

# O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO E O PAPEL DOS TRIBUNAIS DE CONTAS

## *THE PROCESSING OF PERSONAL DATA BY PUBLIC AUTHORITIES AND THE ROLE OF AUDIT COURTS*

Arnaldo Bastos Santos Neto<sup>I</sup>

Lauro Ishikawa<sup>II</sup>

Moises Maciel<sup>III</sup>

<sup>I</sup> Universidade Federal de Goiás, Goiânia, GO, Brasil. Doutor em Direito Público. E-mail: [arnaldobsneto@yahoo.com.br](mailto:arnaldobsneto@yahoo.com.br)

<sup>II</sup> Faculdade Autônoma de Direito – FADISP, São Paulo, SP. Brasil. Doutor em Direito das Relações Sociais. E-mail: [lauro.ishikawa@unialfa.com.br](mailto:lauro.ishikawa@unialfa.com.br)

<sup>III</sup> Faculdade Autônoma de Direito – FADISP, São Paulo, SP. Brasil. E-mail: [arnaldobsneto@yahoo.com.br](mailto:arnaldobsneto@yahoo.com.br)

**Resumo:** O presente artigo, pelo método dedutivo, com investigação analítica e bibliográfica em legislações e doutrinas brasileiras e estrangeiras sobre o tema, analisa o papel dos Tribunais de Contas no que diz respeito à lei de proteção de dados brasileira. Coteja, além da sua necessidade de adequação às exigências legais, sua responsabilidade, como órgãos técnicos do Controle Externo, em relação ao dever de agir em prol de sua fiscalização e consoante sua relevante função pedagógica. Para tanto, primeiramente investiga o tratamento de dados pessoais pelo Poder Público conforme a Lei Geral de Proteção de Dados, realizando paralelo com o Regulamento Geral da União Europeia e dispendo dita proteção como um direito fundamental, inserido no seu tratamento pela Administração Pública brasileira. Em seguida, adentra mais substancialmente no papel do Tribunal de Contas sobre a proteção de dados, cotejando em específico sua função fiscalizadora e sua competência pedagógica, concluindo pelo necessário cumprimento dos enunciados normativos conforme a melhor sistemática procedimental e material a fim de que as Cortes de Contas possam realizar com a maior eficácia a proteção legalmente estabelecida.

**Palavras-chave:** Tribunal de Contas. Lei Geral de Proteção de Dados. Fiscalização.

**Abstract:** The present article, by the deductive method, with analytical and bibliographical research in Brazilian and foreign legislations and doctrines on the theme, analyzes the role of the Audit Courts with respect to the Brazilian data protection law. In addition to their need to adapt to the legal requirements, it examines their responsibility, as technical organs of External Control, in relation to the duty to act in favor of their inspection and according to their relevant

DOI: <http://dx.doi.org/10.20912/rdc.v16i40.604>

Recebido em: 24/08/2021

Aceito em: 28/11/2021



pedagogical function. For this purpose, it first investigates the treatment of personal data by the Public Authorities according to the General Law of Data Protection, making a parallel with the General Regulation of the European Union and disposing this protection as a fundamental right, inserted in its treatment by the Brazilian Public Administration. Then, it enters more substantially into the role of the Court of Auditors regarding data protection, comparing in specific its supervisory function and its pedagogical competence, concluding by the necessary compliance with the normative enunciates according to the best procedural and material system in order for the Courts of Auditors to carry out with the greatest effectiveness the protection legally established.

**Keywords:** Court of Auditors; General Law of Data Protection. Supervision.

## 1 Introdução

Na esteira dos demais países, mormente os pertencentes à União Europeia, o Brasil publicou a sua Lei Geral de Proteção de Dados Pessoais, a lei nº 13.709 de 2018, cuja vigência teve início em setembro de 2020, de maneira parcial, sem sanções administrativas, essas as quais, só a partir de agosto de 2021, passaram a ter aplicabilidade.

O questionamento que aqui é objeto de análise é acerca da eficácia da implementação da LGPD no setor público e em especial o papel dos Tribunais de Contas em sua efetivação.

