Luxemburgo, 2018, pp. 18-21.
[47] Em inglês: "*the Bureau of the Budget of the Executive Office of the President [of the United States]*". Atualmente, denominado "*Office of Management and Budget*".

possibilidade de aprimoramento da segurança da informação de uma base de dados centralizada aperfeiçoaria, também, a privacidade da nação.[48]

No entanto, os contrários à implementação do NDC afirmavam que a **concentração de dados a serem manipulados pelo Estado poderia resultar em desequilíbrio do poder e violação às liberdades civis**. O sociólogo Vance Packard publicou, no *The New York Times*, um artigo intitulado "*Don't Tell It to the Computer*", onde argumentou pela presença de riscos na centralização e **compartilhamento** de tantas informações pessoais. Para tanto, destacou a concentração de poder nos operadores do sistema de armazenamento devido ao acesso a detalhes da vida dos cidadãos.[49]

Diante dos impasses sobre o tema, o Congresso dos EUA convocou audiências em uma comissão própria, o *House Special Subcommittee on Invasion of Privacy*, em 1966. O discurso elaborado por Packard reforça que as implicações de permitir que o Governo Federal reúna, em bancos de dados centralizados, informações fornecidas por ou sobre seus cidadãos são de longo alcance.[50] O projeto representaria **ameaça à liberdade individual**, visto que o tratamento de dados pessoais inadequado provoca um aumento de poder do Estado e, por conseguinte, expõe a população ao seu controle.

Dessa forma, o processamento irrestrito de dados por diversos órgãos públicos de forma simultânea deveria ser matéria de regulação e limitação, em vista da defesa de direitos fundamentais e da necessidade de minimizar os riscos de elaboração de

---

[48] GARFINKEL, Simson. **Database Nation**. Sebastopol: O'Reilly, 2000. p. 14.

[49] "*The most disquieting hazard in a central data bank would be the placing of so much power in the hands of the people in a position to push computer buttons. When the details of our lives are fed into a central computer or other vast file-keeping stocking systems, we all fall under the control of the machine's managers to some extent*" (tradução livre: "[o] perigo mais inquietante em um banco de dados central seria colocar tanto poder nas mãos de pessoas em posição de apertar botões de computador. Quando os detalhes de nossas vidas alimentam um computador central ou outro vasto sistema de armazenamento de arquivos, todos nós, até certo ponto, nos tornamos submissos ao controle dos operadores da máquina". PACKARD, Vance. **Don't Tell It to the Computer**, *The New York Times Magazine*, 08/01/1976, p. 44 e ss. *apud* GARFINKEL, Simson, Op. cit., p. 14.

[50] US HOUSE. **The Computer and Invasion of Privacy. Hearings before a subcommittee of the committee on government operations house of representatives**. July 26, 27 and 28, 1966. p. 7. Disponível em: <https://archive.org/details/U.S.House1966TheComputerAndInvasionOfPrivacy>. Acesso em 20 fev. 2021.

dossiês e perfis dos cidadãos. Esses **riscos foram identificados já nos anos 1960**, de forma a colocar em contraste os benefícios e malefícios de um banco de dados amplo e compartilhado entre o Poder Público de um país.

Outro ponto levantado no Subcomitê foi a **falta de previsão de salvaguardas e medidas criteriosas que criassem um sistema íntegro e legítimo** para o armazenamento de tantas informações pessoais. Nesse sentido, Packard afirmou que, na ausência de salvaguardas, haveria pressão para a coleta e sistematização de informações adicionais sobre pessoas especificamente visadas pela Administração, para além dos dados já descritos na base pretendida.[51]

Ainda em relação aos titulares de dados, argumentou-se que uma **base de amplo acesso estatal** cercearia o desenvolvimento autônomo da personalidade; diminuiria a confiança no Governo devido à sensação de controle e supervisão contínua; e prejudicaria aqueles com informações imprecisas.[52]

À época, Packard frisou a necessidade de análise do **fundamento mais comum para bases de dados nacionais**: a eficiência estatal; visto que a centralidade de informações pode gerar um risco elevado e desproporcional para atingimento da eficiência máxima nas atividades do Estado.[53] Diante da experiência estadunidense, identifica-se a opacidade **do conceito de eficiência, bem como a dificuldade de se aferir sua concretização**.

