OBSERVATÓRIO DA LGPD
UNIVERSIDADE DE BRASÍLIA

ANÁLISE COMPARADA
LGPD E GDPR

ORGANIZADORES

LAURA SCHERTEL MENDES

GIOVANNA MILANESE

FELIPE ROCHA DA SILVA

TAYNÁ FROTA DE ARAÚJO

ISABELA MARIA ROSAL

PAULO RICARDO SANTANA

EDUARDA COSTA

ELIS BRAYNER

ANUÁRIO DO OBSERVATÓRIO DA LGPD DA UNIVERSIDADE DE BRASÍLIA

VOLUME 1

Universidade de Brasília
Faculdade de Direito

Anuário do Observatório da LGPD da Universidade de Brasília

Análise comparada entre elementos da LGPD e do GDPR

Volume 1
Brasília-DF
2023

Anuário do Observatório da LGPD da Universidade de Brasília: Análise comparada entre elementos da LGPD e do GDPR.

Para esclarecimentos sobre esta obra, entrar em contato com observatorio.lgpd.unb@gmail.com

Volume 1

Organização
Coordenação Geral: prof.ª Laura Schertel Mendes;
Coordenação Adjunta: Giovanna Milanese;
Coordenação de Pesquisa: Felipe Rocha e Tayná Frota de Araújo;
Revisão e Organização: Eduarda Costa Almeida, Elis Bandeira A. Brayner, Isabela Maria Rosal e Paulo Ricardo da Silva Santana.

Informações

Observatório da LGPD/Unb
Faculdade de Direito
Universidade de Brasília
Campus Universitário Darcy Ribeiro, CEP: 70.910-900, Brasília-DF, Brasil

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Central da Universidade de Brasília – BCE/UNB)

A636 Anuário do Observatório da LGPD da Universidade de Brasília [recurso eletrônico] : análise comparada entre elementos da LGPD e do GDPR / organização Laura Schertel Mendes … [et al.]. – Brasília : Universidade de Brasília, Faculdade de Direito, 2024. 2 v.

Inclui bibliografia. Modo de acesso: World Wide Web.

ISBN 978-65-00-92398-8 (v. 1).

ISBN 978-65-00-92399-5 (v. 2).

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Universidade de Brasília. 3. Proteção de dados. 4. Direito comparado. I. Mendes, Laura Schertel (org.).

CDU 34

AUTORES

Ana Júlia Prezotti Duarte

Andressa Carvalho Pereira

Angélica Opata Vettorazzi

Gabriel de Araújo Oliveira

Gabriel Cabral Furtado

Eduarda Costa Almeida

Fernanda Passos Oppermann Ilzuka

Isabela de Araújo Santos

Júlia Carvalho Soub

Shana Schlottfeldt

Sofia de Medeiros Vergara

Paulo Ricardo da Silva Santana

Rafael Luís Müller Santos

Wanessa Larissa Silva de Araújo

REVISORES

A realização deste anuário contou com a significativa participação de revisores, que atuaram na avaliação e revisão dos artigos submetidos pelos pesquisadores do Observatório, fornecendo orientações e sugestões de melhoria. Oferecemos nosso mais sincero agradecimento pelas valiosas contribuições de cada um.

Ana Luísa Vogado de Oliveira

Angelo Prata de Carvalho

Davi Ory

Gabriel Fonseca

Isabela Maria Rosal Santos

Maria Cristine Lindoso

Matheus Vinicius Aguiar

Paula Baqueiro

Tainá Aguiar Junquilho

Thiago Guimarães Moraes

SUMÁRIO

LIMITES AO COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE OS ENTES DO PODER PÚBLICO

Júlia Carvalho Soub[1]

Introdução

A distopia literária 1984 de George Orwell demonstra um dos maiores medos da atualidade, isto é, a constante sensação de vigilância pelo governo para com seus cidadãos. Com o advento e avanço da tecnologia esse medo demonstra-se ainda mais palpável, sendo amplamente demonstrado pela arte, a exemplo das séries "Pessoa de interesse" e "Bull".

Diante desse cenário, a fim de que a vida não volte a copiar a arte, o presente artigo busca compreender os limites à possibilidade de o Estado compartilhar dados pessoais de seus cidadãos entre os entes do Poder Público. Isso porque o compartilhamento público-público é fundamental para a maior eficiência e desenvolvimento das atividades administrativas do governo. Todavia, sem as devidas limitações, poderia resultar em cenários indesejados de vigilância (WIMMER, 2021- b), a exemplo dos referenciados como o do *Big Brother*.

Por conseguinte, o presente artigo tem como objetivo identificar quais os limites ao compartilhamento público-público, excluindo-se da presente análise o compartilhamento de dados entre o Estado e entes privados. Para tanto, no tópico 1 - comentários - será feita uma revisão bibliográfica, com o intuito de assimilar as considerações doutrinárias sobre o tema. Ademais, serão analisados, enquanto parâmetros de limitação do referido compartilhamento, os dispositivos do *General Data Protection Regulation* (GDPR), relativos ao art. 5º, 1, b e o art. 6º, 4, a, b, c, d, e.