Assim, diante da necessidade de um recorte contextual mais restrito, foca-se nesses Tribunais, a fim de analisar sua adequação diante da LGPD e identificar sua responsabilidade também sobre a fiscalização e na orientação aos demais órgãos da administração pública.

Para tanto, aborda-se a respeito da aplicabilidade das regras sobre proteção de dados para o poder público, fazendo um breve *benchmarking* sobre a ótica da legislação que foi referência à norma brasileira: o Regulamento Geral da União Europeia (RGPD 2016/679-UE).

Em seguida volta-se a atenção para a análise da proteção de dados como um direito fundamental, em consonância com o papel jurídico da Administração Pública.

Enfim, trata-se da adequação e do papel que os Tribunais de Contas devem assumir no que se refere à LGPD.

Nesse sentido, utiliza-se o método dedutivo, com investigação analítica e bibliográfica em legislações e doutrinas brasileiras e estrangeiras sobre o tema.

## 2 O tratamento de dados pessoais pelo Poder Público conforme a LGPD

Com forte inspiração europeia, a normativa de proteção de dados brasileira consiste na regulamentação do tratamento de dados pessoais por qualquer pessoa física e jurídica, de direito privado e de direito público, abrangendo, então, os agentes privados e a Administração Pública direta e indireta.

Com o enfoque no reconhecimento da relevância do tratamento do uso de dados pelo Poder Público, a Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018) separou um capítulo exclusivamente para regulamentar o tratamento de dados pessoais por dita instituição, o capítulo IV, que, dividido em duas seções, trata das regras e das suas responsabilidades sobre o tema.

### *2.1 O Regulamento Geral da União Europeia: benchmarking internacional*

Fonte de inspiração da LGPD é o Regulamento Geral da União Europeia (RGPD). Antes desse regulamento, em 1995 a UE já contava com a Diretiva nº 95/46/CE, que regulamentava a proteção dos dados das pessoas físicas.

Mais à frente, em 2001, surgiu o Regulamento nº 45, que veio regulamentar o tratamento de dados pessoais pela Administração Pública, sendo substituído, na sequência, pelo Regulamento nº 1725/2018.

Ainda em 2018, a Diretiva 95/46/CE foi revogada pelo RGPD, que passou a ser a norma geral em vigor em toda a União Europeia, com reflexos de impacto em nações fora da EU, inclusive no próprio Brasil.

Consoante o disposto no texto do RGPD, os dados pessoais só poderão ser tratados para fins determinados e previamente especificados, necessitando do consentimento dos titulares, exceto em casos de arquivo público, pesquisas histórico-científicas ou em questões de estatística.

A legislação europeia demanda transparência no tratamento dos dados para permitir, aos seus titulares, o acesso, a identificação, a correção e até mesmo a solicitação de exclusão dos dados da base de tratamento.

O tratamento de dados pessoais pelo poder público, na União Europeia, contudo, ainda necessitava de uma regulamentação mais específica, que surgiu com o Regulamento nº 1725 de 2018, regulamento esse que, por não revogar a RGPD, tem necessária interpretação conjunta e sistemática.

Importante salientar que o Regulamento nº 1725 determina, tal qual dispõe o RGPD, que o tratamento de dados pessoais deve seguir a finalidade informada no momento da sua coleta. Todavia, prevê que nos casos em que o tratamento se fizer necessário para fins de interesse público, ou mesmo para o exercício da autoridade pública, será permitida a definição, *a posteriori*, das tarefas e fins para as quais este tratamento será válido, sempre respeitando o direito de oposição por parte do titular.

Neste sentido, o considerando nº 25 do Regulamento nº 1725 de 2018:

(25) [...] A fim de apurar se a finalidade de um tratamento posterior é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos de licitude do tratamento inicial, deverá ter em atenção, nomeadamente: a existência de uma ligação entre tais finalidades e a finalidade do tratamento posterior previsto; o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, com base na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências do tratamento posterior previsto para

os titulares dos dados; e a existência de garantias adequadas tanto nas operações de tratamento iniciais como nas operações de tratamento posteriores previstas<sup>1</sup>.