Evidencia-se, portanto, que, para além das ferramentas de promoção da eficiência estatal, bases de dados nacionais impactam diretamente o exercício de liberdades civis e garantias fundamentais. Ao transpormos essa discussão para a atualidade, tal como ocorrera com a capacidade de processamento computacional e a

---

[51] *Idem,* p. 10.
[52] *Idem,* p. 12.
[53] Packard defende que figuras distópicas, como o Grande Irmão, do livro 1984 de George Orwell, podem acabar não sendo gananciosos buscadores de poder, mas sim burocratas implacáveis obcecados por eficiência. *Idem,* p. 13.

valoração da ciência de dados, os riscos decorrentes do tratamento de dados pessoais cresceram exponencialmente.

O **Congresso dos EUA decidiu rejeitar a proposta do *National Data Center***. Assim, concluiu-se que a privacidade dos cidadãos preponderou frente à criação de uma base de dados pela qual inúmeras entidades públicas poderiam acessar dados pessoais a nível nacional. A base centralizada estadunidense, portanto, não foi criada e as agências federais continuaram a tratar apenas informações já sob sua custódia.

Pouco depois, foi aprovado o ***Privacy Act* (1974)** a fim de estabelecer um código de práticas justas de informação que rege a coleta, manutenção, uso e disseminação de informações pessoais em sistemas de agências federais.[54] Para tanto, fixou mecanismos de **transparência e controle de dados por seus titulares,** a exemplo do dever de publicação de sistemas de registros nos meios de comunicação oficiais do governo e de disponibilizar meios de acesso e retificação aos titulares de dados.

b. França: SAFARI

Em 1970, o Instituto Nacional de Estatística da França apresentou um projeto semelhante ao estadunidense, o ***Système Automatisé pour lês Fichiers Administratifs et lê Répertoire de Individus*** (SAFARI). Foi uma tentativa do governo francês de criar uma base de dados que permitisse a identificação de cidadãos por diversos serviços governamentais[55] e que permitisse que órgãos estatais transferissem dados pessoais entre si. [56]

---

[54] THE UNITED STATES DEPARTMENT OF JUSTICE. **Privacy Act of 1974**. 2020. Disponível em: <https://www.justice.gov/opcl/privacy-act-1974>. Acesso em 20 fev. 2021.

[55] TRÉGUER, Félix. From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France. 7th Biennial Surveillance & Society Conference, Espanha, Barcelona, Abril, 2016. Disponível em: https://halshs.archives-ouvertes.fr/halshs-01306332v11/document. Acesso em 16 abr. 2021, pp. 7-9.

[56] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados, 2ª ed.. São Paulo: Thomson Reuters Brasil, 2019. p. 164.

Assim como nos EUA, uma publicação local, no jornal *Le Monde*, questionou os impactos negativos desse projeto às garantias fundamentais.[57] O artigo "*SAFARI ou la chasse aux Français*" descreveu o plano do Ministério do Interior francês de utilizar sistemas informáticos para compilar informações pessoais de todos os franceses e argumentou que um sistema centralizador, de fácil acesso aos órgãos do Estado, poderia minar seriamente as **liberdades e o equilíbrio do poder político**.[58] Com o debate iniciado, o **projeto foi rejeitado** pela sociedade e **o primeiro-ministro francês não autorizou qualquer interconexão de dados entre ministérios**.[59]

Como consequência, a França promulgou a **Lei de Proteção de Dados Pessoais (1978)** a fim de que a tecnologia da informação fosse colocada a serviço do cidadão. O diploma fixou que o tratamento de dados pessoais não deveria violar a identidade humana, os direitos humanos, a privacidade ou as liberdades individuais ou públicas.[60] Essa lei é reflexo das discussões iniciadas pela divulgação do projeto SAFARI e tem como escopo minimizar o uso indevido dos dados pessoais também no contexto do processamento de informações no setor público.

---

[57] Em 1974, o artigo "*SAFARI ou la chasse aux Français*" foi publicado no jornal Le Monde apresentando posição contrária ao desenvolvimento do projeto SAFARI em vista dos perigos de interconexão dos dados na Administração Pública. DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados, 2ª ed.. São Paulo: Thomson Reuters Brasil, 2019. p. 164.