Posteriormente, examinar-se-á no tópico 2 - estudo de caso - a decisão proferida na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6529 (MC-ADI 6529), caso no qual se questiona o compartilhamento de dados entre o DETRAN e a ABIN. Será, então, exposta uma breve síntese da referida decisão no subtópico 2.1. O subtópico 2.2, por sua vez, destinar-se-á ao exame da rejeição ao isolamento do interesse público no tratamento de dados

[1] Graduanda no Curso de Direito da Universidade de Brasília. Pesquisadora do Observatório da LGPD da Universidade de Brasília 2020-2021.

pessoais pelo Poder Público, haja vista decisões proferidas pelo Supremo Tribunal Federal. Para além, no subtópico 2.3 será examinada a deliberação da Corte Europeia de Direitos Humanos (CEDH) no caso paradigma *Big Brother and Others vs. The United Kingdom,* a fim de se explorar o cenário que o presente artigo pretende evitar ao sugerir limitações ao tratamento de dados pessoais dos cidadãos brasileiros pelos entes públicos.

Por fim, observar-se-á que a visão dicotômica entre interesse público e privado não se faz adequada para a proteção dos dados pessoais dos cidadãos em relação ao Estado. Isso porque, a relevância, proporcionalidade e razoabilidade do compartilhamento de dados pessoais para a realização do tratamento secundário desses pela Administração Pública apenas poderá ser observada *in concreto*, a partir de uma análise de observância dos princípios constitucionalmente impostos, conforme fora feito na MC-ADI 6529, ora analisada. Para além, verificar-se-á que o conhecimento europeu em muito pode acrescentar nas possibilidades de limitação do poder estatal no que diz respeito ao tratamento das informações dos indivíduos.

1. Comentários

O tratamento de dados pessoais dos cidadãos pelo Estado não é um tema recente, apesar de ter se intensificado e de ter ganhado destaque com a revolução tecnológica. Nesse cenário, sem pretensões de usufruir desse termo de maneira anacrônica, porém a fim de exemplificar a situação apresentada, é possível verificar que o ente estatal a muito concentra a tutela de documentos essenciais, como certidões de nascimento, de casamento e de óbito, que geram dados pessoais. Ou seja, informações pessoais individualizadas/individualizáveis (MENDES, 2021), que, a depender da forma de utilização e interpretação, poderão gerar consequências positivas e/ou negativas aos titulares desses dados (MENDES; MATTIUZZO; FUJIMOTO, 2021).

Dessa maneira, faz-se imprescindível compreender que na atual sociedade da informação, os indivíduos estão a todo momento a produzir dados pessoais, seja com o intuito de desenvolver relações sociais, por intermédio de redes sociais como o *instagram* e o *tik tok*, seja com a compra de medicamentos em farmácias - que não raro solicitam o CPF do cliente. No caso específico de coleta de dados pelo Poder Público, verifica-se que inúmeras são as fontes de coletas de dados, dentre as quais destaca-se o cadastro em sites ou enquanto requisito para obtenção de serviços públicos (CELLA; COPETTI, 2017).

Diante dessa perspectiva, a utilização crescente dos dados pessoais (*input*) para o tratamento de dados, fenômeno também denominado como *big data*, exige a existência de uma assídua preocupação com as consequências que o processamento desses poderá trazer aos indivíduos e os riscos aos quais esses estarão expostos. Nesse sentido, tem-se que as consequências geradas poderão ser drásticas para a vida dos cidadãos, na hipótese de produção de resultados discriminatórios, ilícitos ou abusivos (MENDES; MATTIUZZO; FUJIMOTO, 2021).

A conjuntura apresentada torna-se ainda mais complexa na hipótese de tratamento de dados pessoais pelo Poder Público, haja vista a relação verticalizada entre Estado e cidadão. Essa evidente desigualdade entre titular e controlador de dados é envolta por uma situação de dependência, na qual o cidadão depende do Estado para usufruir de serviços públicos, a exemplo da saúde pública (BLACK; STEVENS, 2013).

Contudo, a tecnologia possui papel fundamental na performance estatal e viabiliza que, a partir do tratamento de dados pessoais, os órgãos e entidades públicas desempenhem seu papel da forma mais eficiente possível e, para além, que as próprias políticas públicas sejam melhor desenhadas e executadas (MENDES; MACHADO; GASIOLA, 2021).

Logo, o compartilhamento dos referidos dados entre os entes que compõem o Poder Público apresenta-se enquanto importante ferramenta no contexto governamental. Tanto é, que o art. 26 da Lei Geral de Proteção de Dados Pessoais (LGPD) autoriza o referido compartilhamento para "execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas", sendo, portanto, a base legal para o denominado tratamento secundário diante da lógica *ex ante* proposta pela LGPD (WIMMER, 2021-a).

Esse dispositivo, apesar de reforçar a necessidade de observância aos princípios de proteção de dados pessoais discriminados no art. 6º da LGPD, autoriza o compartilhamento de forma ampla e, portanto, faz-se fundamental compreender quais os limites para a realização desse (WIMMER, 2021-a). A necessidade de limitações impostas ao tratamento efetuado pelo Poder Público é proveniente da própria noção de respeito aos direitos fundamentais dos indivíduos pelo Estado, dando-se enfoque no presente artigo à proteção da privacidade.

Entende-se, nesse sentido, a privacidade como um direito abrangente, no qual o indivíduo poderá desenvolver sua personalidade, independente de constrangimentos sociais para adotar determinados comportamentos. Assim, este deverá ser "deixado em paz" para que

tenha espaço suficiente para refletir sobre quem pretende ser (SARLET *apud* ARIENTE *et al.*, 2020), todavia, isso não significa dizer que possuirá total controle sobre o tratamento de seus dados pessoais, a fim de, por exemplo, impedir que a Receita Federal processe sua declaração de imposto de renda (WIMMER, 2021- b).