Relativamente ao tratamento de dados, especificamente pelos Tribunais de Contas portugueses, citamos, aqui, a Resolução baixada por este órgão (Resolução nº 3/2018), que determina, dentre outras coisas:

Tendo em vista garantir que os atos do Tribunal que serão publicados não contêm informações pessoais que vão para além do necessário, atendendo ao interesse público prosseguido com a respectiva publicação, e em conformidade com o disposto no artigo 13º do Regulamento do Tribunal de Contas, deverá observar-se o seguinte procedimento:

a) A publicação de acórdãos, sentenças, relatórios de auditoria e outros atos do Tribunal, bem como de atos do Ministério Público neles integrados apenas deve conter os dados pessoais indispensáveis à informação da sociedade sobre a utilização dos recursos financeiros públicos e à garantia da *accountability* dos gestores desses recursos e dos responsáveis financeiros;

b) Ponderando-se o interesse público prosseguido com o direito de proteção de dados pessoais, considera-se legítima, adequada, necessária e proporcional, a explicitação, na publicação dos atos do Tribunal mencionados na alínea anterior, do nome e cargo das pessoas em causa desde que sujeitos à jurisdição do Tribunal, devendo ser omitidos outros dados pessoais, salvo quando se demonstre que estes têm relevo público;

c) Deverá, no entanto, ser ponderada a eventual desnecessidade de referências na publicitação dos atos do Tribunal a empresas ou outros sujeitos privados, singulares ou coletivos, de relações jurídicas com entidades públicas sujeitas à jurisdição do Tribunal e que não tenham qualquer responsabilidade pela gestão ou pela utilização de dinheiro ou ativos públicos;

d) É da responsabilidade do Juiz Conselheiro relator identificar os dados pessoais que devam ser omitidos;

e) Em caso de dúvida sobre os dados pessoais que podem constar na publicação dos dados mencionados atos do Tribunal, deve ser consultado o *Encarregado de Proteção de Dados* do Tribunal. (sic)<sup>2</sup>

Logo após, a Resolução supracitada menciona a nomeação do Encarregado de Dados, em conformidade ao disposto no RGPD, determinando, inclusive, que “o Encarregado de Proteção de Dados reporta ao Plenário Geral do Tribunal (art. 38º, nº 3, do RGPD)” e que poderá, este Encarregado, exercer outras funções e atribuições desde que não exista conflito de interesses.

Em seguida, especifica a missão e as funções do Encarregado, finalizando com a nomeação do seu Encarregado e com a determinação de que este apresente, ao Plenário Geral, até 30 de maio de cada ano, um relatório de suas atividades no ano anterior.

1 UNIÃO EUROPEIA. *Regulamento (UE) 2018/1725*. Considerando nº 25. 2018. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725> Acesso em 17 nov. 2021.

2 PORTUGAL. *Resolução 3/2018 – PG*. do Tribunal de Contas. 2018. Disponível em <https://www.tcontas.pt/pt-pt/NormasOrientacoes/Resolucoes/Documents/2018/res003-2018-pg.pdf>. Acesso em 17 nov. 2021.

## 2.2 O Direito Fundamental à proteção de dados

Como já referido, cabe dizer que o berço da proteção de dados encontra-se na Europa. O Conselho Nacional de Proteção de Dados, de Portugal, por exemplo, possui 25 anos de existência, e a Constituição Portuguesa já previa a proteção de dados como direito fundamental desde 1976<sup>3</sup>. Trata-se de uma cultura disseminada e já sedimentada há muitas décadas. A temática da proteção de dados vem sendo discutida no âmbito global há mais de quarenta anos.

O sistema digital complexo que é parte da contemporaneidade em âmbito mundial permite o que se pode chamar de trilhas digitais, que vêm sendo imensamente exploradas pelas instituições para tomada de decisões, e isso graças ao avanço digital da inteligência artificial e de conexões em rede de algoritmos, os quais permitem que sejam traçados perfis a respeito dos interesses pessoais para toda espécie de finalidade possíveis, levando necessariamente ao questionamento sobre os limites e a vulnerabilidade do direito à privacidade.

Diante dessa preocupação, a Lei Geral de Proteção de Dados brasileira, em seu art. 17, decretou que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta lei”<sup>4</sup>.