[58] BOUCHER, Philippe. **Une division de l'informatique est créée à la chancellerie "Safari " ou la chasse aux Français**. 1974. Disponível em: https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html, Acesso em 20 fev. 2021.

[59] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados, 2ª ed.. São Paulo: Thomson Reuters Brasil, 2019. p. 164.

[60] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties**. Disponível em: https://fra.europa.eu/en/law-reference/act-ndeg78-17-6-january-1978-data-processing-data-files-and-individual-liberties. Acesso em 20 fev. 2021.

c. Decisão do Tribunal Constitucional Alemão em 1983

Outro caso relevante sobre o tratamento de dados pela Administração Pública ocorreu na Alemanha no início dos anos 1980. Com o aumento do fluxo de dados pessoais e a necessidade de proteção dessas informações como forma de garantir equilíbrio de poder e preservação de direitos, o Tribunal Constitucional Alemão, ao analisar a constitucionalidade da Lei de Recenseamento de 1983 (*Volkszählungsgesetz)*, reconheceu a existência do **direito à autodeterminação informativa** no ordenamento jurídico.[61]

A lei em questão tinha como objetivo coletar informações sobre profissão, moradia e outros âmbitos da vida do cidadão para fins estatísticos, mas permitia a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para fins administrativos. Diante disso, a Corte confirmou a constitucionalidade da lei, mas **declarou nulos os dispositivos que autorizavam a transmissão de dados entre órgãos públicos**, já que representavam um risco aos titulares de dados de perderem o controle sobre seus dados pessoais.[62] Este caso evidencia a principal problemática de cadastros nacionais: o compartilhamento e acesso de dados pessoais entre órgãos públicos como se fossem um grande e único agente.

A "autodeterminação sobre a informação", de acordo com o Tribunal Constitucional Alemão, assegura autonomia e controle ao titular dos dados pessoais, ou seja, a garantia de decidir de forma livre e racional para qual finalidade seus dados seriam tratados.[63] O tribunal concluiu que "**quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas [...] pode**

---

[61] Disponível em https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=15.12.1983&Aktenzeichen=1%20BvR%20209%2F83

[62] MARTINS, Leonardo (Org.). **Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Konrad-Adenauer-Stiftung E. V., 2005., p. 233. Disponível em: <https://www.kas.de/c/document_library/get_file?uuid=c0b3d47d-beba-eb55-0b11-df6c530ddf52&groupId=252038>. Acesso em 20 fev. 2021.

[63] MIRAGEM, Bruno. **A lei geral de proteção de dados (Lei 13.709/2018) e o direito do consumidor**. Revista dos Tribunais, v. 1009, p. 173-222, nov., 2019. p. 2.

ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação".[64] Disto decorre que o titular de dados pessoais deve estar ciente das informações disponibilizadas, bem como de cada instituição recipiente. Somente então viabiliza-se sua autodeterminação e o livre desenvolvimento da personalidade.

O julgamento também reconheceu a **separação informacional de poderes**. Tal como mencionado na **Seção II** e na decisão alemã, esse conceito está alinhado com a obrigação de que "todas as autoridades que reúnem dados pessoais para cumprir suas tarefas devem se restringir ao mínimo indispensável para alcançar seu objetivo definido".[65] Diante da previsão de finalidades amplas, a decisão alemã introduziu uma espécie de separação de poderes no tratamento de dados. Isso porque seria "**incompatível com a proteção de dados a possibilidade de Administração Pública e o Estado serem concebidos como uma unidade informacional**".[66] Com isso, a divisão de competência e o princípio da finalidade se tornaram centrais para a identificação de quais dados são imprescindíveis e proporcionais para o alcance de algum objetivo por um órgão específico da Administração Pública.