Diante desse cenário, é extremamente importante compreender que a Administração Pública, enquanto concretizadora da previsão abstrata da lei, necessita avaliar o contexto fático, a fim de optar e executar as Políticas Públicas. Dentro dessa lógica estatal, os dados pessoais dos cidadãos apresentam grande relevância, haja vista a atual sociedade da informação (MENDES; MACHADO; GASIOLA, 2021).

O art. 26 da LGPD, por conseguinte, foi promulgado com o intuito primordial de viabilizar o compartilhamento de dados entre os órgãos e entidades do Poder Público - compartilhamento Público-Público (WIMMER, 2021-a) -, concretizando, portanto, o princípio da eficiência, previsto no art. 37, *caput*, da Constituição Federal.

No entanto, ainda que vise promover maior agilidade à Administração, conforme fora anteriormente destacado, sua natureza principiológica e harmônica para com os ideais trazidos na LGPD deixa evidente a necessidade de observância aos princípios previstos no art. 6º desta lei (WIMMER, 2021-a). Desta feita, destacam-se aqueles presentes nos incisos I, II e III. Vejamos:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - **finalidade:** realização do tratamento para **propósitos legítimos, específicos, explícitos e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - **adequação:** compatibilidade do tratamento com as **finalidades informadas** ao titular, de acordo com o contexto do tratamento;
> III - **necessidade**: 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; **(GRIFOS NOSSOS)**

Mediante a leitura dos referidos incisos, é possível aferir que os dados compartilhados entre os entes do Poder público apenas poderão dar ensejo a um tratamento secundário que tenha finalidade compatível com o tratamento que possibilitou a coleta dessas informações individualizadas, sendo, portanto, uma das mais relevantes limitações ao compartilhamento público-público (WIMMER, 2021-a).

Essa adequação às finalidades informadas ao titular deverá estar sempre combinada ao mínimo tratamento necessário, uma vez que deverão os dados serem sempre pertinentes, proporcionais e não excessivos, para que não se tenha um resultado viciado, com correlações abusivas ou ilícitas (MENDES; MATTIUZZO; FUJIMOTO, 2021).

Apesar de serem balizas de extrema relevância, a finalidade, adequação e necessidade não são suficientes para limitar o poder estatal, a fim de que o tratamento secundário de dados não origine um verdadeiro cenário de vigilância. Assim, a título de aplicar a experiência internacional no contexto brasileiro, entende-se que os artigos 5, 1, b, e 6, 4, da GDPR poderão ser entendidos enquanto excelentes balizas limitadoras para o referido compartilhamento de dados. Verifiquemos, portanto, sua redação em português:

> **Artigo 5. Princípios relativos ao tratamento de dados pessoais**
>
> 1. Os dados pessoais são:
>
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e **não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades**; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89. , n. 1 («l**imitação das finalidades**»);
>
> **Art. 6. Licitude do tratamento**
>
> 4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23. o , n. o 1, o responsável pelo tratamento , a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:
>
> a) Qualquer **ligação entre a finalidade** para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
>
> b) O **contexto em que os dados pessoais foram recolhidos**, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
>
> c) A **natureza dos dados pessoais**, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9., ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.;
>
> d) As **eventuais consequências** do tratamento posterior pretendido para os titulares dos dados;

> e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a **anonimização**. (**GRIFOS NOSSOS)**

Cabe destacar que o art. 5, 1, b, fora de certa forma reproduzido na própria redação do art. 26 da LGPD, uma vez que estabelece a compatibilidade entre finalidades enquanto requisito essencial para o tratamento secundário de dados pessoais pelo Poder Público. Esse juízo de finalidade, adequação e necessidade deverá ser feito dentro dos parâmetros do caso concreto, conforme evidenciado nos dispositivos analisados. Essa perspectiva também se encontra englobada no art. 6, 4, a e b.

No que diz respeito ao art. 6, 4, c, é interessante notar que a natureza dos dados pessoais foi levada em consideração para a possibilidade de compartilhamento. Nesse sentido, cabe destacar que dados sensíveis dizem respeito a futuras informações que são potencialmente discriminatórias. Diante dessa conjuntura, os titulares adquirem direitos subjetivos em face dos controladores, sendo um grande exemplo dessa situação a possibilidade de revogação sem justificativa do consentimento para usufruto desses dados, na hipótese de essa ser a base legal que justifica o tratamento. Ademais, destaca-se que dados podem aparentar ser insignificantes, porém, a depender do tratamento realizado, podem tornar-se sensíveis (MENDES, 2014). Haja vista relativo consenso de que o tratamento de dados sensíveis provoca riscos maiores à personalidade individual, seria de extrema relevância a adoção desse critério enquanto limitação para o compartilhamento público-público.

Quanto a necessidade de levar em consideração as eventuais consequências do tratamento posterior, conforme descrito na alínea d do referido artigo 6, cabe destacar que no contexto brasileiro a LGPD foi a primeira legislação que previu o relatório de impacto, instrumento que possibilita a verificação da aderência das condutas do controlador à lei. Observa-se que na legislação europeia o *Data Protection Impact Assessment* (DPIA), que serviu de inspiração ao relatório de impacto, encontra-se diretamente ligado à noção de prevenção e mitigação de riscos aos titulares de dados (GOMES, 2019).