Laura Schertel ensina, neste sentido, que:

A tutela jurídica para a proteção de dados da personalidade em face do tratamento de dados pessoais envolve o estabelecimento de uma série de procedimentos, princípios e direitos, que limitam o processamento de dados pessoais ao mesmo tempo que empoderam o cidadão para controlar o fluxo de seus dados<sup>5</sup>.

A autora mencionada explica que a maior preocupação no que concerne à proteção dos dados pessoais não consiste em proteger os dados propriamente falando, mas as informações dele decorrentes, que poderão impactar no direito à privacidade e à intimidade do seu titular. Na esteira desse raciocínio, vale salientar que o direito fundamental à proteção dos dados pessoais não é um direito absoluto, devendo, como bem já dito sobre os enunciados da RGPD da União Europeia, estarem conciliados com a necessidade de realização das funções da própria Administração Pública, tais como o controle, a auditoria e a investigação, por exemplo, que, por sua vez, precisarão ser exercitados com total respeito à pessoa do titular, além da observância do sigilo necessário.

## 2.3 O direito fundamental à proteção de dados e o tratamento pela Administração Pública brasileira

Considerando todo o exposto e trazendo esse raciocínio para a legislação nacional, apesar de reconhecidamente ter sofrido forte influência da legislação europeia, a lei de proteção de dados brasileira, por ocasião dos vetos sofridos, acabou aprovada com algumas lacunas, principalmente no que concerne ao tratamento de dados pelo poder público, que necessitam ser preenchidas.

3 SILVEIRA, Luís Novais Lingnau da. O Direito à proteção de dados pessoais. *Comissão Nacional de Protecção de Dados*. Disponível em [https://apdsi.pt/wp-content/uploads/prev/2.11\\_luis%20silveira\\_070626.pdf](https://apdsi.pt/wp-content/uploads/prev/2.11_luis%20silveira_070626.pdf) Acesso em 17 de nov. 2021.

4 BRASIL. Lei nº 13.709/2018 – LGPD. Disponível em [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em 17 nov. 2021.

5 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, p. 189.

Para tanto, citamos como exemplo, o veto dos arts. 23 e 28, que culminou na aprovação da lei sem maiores considerações acerca do compartilhamento de dados pessoais pelo Poder Público.

O art. 23 determinava que:

II - sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado;

E as razões do veto foram assim expressadas:

O dispositivo veda o compartilhamento de dados pessoais no âmbito do Poder Público e com pessoas jurídicas de direito privado. Ocorre que o compartilhamento de informações relacionadas à pessoa natural identificada ou identificável é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas. É o caso, por exemplo, do banco de dados da Previdência Social e do Cadastro Nacional de Informações Sociais, cujas informações são utilizadas para o reconhecimento do direito de seus beneficiários e alimentados a partir do compartilhamento de diversas bases de dados administrados por outros órgãos públicos. Ademais, algumas atividades afetas ao poder de polícia administrativa poderiam ser inviabilizadas, a exemplo de investigações no âmbito do Sistema Financeiro Nacional, dentre outras<sup>6</sup>.

Já quanto ao art. 28, seu texto expressava que: “a comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I, do *caput* do art. 23 desta Lei”. E as razões do veto se deram em virtude de que

A publicidade irrestrita da comunicação ou do uso compartilhado de dados pessoais entre órgãos e entidades de direito público, imposta pelo dispositivo, pode tornar inviável o exercício regular de algumas ações públicas como as de fiscalização, controle e polícia administrativa<sup>7</sup>.

Na busca por suprimir as lacunas deixadas pelos vetos supramencionados, foi publicado o Decreto nº 10.046 de 2019, que dispõe sobre a governança no compartilhamento de dados por parte da administração pública, além de instituir o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

É sabido que o tratamento de dados pessoais pela Administração Pública, consoante o disposto na LGPD, independe do consentimento do titular quando for realizado para cumprir uma obrigação legal ou para a realização de políticas pública, inobstante, precisará se atentar à finalidade pública e ao interesse público. Neste sentido manifestou-se o Ministério Público Federal:

De outro lado, o tratamento de dados pessoais por entes públicos deve ser sempre atrelado ao atendimento de sua finalidade pública e à persecução do interesse público, devendo haver ainda a explicitação das hipóteses em que realizam o referido tratamento – com especificação dos procedimentos e práticas usados. Além disso, o uso compartilhado de

6 BRASIL. Câmara dos Deputados. Lei nº 13.709, de 14 de agosto de 2018 – Veto. Disponível em <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html>. Acesso em 07 set. 2021.