No contexto alemão, a **Lei Federal de Proteção de Dados, de 1977,** foi central para a decisão da Corte Constitucional no caso da Lei de Recenseamento. Esse marco legislativo teve como escopo proteger as informações pessoais contra tratamento abusivo e, para isso, previu direitos ao titular, a exemplo do direito à informação, retificação e eliminação de dados. De forma específica, a lei alemã determinava que organizações públicas e privadas que processassem dados pessoais deveriam adotar medidas organizacionais e técnicas necessárias para tutela da proteção de dados.[67]

---

[64] MARTINS, Leonardo (Org.). Op. Cit., p. 237.
[65] MARTINS, Leonardo (Org.). Op. Cit., p. 240.
[66] IACOMINVS. **Separação de poderes informacional**. 2020. Disponível em: https://near-lab.com/2020/10/04/separacao-de-poderes-informacional/. Acesso em 20 fev. 2021.
[67] ASSMANN, Jhonata. **O direito à autodeterminação informativa no direito germânico e brasileiro**. 2014. Monografia (Graduação em Direito) - Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina. Florianópolis, p. 41. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/117169/Jhonata%20Assmann%20TCC%20pdfa.pdf?sequence=1&isAllowed=y>. Acesso em 20 fev. 2021.

Logo, foram prescritas formas de se garantir direitos e a proteção de dados pessoais também frente ao tratamento realizado pelo Poder Público.

d. O Decreto nº 10.046/2019 à Luz das Experiências Estrangeiras

Os projetos de construção de uma base de dados nacional que possibilita o compartilhamento facilitado de dados pessoais não alcançaram êxito nos países analisados devido aos questionamentos acerca de violações de direitos fundamentais e riscos decorrentes do controle estatal sobre indivíduos. Com relação às ameaças representadas por esses projetos, foram elaboradas legislações específicas para endereçar a concretização do direito à proteção de dados.

Tais formas iniciais de regulação são conhecidas na literatura especializada[68] como a **primeira geração de leis de proteção de dados.** Essas foram elaboradas como resposta ao advento do processamento eletrônico de dados dentro do aparato estatal e de grandes corporações, além dos projetos nacionais de bancos de dados centralizados[69]. O conjunto regulatório é marcado pelo impasse entre a necessidade estatal de tratar dados para alcançar maior eficiência e os riscos a direitos e liberdades fundamentais.

Para o Prof. Viktor Mayer-Schönberger, vários dos primeiros estatutos de proteção de dados abordam explicitamente a **ameaça do tratamento de dados para o equilíbrio de poder dentro do governo**. Como o poder executivo coleta uma expressiva quantidade de dados individuais, este possui um poderoso **instrumento de planejamento e controle de poder**.[70]

Nesse sentido, para além da primeira geração de leis, que inclui a Lei Federal de Proteção de Dados alemã (1977), a segunda geração passou a reconhecer a proteção de

[68] MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. *In*: Technology and privacy: the new landscape. Cambridge: MIT Press, 1997. p. 219-241.
[69] *Idem*, p. 224.
[70] *Idem*, p. 224.

dados pessoais como uma liberdade negativa, como é o caso da Lei de Proteção de Dados francesa (1978).[71] A terceira geração surgiu nos anos 1980 com o paradigma inaugurado pelo julgamento da Corte Alemã. O caso inspirou diversos países a promulgarem leis de proteção de dados fundamentadas no conceito de autodeterminação informativa.[72]

Além disso, o **desenvolvimento tecnológico acabou por não evoluir em direção à criação de um banco de dados único e central.** Neste ponto, a professora Laura Schertel afirma que "foram desenvolvidas técnicas para permitir o processamento de dados de forma descentralizada, como os PCs (computadores pessoais), o que transformou completamente o debate sobre a proteção de dados pessoais".[73]

Assim, a solução de descentralização, aliada à criação e o acesso a bases com dados delimitados e necessários para a finalidade específica de cada órgão público é suficiente para os objetivos estatais. Isso porque o acesso e tratamento de dados pessoais desnecessários ou inadequados aos fins do órgão público individualmente considerado colocam em risco os direitos fundamentais.

De modo a trazer o debate a uma perspectiva mais recente, dos anos 2000, vale analisar a decisão do Tribunal de Justiça da União Europeia (TJUE) no **caso Huber v. Alemanha**.[74] Na ocasião, o Escritório Federal de Migração e Refugiados rejeitou o pedido de Heinz Huber, um nacional austríaco residente na Alemanha, para que seus dados fossem deletados do Registro Central de Estrangeiros (RCE). Este centralizava

---

[71] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], 12(2), 91-108, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em 20 fev. 2021.