Nesse sentido, o risco pode ser entendido enquanto uma visão subjetiva na qual o controlador, a partir do conhecimento de eventos futuros, deverá tomar uma decisão de assumir ou não a possibilidade de sofrer eventual sanção (GOMES, 2019). Logo, entende-se que poderá a Autoridade Nacional de Proteção de Dados (ANPD) indicar modelos de relatórios de impactos, com o intuito de possibilitar que os entes da Administração Pública verifiquem as consequências de eventual tratamento secundário, podendo, dessa forma, mitigar e,

principalmente, prevenir eventuais riscos aos direitos dos titulares, em especial os direitos fundamentais previstos no art. 5º da Constituição Federal, a exemplo das liberdades civis.

Por fim, no que diz respeito à anonimização prevista no art. 6º, 4, e da GDPR, é necessário, antes de tudo, compreender a definição de dados pessoais. Assim, toda informação que possibilitar a identificação de uma pessoa natural, a exemplo de seu nome, endereço, endereço eletrônico, entre outros, será considerado um dado pessoal (FINKELSTEIN; FINKELSTEIN, 2019) que, eventualmente, a depender da forma com a qual for tratado, poderá gerar riscos a esse indivíduo (MENDES; MATTIUZZO; FUJIMOTO, 2021).

Dados "anonimizados", por outrora, ao não possibilitarem a identificação dos titulares, não encontram-se resguardados pelo escopo da LGPD. Essa anonimização advém da impossibilidade de rastrear os titulares, levando-se em consideração meios técnicos razoáveis e disponíveis em seu tratamento (FINKELSTEIN; FINKELSTEIN, 2019). Por óbvio existe uma evidente zona de penumbra que fora melhor desenvolvida pela pesquisadora Ana Júlia Prezotti no presente anuário. Porém, para os fins deste artigo, entende-se que a anonimização, sempre que possível, de dados compartilhados entre os entes do Poder Público poderá ser uma excelente baliza de limitação do poder estatal.

Levando-se em consideração todo o exposto, o presente artigo irá se dedicar no tópico seguinte à análise da MC-ADI 6.529/DF e das demais decisões - ADI 6529 MC-Ref, ADI 6387 MC-Ref. SL 1103 e MS 36150 MC -, a fim de compreender como a Suprema Corte brasileira vem se posicionando sobre o tema ora debatido. Por fim, serão feitas considerações sobre o posicionamento da CEDH no caso *Big Brother and Others vs. United Kingdom* com o propósito de demonstrar que eventual tratamento secundário deverá sofrer limitações, para que esse não proporcione a vigilância de cidadãos sob um falso pretexto.

2. Estudos de Caso

2.1. Síntese geral da MC-ADI 6.529/DF

Trata-se de Ação Direta de Inconstitucionalidade (ADI), com pedido de medida cautelar, proposta pelo Partido Socialista Brasileiro e pela Rede de Sustentabilidade, a fim de declarar parcialmente a inconstitucionalidade do §1º, art. 2º, parágrafo único, art. 4º e do art. 9º-A da Lei nº 9.883/1999:

> **Art. 2º. § 1º** O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.
>
> **Art. 4º** À ABIN, além do que lhe prescreve o artigo anterior, compete:
>
> **Parágrafo único**. Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.
>
> **Art. 9º A -** Quaisquer informações ou documentos sobre as atividades e assuntos de inteligência produzidos, em curso ou sob a custódia da ABIN somente poderão ser fornecidos, às autoridades que tenham competência legal para solicitá-los, pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, observado o respectivo grau de sigilo conferido com base na legislação em vigor, excluídos aqueles cujo sigilo seja imprescindível à segurança da sociedade e do Estado. (Vide Medida Provisória nº 2.123-30, de 2001) (Incluído pela Medida Provisória nº 2.216-37, de 2001)

Outrossim, a referida ADI pretende a declaração da inconstitucionalidade por arrastamento do art.1º, §3º, da Estrutura Regimental da Agência Brasileira de Inteligência (ABIN), aprovada pelo Decreto nº 10.445/2020. *Vide*:

> **Art. 1º** A Agência Brasileira de Inteligência - Abin, órgão integrante do Gabinete de Segurança Institucional da Presidência da República, criada pela Lei nº 9.883, de 7 de dezembro de 1999, é órgão central do Sistema Brasileiro de Inteligência e tem por competência planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas a política e as diretrizes estabelecidas em legislação específica.
>
> **§ 3º** Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à Abin, sempre que solicitados, nos termos do disposto no Decreto nº 4.376, de 13 de setembro de 2002, e na legislação correlata, para fins de integração, dados e conhecimentos específicos relacionados à defesa das instituições e dos interesses nacionais.

Em suma, intenta-se que o Sistema Brasileiro de Inteligência (Sisbin) apenas possa compartilhar dados pessoais à Agência Brasileira de Inteligência (Abin) quando for de interesse público, não sendo possibilitado o compartilhamento na hipótese de interesse privado/pessoal. Diante do referido pedido, a decisão majoritária usufruiu da técnica relativa à interpretação conforme à constituição, estabelecendo a necessidade de motivação do ato de solicitar os dados a serem compartilhados, para além da necessidade de instauração de procedimento formal, a

fim de que se possa sofrer eventual controle de legalidade pelo judiciário, ocorrendo, inclusive responsabilização nos casos de omissões, desvios e abusos (SUPREMO TRIBUNAL FEDERAL, 2020).