7 BRASIL. Câmara dos Deputados. Lei nº 13.709, de 14 de agosto de 2018 – Veto. Disponível em <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html>. Acesso em 07 set. 2021.

dados pessoais pelo Poder Público deve sempre respeitar os princípios da proteção de dados pessoais, especificados no art. 6º da LGPD.<sup>8</sup>

Reforçando o disposto acima, é importante lembrar de outros dois princípios previstos na LGPD: o *privacy by design* e o *privacy by default*, segundo os quais as instituições, sejam elas privadas ou públicas, precisam adotar as medidas de segurança necessárias para a proteção dos dados coletados e armazenados, bem como observar todas as medidas técnicas e administrativas, no mesmo sentido, desde o momento em que se inicia o tratamento até a sua execução final, tratando-se de uma boa prática que persiste e permanece, durante a realização de todo o procedimento.

Com o intuito de esclarecer essa necessidade, a LGPD trouxe, expressa, a indispensabilidade de um programa de governança em privacidade com vistas a evidenciar algumas regras de boas práticas que devem ser observadas por todos os que tratam dados pessoais, tomando por base não apenas a natureza do tratamento como, ainda, seus objetivos e fins, bem como a probabilidade e a gravidade dos riscos, devidamente sopesados com base nos benefícios a serem auferidos.

Recomenda, ainda, o texto legal, que os dados tratados pelo Poder Público sejam mantidos em formato interoperável e estruturado, de modo a facilitar o seu compartilhamento nos casos de execução de políticas públicas ou de prestação de serviços públicos em geral, além de garantir o acesso às informações pela sociedade.

Importa, ainda, não olvidar que, qualquer compartilhamento realizado pela Administração Pública, no exercício de suas funções, deverá se dar, exclusivamente, para a finalidade específica de execução de políticas públicas e mediante a observância dos princípios legais, dentre eles ressaltamos o princípio da transparência que, consoante o art. 6º, VI da LGPD consiste em “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”.<sup>9</sup>

No que consiste a esse compartilhamento, referido art. foi objeto de veto presidencial mediante a justificativa de que a publicidade irrestrita do uso compartilhado de dados entre os órgãos do poder público poderia inviabilizar o exercício regular de determinadas ações como, por exemplo, a fiscalização, o controle e a polícia administrativa.

No intuito de suprir essa ausência, ocasionada pelo veto presidencial ao art. 28 do Projeto da LGPD, o Decreto nº 10.046 de 2019 veio regulamentar o compartilhamento de dados pessoais pelo poder público. Referido decreto estipula, quanto ao compartilhamento de dados pelos órgãos da administração pública, algumas diretrizes:

Art. 3º. [...]

8 BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão 3. *Roteiro de Atuação*. Sistema Brasileiro de Proteção e Acesso a Dados Pessoais. Análise de dispositivos à lei de acesso à informação, da lei de identificação civil, da lei do marco civil da internet e da lei nacional de proteção de dados. v. 3. Brasília: MPE, 2019, p. 25. Disponível em <http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3> Acesso em 17 de nov. 2021.

9 BRASIL. Lei nº 13.709/2018 – LGPD. Disponível em [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em 17 nov. 2021.

I - 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 Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;

II - o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo recebedor de dados, dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados;

III - os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades de que trata o art. 1º, para facilitar a execução de políticas públicas orientadas por dados;

IV - os órgãos e entidades de que trata o art. 1º colaborarão para a redução dos custos de acesso a dados no âmbito da administração pública, inclusive, mediante o reaproveitamento de recursos de infraestrutura por múltiplos órgãos e entidades;

V - nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação; e

VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018<sup>10</sup>.