[72] MAYER-SCHÖNBERGER, V. "**Generational Development of Data Protection in Europe**". In: AGRE, P.; ROTENBERG, M. Technology and Privacy: the New Landscape. Cambridge: MIT Press, 1997.

[73] SCHERTEL, Laura. Op. Cit., p. 32.

[74] UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia (Grande Seção). Julgamento. Heinz Huber v. República Federal da Alemanha (C-524/06). Relator: Juiz Egils Levits. Luxemburgo, 16 dez. 2008. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62006CJ0524&from=EN>. Acesso em 18 abr. 2021.

dados de estrangeiros residentes na Alemanha para fins estatísticos; persecução penal; e aplicação da legislação sobre residência.

O TJUE destacou que esta última finalidade era legítima; mas que o tratamento de dados apenas seria legal se o RCE armazenasse somente o necessário para tal fim. Para tanto, condicionou que (i) apenas as autoridades competentes para aplicar tal legislação deveriam ter acesso e (ii) a centralização de dados deveria tornar tal aplicação mais eficaz. Por fim, considerou desnecessário - portanto, ilegal - o acesso ao RCE para fins estatísticos e persecução penal, vez que, o primeiro, poderia ser realizado com dados anonimizados e, o segundo, constituía discriminação em razão de nacionalidade.[75]

À luz das preocupações levantadas desde os anos 1960, percebe-se que o **Decreto nº 10.046/2019 ignora a experiência histórica internacional** ao não criar mecanismos para que os titulares de dados exerçam seus direitos, não estabelecer ferramentas e critérios mínimos de segurança da informação, além de não definir instrumentos legais e técnicos que garantam a privacidade e a autodeterminação informativa.

A separação informacional dos poderes, em conformidade com o direito à autodeterminação, deve ser observada pelo ecossistema brasileiro de proteção de dados.[76] Tal conceito, introduzido na decisão alemã, evita o acúmulo excessivo e desproporcional de dados pela Administração Pública e identifica os **riscos no compartilhamento amplo de dados entre órgãos do setor público como facilitador de atividades vigilantistas**.

Os questionamentos suscitados ainda no século passado não foram devidamente endereçados pelo Decreto. Portanto, os desafios ora presentes

---

[75] Idem, §§ 53-68.

[76] MARANHÃO, Juliano; CAMPOS, Ricardo. **A divisão informacional de poderes e o cadastro base do cidadão**. Jota, 18 out. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019>. Acesso em 20 fev. 2021.

assemelham-se **aos evidenciados no debate supracitado, porém maior escalonados, porquanto o estado avançado da ciência de dados contemporânea torna exponencial o risco à liberdade, autonomia e privacidade dos cidadãos**.

V. DA FRÁGIL SEGURANÇA DA INFORMAÇÃO NO ESTADO BRASILEIRO

A segurança da informação é um eixo central para as atividades do Estado, especialmente considerando as iniciativas para maximização da eficiência administrativa pelo projeto de Governo Digital do Governo Federal. O Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIRGov), órgão encarregado de responder a incidentes de segurança da informação no âmbito da Administração Pública federal, disponibiliza estatísticas de notificações reportadas e de incidentes e vulnerabilidades confirmados[77].

Os números são alarmantes. Somente em 2020, **o CTIRGov recebeu 24.303 notificações e confirmou 5.442 incidentes e 2.489 vulnerabilidades nos sistemas usados pelo Estado**, o que demonstra que a segurança da informação da Administração Pública federal é extremamente frágil.

No final de 2020, um vazamento de senhas do Ministério da Saúde permitiu o acesso a dados de pacientes diagnosticados ou com suspeita de Covid-19.[78] Uma semana depois, uma falha no e-SUS Notifica permitiu o vazamento de dados de mais de duzentos milhões de cidadãos.[79]

Em fevereiro de 2021 houve uma invasão ao FormSUS, serviço de criação de

---

[77] Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo. **CTIRGov em Números**. Disponível em: <https://emnumeros.ctir.gov.br/>. Acesso em 20 fev. 2021.