Ademais, foi firmado o entendimento de que existem hipóteses específicas as quais se reservam à jurisdição, sendo apenas possível com prévia análise e autorização judicial, como, por exemplo, as interceptações telefônicas. Por sua vez, a divergência compreendeu que estando a referida legislação em vigor há 21 anos, não haveria riscos em se aguardar a manifestação do Congresso Nacional, autoridade competente (SUPREMO TRIBUNAL FEDERAL, 2020). A Ementa da referida Medida Cautelar foi pronunciada nos seguintes termos:

> DIREITO CONSTITUCIONAL. AÇÃO DIRETA DE INCONSTITUCIONALIDADE. PARÁGRAFO ÚNICO DO ART. 4o DA LEI N. 9.883/99. INTERESSE PÚBLICO FORMALMENTE DEMONSTRADO COMO ÚNICO ELEMENTO LEGITIMADOR DO DESEMPENHO ADMINISTRATIVO. VEDAÇÃO AO ABUSO DE DIREITO E AO DESVIO DE FINALIDADE. OBRIGATORIEDADE DE MOTIVAÇÃO DO ATO ADMINISTRATIVO QUE SOLICITA DADOS DE INTELIGÊNCIA AOS ÓRGÃOS DO SISTEMA BRASILEIRO DE INTELIGÊNCIA. NECESSÁRIA OBSERVÂNCIA DA CLÁUSULA DE RESERVA DE JURISDIÇÃO. DEFERIMENTO PARCIAL DA MEDIDA CAUTELAR PARA DAR INTERPRETAÇÃO CONFORME AO PARÁGRAFO ÚNICO DO ART. 4o DA LEI N. 9.883/99.
>
> **1.** Para se concluir válido o texto legal e dar-se integral cumprimento ao comando normativo infralegal pelo Poder Executivo há de adotar-se como única interpretação e aplicação juridicamente legítima – como é óbvio – aquela que conforma a norma à Constituição da República. **É imprescindível vinculem-se os dados a serem fornecidos ao interesse público objetivamente comprovado e com motivação específica.**
>
> **2. Todo fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal.**
>
> **3. Práticas de atos à margem ou diversos do interesse público, especificado em cada categoria jurídica, devem ser afastadas pelo Poder Judiciário, quando comprovado o desvio de finalidade no cometimento.**
>
> **4.** A ausência de motivação expressa impede o exame da legitimidade de atos da Administração Pública, incluídos aqueles relativos às atividades de inteligência, pelo que a motivação é imprescindível.

> **5.** Mesmo nos casos de prática de atos motivados pelo interesse público, não é possível que os órgãos componentes do Sistema Brasileiro de Inteligência forneçam à ABIN dados que importem em quebra do sigilo telefônico ou de dados, por ser essa competência conferida ao Poder Judiciário, nos termos constitucionalmente previstos. **6.** Medida cautelar parcialmente deferida para dar interpretação conforme ao parágrafo único do art. 4o da Lei no 9.883/99 estabelecendo-se que: *a)* **os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade desses dados atenderem interesses pessoais ou privados**; *b)* toda e qualquer solicitação de dados deverá ser devidamente motivada para eventual controle de legalidade pelo Poder Judiciário; *c)* mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal, em razão daquela limitação, decorrente do necessário respeito aos direitos fundamentais; *d)* **nas hipóteses cabíveis de fornecimento de informações e dados à ABIN é imprescindível procedimento formalmente instaurado e a existência de sistemas eletrônico de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventual omissão desvio ou abuso. (GRIFOS NOSSOS)**

Com a devida vênia à divergência, compreende-se que a prevalência da decisão majoritária era necessária, pois, ainda que a legislação questionada tenha sido editada há 21 anos, inegável o avanço tecnológico durante esse período, sendo que o compartilhamento de dados atualmente poderá trazer inúmeras consequências que seriam inimagináveis durante a década de 90.

Haja vista o cenário apresentado, passar-se-á às considerações sobre o posicionamento do Supremo Tribunal Federal em decisões cujo teor diz respeito às limitações impostas ao compartilhamento público-público.

2.2. Tratamento de dados pessoais pelo Poder Público: princípios constitucionais aplicáveis e rejeição ao isolamento do interesse público

Inicialmente ressalta-se que a discussão jurídica travada nesta ADI assume contornos bem particulares em relação ao debate enfrentado pelo Supremo Tribunal Federal na análise da ADI 6.389 MC-Ref (Caso IBGE), acórdão paradigma no contexto da proteção de dados

pessoais. Isso se deve principalmente às complexidades que permeiam o tratamento de dados no âmbito do Poder Público.

Considerando o interesse público envolvido nas atividades de proteção de dados pessoais pela Administração e o próprio caráter compulsório do relacionamento entre os particulares e o Estado (BLACK; STEVENS, 2013), é possível aferir a essencialidade do tratamento de dados pessoais pelo Estado, a fim de que esse possa executar o que lhe fora constitucionalmente imposto (WIMMER, 2021-b). Ademais, conforme ressaltado pela autora Miriam Wimmer (2021-b), seria inimaginável, por exemplo, que os indivíduos possuíssem o direito subjetivo de requerer à Administração Pública a portabilidade de seus dados pessoais, exigindo sua eliminação.