Traz, assim, um texto extremamente similar ao vetado art. 28, determinando que o compartilhamento dos dados pelo poder público deverá observar o disposto no art. 23 (já alterado) da LGPD e, desta forma, estabelecendo a necessidade de informações “claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas”<sup>11</sup> que forem adotadas no tratamento dos dados, de modo a assegurar a tão necessária transparência.

O legislador partiu do pressuposto, para tanto, de que dados públicos não possuem quaisquer restrições de acesso e, deste modo, sua divulgação deve ser assegurada a qualquer interessado, razão pela qual entram na categoria de compartilhamento amplo, enquanto as demais categorias de compartilhamento (restrito e específico) estariam resguardados a dados protegidos por sigilo sendo que, no compartilhamento restrito, o acesso a órgãos e demais entidades da administração pública federal deverá exigir a execução de políticas públicas e o compartilhamento, propriamente falando, deverá ter suas regras traçadas pelo Comitê Central de Governança de Dados, de maneira simplificada. No segundo caso (compartilhamento específico), o compartilhamento deverá exigir hipóteses e finalidades expressamente previstas na lei.

A dúvida que sobressai, aqui, com relação ao disposto no Decreto, se dá quanto ao Comitê Central de Governança de Dados, cuja composição, segundo o próprio Decreto, consistiria em representantes indicados pelo Poder Executivo. Qual seria o seu vínculo com a ANPD? Haveria uma hierarquia entre eles? O Comitê estaria sujeito ao disposto à ANPD? Não haveria, neste caso, uma espécie de sobreposição de suas atribuições que, por sua vez, poderia ensejar litígios que sobrecarregariam, consideravelmente, o judiciário?

10 BRASIL. Decreto nº 10.046 de 2019. Disponível em [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/decreto/D10046.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm). Acesso em 17 de nov. 2021.

11 BRASIL. Lei nº 13.709/2018 – LGPD. Disponível em [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em 17 nov. 2021.

Criado, assim, para suprir uma lacuna quanto a observância da transparência, como direito dos titulares e da sociedade como um todo, o Decreto acabou mais por confundir e restringir, até mesmo, a publicidade inerente aos atos administrativos em geral.

No concernente ao compartilhamento de dados pelo Poder Público, importa tecer algumas considerações no tocante a decisão proferida pelo Supremo Tribunal Federal, na ADI nº 6529, que deferiu, por maioria, parte do solicitado em medida cautelar que buscava assegurar o fornecimento de dados e conhecimentos específicos à ABIN (Agência Brasileira de Inteligência) pelos órgãos do Sistema Brasileiro de Inteligência – SISBIN, determinando que tal compartilhamento só pode se dar quando restar devidamente comprovado o interesse público.

Ainda assim, por se tratar de uma limitação aos direitos fundamentais, o Supremo determinou a instauração de procedimento formal para tais casos, bem como a comprovação da existência de sistemas de segurança eletrônicos e registros de acesso que servirão, inclusive, como evidências para situações que envolvam a responsabilização dos agentes.

A questão basilar, neste caso, trata de encontrar o equilíbrio entre a publicidade dos atos administrativos e a proteção dos dados pessoais, mormente no que concerne à fiscalização e auditoria e é justamente neste ponto que entram os Tribunais de Contas. Qual o impacto da LGPD no trabalho realizado pelos Tribunais de Contas e como eles poderiam colaborar para a aplicabilidade eficaz da LGPD?

### **3 A proteção de dados como direito fundamental e o papel dos Tribunais de Contas**

Um dos principais impactos da LGPD no que se refere ao trabalho dos Tribunais de Contas diz respeito à necessidade de informar a finalidade pela qual se trata o dado pessoal, algo que por muitos anos foi negligenciado, diante da falta de uma exigência legal, de modo que o tratamento de dados, até pouco tempo, se dava indiscriminadamente, sem maiores preocupações com privacidade, com segurança da informação ou, até mesmo, com o dever de informar a finalidade do tratamento.