[78] CAMBRICOLI, Fabiana. Vazamento de senha do Ministério da Saúde expõe dados de 16 milhões de pacientes de covid. O Estado de S.Paulo. São Paulo, 26 nov. 2020. Disponível em: <https://saude.estadao.com.br/noticias/geral,vazamento-de-senha-do-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid,70003528583>. Acesso em 18 abr. 2021.

[79] CAMBRICOLI, Fabiana. Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. O Estado de S.Paulo. São Paulo, 02 dez. 2020. Disponível em: <https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340>. Acesso em 18 abr. 2021.

formulários do DataSUS.[80] No mesmo mês, um vazamento de dados do INSS expôs dados de centenas de milhões de brasileiros, incluindo endereço, telefone, e-mail, score de crédito e renda, dentre outras informações.[81]

Esses exemplos (que sequer esgotam os incidentes ocorridos no ano de 2021 em órgãos públicos) evidenciam não só os riscos já mencionados aqui, como demonstram o cenário de descaso e ausência de adoção de salvaguardas e medidas que protejam dados dos cidadãos por parte de diversos órgãos públicos.

A seguir, veremos como a LGPD disciplina a segurança da informação e as boas práticas, e, por fim, quais são as práticas de segurança da informação descritas no Decreto nº 10.046/2019.

a. Segurança da Informação e Boas Práticas na LGPD

O Capítulo VII da LGPD trata (i) da segurança e do sigilo dos dados e (ii) das boas práticas e governança, determinando que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a impedir incidentes de segurança da informação (art. 46). Tais medidas devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução, conceito denominado como ***privacy by design*** (art. 46, §2º).[82]

Adicionalmente, a LGPD dispõe também que qualquer agente que se envolver

---

[80] SOUZA CRUZ, Bruna. Hacker sincero: sistema do Ministério da Saúde é novamente alvo de invasão. UOL, Tilt. São Paulo, 18 fev. 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/02/18/hacker-sincero-sistema-do-ministerio-da-saude-e-novamente-alvo-de-invasao.htm>. Acesso em 18 abr. 2021.

[81] ROHR, Altieres. Megavazamentos de dados expõem informações de 223 milhões de números de CPF. G1. 25 jan. 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml>. Acesso em 18 abr. 2021.

[82] EUROPEAN DATA PROTECTION BOARD. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Bélgica, Bruxelas, 13. nov. 2019. Disponível em: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf>. Acesso em 18 abr. 2021, pp. 6-10.

em uma das fases do tratamento de dados fica obrigado a garantir a segurança da informação dos dados (art. 47). Ainda, na ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, a Autoridade Nacional de Proteção de Dados - ANPD e os titulares de dados afetados deverão ser comunicados em prazo razoável, a ser definido pela ANPD (art. 48).

No artigo 49, a LGPD determina que "os sistemas utilizados no tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos" na própria Lei e nas normas regulamentares que a ANPD editará. Além disso, **a LGPD recomenda, de forma extensa, a institucionalização de boas práticas e de governança pelos agentes de tratamento de dados**, que "poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

Cabe destacar que **a atuação da ANPD nesta frente é essencial** para definir e estimular a adoção de padrões técnicos aplicáveis, receber comunicações de incidentes, bem como ratificar, promover e divulgar boas práticas das organizações públicas e privadas. Na agenda regulatória do biênio 2021-2022, a ANPD já destaca a importância da segurança da informação, tendo iniciado o processo regulatório para elaboração de resolução sobre notificação de incidentes de segurança da informação em 22 de fevereiro de 2021[83], por meio da Tomada de Subsídios nº 2/2021.

[83] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **ANPD inicia processo de regulamentação sobre incidentes de segurança com tomada de subsídios**. Gov.br, 22 fev. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-processo-de-regulamentacao-sobre-incidentes-de-seguranca-com-tomada-de-subsidios>. Acesso em 22 fev. 2021.

b. Segurança da Informação no Cadastro Base do Cidadão

O Decreto traz disposições genéricas e omissas relativas à segurança da informação no contexto do CBC, restringindo-se a definir "requisitos de segurança da informação e comunicação" (art. 2º, XXIII) e consignar que "a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na LGPD".