A discussão sobre a privacidade nas relações com a Administração Estatal, todavia, não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. Como bem destacado por Gillian Black e Leslie Stevens (2013), se a privacidade fosse compreendida apenas enquanto um interesse particular do titular dos dados pessoais, sempre haveria a possibilidade do tratamento desses pela Administração Pública, uma vez que as finalidades públicas que o justificam sempre seriam consideradas necessárias e proporcionais.

Convém destacar que essa visão de compatibilização dos interesses da Administração Pública com a defesa de garantias individuais na temática da proteção de dados pessoais no Poder Público não é de todo estranha à jurisprudência do STF. Em pelo menos duas ocasiões o Tribunal impôs limitações a um modelo de fluxo multidirecional e irrestrito do compartilhamento de dados entre órgãos e instituições públicas.

Na primeira ocasião, tem-se a Suspensão de Liminar 1.103 MC, julgada monocraticamente pelo então Ministro Presidente - Min. Dias Toffoli - em 30 de maio de 2019. A referida decisão determinou que o IBGE se abstivesse de fornecer ao Ministério Público Federal dados reputados necessários à identificação de 45 (quarenta e cinco) crianças, na área urbana do município de Bauru/SP, desprovidas de registro de nascimento e, por conseguinte, da proteção do Estado e da sociedade.

Nessa decisão, destacou-se a necessidade de conciliação dos valores constitucionais em jogo ao pontuar que manter em sigilo as informações fornecidas é fundamental para que haja confiança nas pesquisas a serem efetuadas pelo IBGE. Observa-se, nesse sentido:

> "**O dever de sigilo proporciona segurança a quem presta as informações e contribui para a confiabilidade das pesquisas efetuadas. Recepção das normas que estabelecem o sigilo das informações colhidas pelo IBGE (art. 2º, § 2º, do Decreto-lei n. 16111967 e parágrafo único, do art. 1–, da Lei no 5.534/1968) pela Constituição Federal de 1988**. IV. Quando princípios fundamentais da Constituição conflitam entre si, a questão deve ser analisada tendo em vista o caso concreto, respeitados os valores supremos consagrados na ordem constitucional. Com base no juízo de ponderação, busca-se identificar em qual dimensão deve um direito fundamental preponderar quando contraposto a outro direito também fundamental. Para isso, deve-se recorrer aos princípios instrumentais da razoabilidade e da proporcionalidade, implícitos na Constituição, e sopesar os valores protegidos pelas normas em conflito. Não se trata de eliminar um direito para fazer predominar exclusivamente outro, mas sim de conciliar os bens jurídicos em conflito e harmonizá-los com os princípios consagrados no sistema jurídico constitucional". (SSL 1.103 MC, Rel. Min. Cármen Lúcia, julgado em 5.2.2017, DJe 8.5.2017).

Na segunda ocasião, cumpre citar ainda a Medida Cautelar nos autos do Mandado de Segurança 36.150. Diante das circunstâncias do caso concreto, o Relator deferiu a cautelar para cassar determinação do Tribunal de Contas da União (TCU), que ordenara ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família.

Destaca-se que, nessa decisão, apontou-se o risco de o tratamento dos dados compartilhados pelo INEP ser submetido a uma finalidade diversa daquela originalmente declarada no ato da coleta, uma vez que ocorreria a subversão da autorização que possibilitou a coleta desses. Desse modo, dialoga profundamente com a noção do princípio da finalidade ao compreender que eventual tratamento secundário que desvirtue a autorização inicialmente concedida viola o dever de sigilo e, para além, fere a própria intimidade do titular. Nesse sentido:

> "7. É certo que o art. 71, IV, da Constituição confiou ao TCU a competência para a realização de inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial nos órgãos e entidades da Administração. A atribuição dessa competência, por óbvio, supõe o reconhecimento dos meios necessários ao cumprimento desse encargo. Isso inclui a prerrogativa de requerer aos responsáveis pelos órgãos e entidades as informações necessárias à instrução de processos de auditoria e inspeção. No caso, no entanto, as informações que se quer acessar foram prestadas para uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo do INEP quanto às informações pessoais. 8. **Nesse aspecto, a transmissão**

> **a outro órgão do Estado dessas informações e para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade**. De igual modo, é plausível a alegação de que a franquia desses dados quebra a confiança no órgão responsável pela pesquisa por violação do sigilo estatístico. Há, pois, risco à própria continuidade das atividades desempenhadas pelo INEP, com efetivo prejuízo ao monitoramento das políticas públicas de educação". (MS 36.150 MC, Rel. Min. Roberto Barroso, julgado em 10.12.2018, DJe 13.12.2018, grifo nosso)

Assim, fica evidente que o Supremo Tribunal Federal está a ponderar os valores constitucionais da eficiência da Administração Pública com o regime constitucional de proteção aos direitos individuais, notadamente com a garantia de autodeterminação informativa espalhada no art. 5º, *caput* e incisos X, e LXXII, da Constituição Federal.

A postura de limitar o poder governamental no compartilhamento de dados pessoais de seus cidadãos, por outro lado, não foi igualmente observada pela CDHU, originando verdadeiro cenário de vigilância que se pretende evitar, conforme será demonstrado a seguir.