Em pesquisa realizada (junho de 2021), no âmbito do Comitê de Tecnologia, Governança e Segurança da Informação dos Tribunais de Contas e divulgada no site do Instituto Rui Barbosa<sup>12</sup>, onde 73% dos Tribunais participaram, consta que:

- 75% deles já iniciou a adequação do órgão à LGPD contando com apoio da própria equipe e 8% iniciou com apoio externo;
- 54% possui programa de capacitação continuada ou esporádica;
- 33% considera que conseguirá atender às requisições dos titulares;
- 42% já designou o Encarregado de dados sendo que, destes, 8% são servidores da área de TI;
- 79% já possui equipe de segurança da informação;
- 21% possui um programa de Governança em privacidade;

12 XAVIER, Fábio Correa. Tribunais de Contas avançam na implementação da LGPD. *Equipe Instituto Rui Barbosa*. 21 jun. 2021. Disponível em <https://irbcontas.org.br/tribunais-de-contas-avancam-na-implementacao-da-lgpd/>. Acesso em 17 de nov. 2021.

- 8% já finalizou a revisão de contratos à luz da LGPD;
- 4% finalizou o inventário de dados;

A pesquisa demonstra que a adequação está ocorrendo, ainda que a passos lentos, mas a pergunta é: como a LGPD poderá impactar os trabalhos destes importantes órgãos de fiscalização?

Para uma resposta adequada precisamos entender o papel dos Tribunais de Contas, cuja missão constitucional é realizar o Controle Externo da Administração Pública, conforme disposto na Carta Constitucional.

Neste sentido, o primeiro desafio dos TCs consiste em sua própria reestruturação, a fim de proceder a adequação, necessária, ao texto expresso na lei de proteção de dados brasileira.

Para tanto, impende criar, em primeiro lugar, um Grupo de trabalho ou um Comitê de privacidade e, em seguida, efetivar a nomeação do Encarregado de Dados, que auxiliarão nos primeiros passos, rumo a essa necessária adequação.

Importante salientar que, devido à forte possibilidade de conflito de interesses, não é recomendável que o Encarregado de dados seja alguém vinculado à direção da TI, do mesmo modo que não se recomenda a vinculação do Encarregado à Ouvidoria. A LGPD sugere que o encarregado seja dotado de autonomia e independência.

A nomeação do Encarregado, ou DPO, deve ser evidenciada por meio da publicação de Portaria, e o contato telefônico deste servidor público deve ser publicado em local de fácil acesso, de preferência, no próprio site do tribunal.

Em seguida, deverão ser atualizadas e publicadas as políticas de privacidade e demais documentos neste sentido, mas a prioridade deve ser o aprimoramento (e dependendo do caso até mesmo a criação) de uma cultura da privacidade dentro dessas instituições, que deverá refletir para todos os que tenham acesso à instituição.

A recomendação é de que o sítio eletrônico da instituição seja remodelado, de modo a deixar clara a preocupação institucional com a privacidade dos dados, e algumas atitudes podem demonstrar isso como, por exemplo, avisos curtos mas de clara visibilidade, de maneira que logo ao acessar a página da internet, todos possam ficar cientes de que a instituição está em conformidade com a LGPD (ou está se adequando); uma política de privacidade de dados objetiva e clara, que seja fácil de encontrar; uma aba ou um link, especificamente para tratar de temas relacionados a proteção de dados, são alguns exemplos de boas práticas.

O uso de *cookies*, muito comum nos dias atuais, deve ser claramente informado. Todavia, ao contrário do que vemos em muitas páginas da internet, o aviso de uso de *cookies* deve possibilitar que o leitor negue sem perder o acesso à página. É muito comum vermos esses avisos atualmente, todavia, na maior parte das vezes, as únicas opções ofertadas ao avisado são: “aceitar e fechar”, “entendi”, “fechar” ou apenas “aceitar”, ou outras expressões similares. No site do TCU, “você pode instruir seu navegador a recusar todos os cookies ou indicar quando um cookie está sendo enviado. No entanto, se você não aceitar cookies, talvez não consiga usar algumas partes de nosso Serviço”.<sup>13</sup>

Outro ponto que merece atenção se refere à determinação da lei de facilitar o acesso aos dados, por parte do titular. A recomendação é de que essa facilitação se dê por meio de

13 BRASIL. TCU e a Lei Geral de Proteção de Dados – LGPD. *Tribunal de Contas da União*. 2021. Disponível em: <https://portal.tcu.gov.br/lgpd/> Acesso em 17 nov. 2021.

formulários, disponibilizados na página institucional, na Internet, que permita ao titular ter conhecimento acerca dos dados tratados a seu respeito, corrigir aqueles que estiverem errados e, até mesmo, solicitar a exclusão dos seus dados. Neste caso, ao solicitar a exclusão, seu pedido deverá ser imediatamente acatado, exceto nos casos em que existirem leis que determine a manutenção da guarda desses dados, mas apenas pelo tempo que a lei determinar.