O texto do Decreto menciona o termo "segurança" onze vezes, mas apenas de forma programática como um fator a ser observado no compartilhamento de dados.[84] Destaca-se que o Decreto dispõe, no art. 12, que os órgãos solicitantes e recebedores de dados deverão se submeter às regras de sigilo e segurança da informação definidas pelo CCGD. O art. 21 também lista como competências do CCGD a definição de regras, parâmetros e padrões relativos à preservação do sigilo e da segurança (inciso II) e a compatibilidade entre as políticas de segurança da informação dos órgãos (inciso III).

Observa-se que o *privacy by design*, positivado no art. 46, §2º[85], da LGPD, não foi observado na criação e implementação do CBC, pois não há nenhum indicativo de medidas concretas de segurança, técnicas e administrativas dispostas no texto do Decreto, nas regulações do CCGD ou nos sites do Governo Digital, que demonstrem o cumprimento da lei ou a adoção desta prática.

Há grande risco em permitir amplo compartilhamento por gestores públicos de tantos dados dos cidadãos brasileiros, como o de vazamentos e acessos indevidos. De acordo com o CTIRGov, **somente em 2020 foram registrados 404 vazamentos de**

---

[84] ANASTÁCIO, Kimberly; VARON, Joana; SANTOS, Bruna. **Cadastro Base do Cidadão**: A Megabases de Dados. Coding Rights. Dez 2020, p. 19. Disponível em: <https://www.codingrights.org/docs/megabase.pdf>. Acesso em 20 fev. 2021.

[85] LGPD, Art. 46: "Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito. (...) § 2º As medidas de que trata o caput deste artigo deverão ser observadas **desde a fase de concepção do produto ou do serviço até a sua execução**" (grifou-se).

dados na Administração Pública federal[86]. Com isso em mente, quais garantias e salvaguardas o governo federal implementou para mitigar os riscos envolvendo incidentes de segurança da informação no âmbito do Cadastro Base do Cidadão?

Vale destacar como precedente recente de incidente de segurança em bases de dados integradas contendo dados de bilhões de cidadãos o vazamento de dados pessoais e sensíveis ocorrido na Índia no começo de 2018. O país implementou um sistema chamado *Aadhar*, buscando aplicar biometria para evitar fraudes e garantir acesso facilitado a políticas públicas de saúde, educação e assistência social. Os dados do sistema foram integrados a um banco de dados central sob responsabilidade da *Unique Identification Authority of India* (UIDAI), onde ficam ligados a dados biométricos de íris e impressões digitais.[87]

Um jornal local da Índia, The Tribune, publicou um relatório alegando que os dados foram vazados e que seus repórteres pagaram aproximadamente 8 dólares para obter acesso ao UIDAI, o que os possibilitou tratar dados pessoais de aproximadamente 1,2 bilhão de cidadãos indianos.[88]

Em conclusão, **a frágil segurança da informação adotada pelo Estado brasileiro e as vulnerabilidades relacionadas ao tratamento de expressivo volume de dados demonstram os riscos que envolvem a operacionalização do CBC** enquanto instrumento de ampliação de acesso a dados na Administração Pública federal.

Afinal, caso não se altere o curso dos eventos recentes, as disposições do Decreto podem proporcionar riscos imensos de vazamentos e incidentes de segurança que podem comprometer de forma irreversível a privacidade e a proteção

---

[86] CTIRGov, Op. cit.
[87] UNIQUE IDENTIFICATION AUTHORITY OF INDIA. Aadhar Handbook for Residents. Índia, Nova Delhi, Mar. 2021. Disponível em: <https://uidai.gov.in/images/AadhaarHandbook2021.pdf>. Acesso em 18 abr. 2021.
[88] DIXIT, Pranav. **India's National ID Database With Private Information Of Nearly 1.2 Billion People Was Reportedly Breached**. BuzzFeed News, 04 jan. 2018. Disponível em: <https://www.buzzfeednews.com/article/pranavdixit/indias-national-id-database-with-private-information-of>. Acesso em 20 fev. 2021.

de dados no Brasil. A carência de instrumentos que garantam os direitos de titulares de dados, como demonstrado ao longo do texto, torna o Decreto 10.046/2019 um instrumento que pode trazer perigos expressivos à sociedade.