2.3. Da decisão da Corte Europeia de Direitos Humanos no caso Big Brother Watch *and Others vs. The United Kingdom: o que se pretende evitar*

Voltando à introdução do presente artigo, o leitor atento percebeu que a expressão "a fim de que vida não VOLTE a copiar a arte" foi utilizada ao versar sobre o Big Brother enquanto referência cultural. Isso porque, diversos movimentos de espionagem e vigilância muito semelhantes a esse ocorreram e são de conhecimento geral.

Nesse cenário, cita-se o denominado Sistema de Vigilância Global "Echelon", que diz respeito a um sistema de espionagem que captura informações e comunicações efetuadas pelos mais diversos meios, a exemplo da fibra óptica e da internet. Desenvolvido no contexto da 2ª Guerra mundial, seu principal objetivo em 1940 era o de espionar militares, porém, na década de 1960 passou a possibilitar a espionagem comercial e industrial e em 1990 foi utilizado enquanto meio de combate ao terrorismo e tráfico de drogas (OLIVEIRA; PESSOA, 2019). Para além, um caso de conhecimento mundial que é referência quando se trata de vigilância governamental foi a denúncia efetuada por Edward Snowden, que expôs o tratamento abusivo

de dados e verdadeira espionagem efetuada pelo governo estadunidense (GREENWALD, 2014).

Compreendendo, por conseguinte, que a vigilância não representa uma temática nova, analisar-se-á o caso paradigma europeu relativo ao *Big Brother Watch and Others vs. The United Kingdom* que fora julgado definitivamente em 25 de maio de 2021, apresentando, também, deliberações privadas entre 11 de julho de 2019, 4 e 6 de setembro de 2019 e 17 de fevereiro de 2021 (GRAND CHAMBER, 2021). Relativo ao primeiro julgamento em massa após o caso Snowden, foi resultado do questionamento das organizações não governamentais *Big Brother Watch, English PEN* e *Open Rights Group* perante a Corte Europeia de Direitos Humanos (CEDH) acerca do regime jurídico de vigilância resguardado sobre o *Regulation of Investigatory Powers*. Argumentou-se, nesse sentido, que a conduta de vigilância em massa do Governo inglês feriria o artigo 8º e 10º da Convenção Europeia de Direitos Humanos (SHARMA, 2018).

A partir da pequena introdução do caso apresentado, já é possível compreender que dele emanam nuances não abordadas no presente artigo a exemplo da interceptação em massa, que fora considerada possível pela CEDH, desde que autorizada por um órgão independente do executivo, o que não ocorrera no caso concreto (ZALNIERIUTE, 2021). No entanto, ele se mostra um excelente paradigma para demonstrar aquilo que o presente artigo visa evitar a partir de limitações à possibilidade de compartilhamento de dados, isto é, um cenário de vigilância e desconfiança da população para com o seu governo.

Ademais, verifica-se ponto de grande valia à discussão relativa aos limites ao compartilhamento de dados entre os entes estatais para que se evite um cenário de vigilância, uma vez que a CEDH entendeu pela possibilidade de compartilhamento de informações (dados pessoais) entre as autoridades do Reino Unido e o serviço de inteligência estadunidense, desde que presentes medidas contra eventuais abusos, para além de sujeição a revisão posterior (ZALNIERIUTE, 2021). Nesse cenário, a Corte Europeia compreendeu que a legislação interna seria clara sobre a possibilidade de intercâmbio de informações entre as agências de inteligência dos Estados Unidos e do Reino Unido, sendo recomendado que o material fosse apenas analisado e investigado caso todas as exigências para uma interceptação nacional fossem supridas. Em outros termos, os dados compartilhados apenas deveriam sofrer eventual tratamento se houvesse autorização e existisse um cenário que exigisse essa intervenção (OLIVEIRA; PESSOA, 2019).

No Brasil, a hipótese de interceptação em massa não seria viável, pois não há legislação que autorize essa conduta. Entretanto, o que mais chama atenção na situação retratada foi se considerar possível e não afrontoso aos direitos humanos a possibilidade de compartilhamento de dados pessoais entre os governos em questão, desde que só fosse realizado um tratamento posterior caso houvesse um cenário propício para tanto.

Essa visão não poderia ser importada para o cenário brasileiro, pois conforme fora amplamente desenvolvido nos tópicos anteriores, o tratamento secundário que justifica o compartilhamento de dados não poderá subverter o tratamento inicial que possibilitou a coleta desses. Essas limitações demonstram-se imprescindíveis em qualquer contexto, pois o Estado, seja qual for, sempre deverá garantir a segurança de seus cidadãos e um cenário de vigilância igual o retratado nunca será a solução.

Considerações Finais

Ante todo o exposto, é possível afirmar que o tratamento de dados pessoais é extremamente relevante para o desempenho estatal, sendo o compartilhamento desses essencial para a dinâmica governamental. No entanto, a relação verticalizada entre Estado e cidadão torna imprescindível a adoção de limites a eventual compartilhamento público-público, para que não ocorra um cenário de vigilância tal qual o denunciado por Edward Snowden e questionado em juízo europeu pela organização não governamental *Big Brother* e outros.

Dessa maneira, a LGPD em seu artigo 26 traz a finalidade específica do tratamento secundário a ser realizado enquanto importantíssima baliza a referida limitação. Contudo, também ficou evidente que a experiência internacional pode ser de grande valia ao tema. Nesse sentido, os art. 6, 4, c, d, e da GDPR demonstram que a natureza dos dados que serão compartilhados, eventuais consequências que o tratamento secundário poderá trazer ao particular e a anonimização dessas informações também poderão influenciar na possibilidade do compartilhamento pretendido.

Por fim, a análise das decisões do Supremo Tribunal Federal - em específico: ADI 6529 MC-Ref, ADI 6387 MC-Ref, SL 1103 e MS 36150 MC - ainda possibilitou a conclusão de que a corte brasileira tende a ponderar a eficiência da Administração Pública em relação a proteção dos direitos individuais dos indivíduos, de modo a não prevalecer a supremacia do interesse

público no que diz respeito ao tratamento de dados pessoais. Pode-se, assim, concluir que a possibilidade de compartilhamento de dados entre os entes que compõem o Poder Público dependerá da análise concreta da situação, devendo-se levar em consideração as limitações acima descritas, para além dos princípios constitucionais da proporcionalidade e razoabilidade.

Referências bibliográficas

ARIENTE, Eduardo Altomare; SANTOS, Alessandro Santiago; PALHARES, Gabriela Capobianco; GOMES, Jefferson de Oliveira. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. *Estudos avançados* 34 (99), 2020.

BLACK, Gillian e STEVENS, Leslie. Enhancing Data Protection And Data Processing In The Public Sector: The Critical Role Of Proportionality And The Public Interest. *Scripted*. Vol. 10, n. 1, 2013, p. 95

BRASIL. *Lei Geral de Proteção de Dados Pessoais* (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. ADI 6529 MC-Ref, Relator(a): CÁRMEN LÚCIA, Tribunal Pleno, julgado em 11/10/2021, processo eletrônico DJe-210. Divulgado em 21-10-202. Publicado em 22-10-2021. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur454781/false>. Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, Processo Eletrônico DJe-270 Divulgado 11-11-2020 Publicado 12-11-2020. Disponível em:<https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false>.Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. SL 1103. Relator: Min. Presidente. Decisão proferida pelo Min. DIAS TOFFOLI. Julgamento: 30/05/2019. Publicação: 04/06/2019. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/despacho986145/false>.Acesso em: 12 de novembro de 2021.

BRASIL. Supremo Tribunal Federal. MS 36150 MC. Relator: Min. Roberto Barroso. Julgamento: 10/12/2018. Publicação: 13/12/2018. Disponível em: < https://jurisprudencia.stf.jus.br/pages/search/despacho937080/false>. Acesso em: 12 de novembro de 2021.

CELLA, J. R. G.; COPETTI, R. Compartilhamento de Dados Pessoais e a Administração Pública Brasileira. *Revista de Direito, Governança e Novas Tecnologias*, Maranhão, v. 3, p. 39-58, jul./dez. 2017.

FINKELSTEIN, Cláudio; FINKELSTEIN, Maria Eugênia. Privacidade e Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Brasileira*. Florianópolis, SC. v. 23 | n. 9. p. 284-301. Mai./ago. 2019

GENERAL DATA PROTECTION REGULATION. Disponível em: <https://gdpr.algolia.com>. Acesso em: 12 de novembro de 2021.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados: uma breve análise da sua definição e papel na LGPD. *Revista do Advogado*, São Paulo, n. 144, nov. 2019.

GRAND CHAMBER. *Case of Big Brother Watch and Others v. United Kingdom.* STRASBOURG, 2021. Disponível em: <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}> . Acesso em 12 de novembro de 2021.

GREENWALD, Gleen. S*em lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo americano*. Rio de Janeiro: Sextante, 2014

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, Carlos Affonso (coord.); MAGRANI, Eduardo (coord.); SILVA, Priscilla (coord.). *Tratado de Proteção de Dados Pessoais.* Rio de Janeiro: Forense, 2021

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, cap. 1

MENDES, Laura Schertel; MACHADO, Diego; GASIOLA, Gustavo Gil. A Administração Pública entre transparência e proteção de dados. *Revista de Direito do Consumidor. vol*. 135/2021. p. 179 - 201. Maio - Junho, 2021.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz(coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

OLIVEIRA, Rafael dos Santos. PESSOA, João Pedro Seefeldt. Big Brother Watch and Others v. The United Kingdom": el régimen de vigilancia social y el derecho al respecto a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos. *Pensar: revista de ciências jurídicas.* Fortaleza, v. 24, n. 3, p. 1-12, jul./set. 2019.

SHARMA, Chinmayi. Summary: Big Brother Watch and Others v. The United Kingdom. *Lawfareblog*, 2018. Disponível em:<https://www.lawfareblog.com/summary-big-brother-watch-and-others-v-united-kingdom> Acesso em: 12 de novembro de 2021.

SUPREMO TRIBUNAL FEDERAL. STF impõe limites ao compartilhamento de dados do Sistema Brasileiro de inteligência (Sisbin). *Portal STF*, 2020. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449549&ori=1>. Acesso em: 12 de novembro de 2021.

WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no Poder Público: lições da Pandemia. *Revista Brasileira de Políticas Públicas*. Uniceub, volume 11, nº 1. Brasília, abril de 2021 a.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz(coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais.* Rio de Janeiro: Forense, 2021b.

ZALNIERIUTE, Monika. Procedural Fetishism and Mass Surveillance under the ECHR. *Verfassungsblog on Matters Constitucional*, 2021. Disponível em: <https://verfassungsblog.de/big-b-v-uk/>. Acesso em: 12 de novembro de 2021.


OBSERVATÓRIO DA
LGPD
UNIVERSIDADE DE BRASÍLIA