VI. DA CONCLUSÃO

A privacidade e a proteção de dados são direitos fundamentais essenciais para que aqueles sob jurisdição brasileira sejam empoderados a exercer o livre pensamento e a autodeterminação, de forma a plenamente concretizar a cidadania e expandir as liberdades civis.[89] Ou seja, esses direitos são elementares para o integral exercício da democracia e, portanto, à legitimidade do Estado Democrático de Direito.

Rodotà afirmou que "[a] sociedade da informação propõe novos desafios à democracia. Oferece a ela a possibilidade de coletar qualquer informação sobre os cidadãos, com o argumento de que tudo pode enfim se revelar útil para a tutela da segurança, da saúde, e assim por diante. Mas a democracia é também sobriedade, até mesmo renúncia, quando pode existir um risco para a liberdade dos cidadãos."[90]

Considerando que a relação entre cidadão e Estado não é voluntária, transcorrendo desde o nascimento até a morte, compreende-se que a confiança no Estado deve ser construída cotidianamente por meio de políticas públicas e procedimentos que (**i**) sejam pautados na estrita legalidade, (**ii**) deem transparência e publicidade às ações governamentais e (**iii**) promovam *accountability*. **O Decreto nº 10.046/2019 contraria tais preceitos, contando com diversas fragilidades e omissões em seu texto.**

---

[89] DEBRABANDER, Firmin. **The Problem With "Privacy"**. Jacobin, 18 nov. 2020. Disponível em: <https://www.jacobinmag.com/2020/11/covid-19-privacy-big-data-surveillance>. Acesso em 20 fev. 2021.

[90] RODOTÀ, Stefano. **A Vida na Sociedade de Vigilância**: A privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 162.

Em resumo, o Decreto desrespeita os princípios regentes da proteção de dados pessoais; não fixa mecanismos que garantam o exercício de direitos por seus titulares; não opera como base legal válida para atividade de tratamento; e tampouco apresenta medidas de segurança adequadas.

A norma também promove fragmentação terminológica ao definir conceitos que conflitam com aqueles da LGPD. Sua sistemática de controle de acesso aos dados utiliza categorizações estanques que falham em endereçar as peculiaridades contextuais que a proteção de dados demanda em cada circunstância. Além de confundir a classificação de dados, permite sua transmissão ampla e potencialmente irrestrita entre os órgãos públicos como se todos formassem uma entidade única. Ainda na década de 1970, essas questões foram enfrentadas por outros países que optaram por não criar sistemas de acesso amplo aos órgãos públicos.

Nesta manifestação, o **Laboratório de Políticas Públicas e Internet - LAPIN**, em parceria com a **Coalizão Direitos na Rede - CDR**, se propôs a explicitar e aprofundar eixos centrais que revolvem a controvérsia, abordando a aplicação da LGPD no tratamento de dados pelo Poder Público, dissecando o funcionamento técnico do CBC e a experiência internacional na Europa e nos EUA sobre bases nacionais centralizadas, similares ao caso *sub judice*. Isto posto, **recomendam sejam deferidos os pedidos feitos na inicial desta Ação Direta de Inconstitucionalidade.**

Termos em que,

Pede deferimento.

Brasília/DF, 05 de maio de 2021.

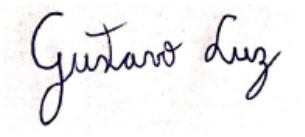
José Renato Laranjeira de Pereira

OAB/DF nº 59.985

Paulo Henrique Atta Sarmento

OAB/DF nº 63.259

LAPIN
LABORATÓRIO DE POLÍTICAS PUBLICAS E INTERNET



Gustavo Henrique Luz Silva

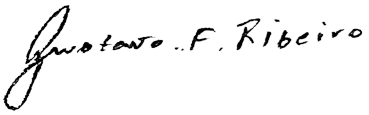
CPF nº 442.225.898-29

Eduarda Costa Almeida

CPF nº 054.702.991-80

Julia D'Agostini Alvares Maciel

OAB/MG nº 193.547



Gustavo Fonseca Ribeiro

CPF nº 062.783.047-16

Henrique Bawden Silverio de Castro

OAB/DF nº 58.680