No que concerne ao Portal Transparência, uma boa prática de alinhar o disposto na LGPD à Lei de Acesso à Informação (LAI – Lei nº 12.527/11), que tem sido observada, é a divulgação dos salários conforme o cargo, apenas sem citar o nome do servidor, e, para os casos em que for necessário o nome do servidor, solicitar o nome e o CPF do requerente. Nesses casos, contudo, é importante informar que a finalidade da coleta é para a segurança do servidor (titular do dado que está sendo requerido), bem como informar onde esse dado ficará arquivado, por quanto tempo e quem terá acesso ao mesmo.

Informar que o IP do computador do requerente ficará gravado, também tem sido utilizado como boa prática. Tudo isso poderá inibir os acessos com fins meramente especulativos, assegurando a publicidade conforme a exigência da LAI, com a devida proteção dos dados dos titulares e, portanto, também em conformidade com a LGPD.

Com a LGPD, não há mais possibilidade de manter arquivos contendo dados pessoais indefinidamente. O tratamento dos dados deve ter prazo para acabar podendo, o titular, requerer a exclusão dos seus dados a qualquer tempo e, diante dessa possibilidade, a LGPD prevê que o controlador poderá se eximir de cumprir tal solicitação quando comprovar a existência de lei que estabeleça prazo certo e determinado para o armazenamento desses dados.

### *3.1 Da Fiscalização pelos Tribunais de Contas frente à proteção de Dados: principais impactos*

Em anexo à Nota Técnica de nº 01 de 2019, o Instituto Rui Barbosa manifestou-se a respeito da aplicabilidade da LGPD no âmbito dos Tribunais de Contas, reconhecendo “o imperioso que as Cortes de Contas busquem adequar-se aos aspectos inovadores da lei,”<sup>14</sup>, e, neste contexto, estabeleceu 15 diretrizes a serem observadas por esses órgãos, este o qual, conforme ressalta, deve sempre considerar a necessidade de um diálogo constante entre a LGPD e legislações outras como a Lei Federal nº 131/2009 (Lei da Transparência), a Lei Federal nº 12.527/2011 (Lei de Acesso à Informação – LAI), a fim de aplicá-las de maneira integrada.

Para tanto, a referente nota se baseou em premissas como:

1. A LGPD se aplica a qualquer operação de tratamento;
2. Os Tribunais de Contas produzem e recebem dados e informações no exercício de suas competências constitucionais, legais e regulamentares;
3. No exercício de sua função fiscalizatória, os Tribunais de Contas necessitam ter acesso a dados pessoais a fim de assegurar o cumprimento de sua missão constitucional;
4. Os Tribunais de Contas devem observar o disposto no art. 7º, III e § 3º e art. 23 da LGPD, tendo em vista que sua atuação deve ser, sempre, pautada nos princípios da legalidade e na persecução do interesse público;

<sup>14</sup> INSTITUTO RUI BARBOSA. Anexo. Nota Técnica 01/2019. ATRICON. 2019. Disponível em <https://www.atricon.org.br/wp-content/uploads/2019/11/NOTA-TECNICA-ANEXO-I.pdf>. Acesso em 17 nov. 2021.

5. Para a eficácia e eficiência da atividade fiscalizatória de qualidade, mister se faz assegurar, aos Tribunais de Contas, o exercício de suas competências constitucionais e legais consoante os princípios da publicidade, eficiência, supremacia do interesse público, transparência das informações e acesso geral às prestações de contas (arts. 5º, 37 e 71 CR/88);
6. O compartilhamento de dados e informações torna as atividades desempenhadas mais eficientes e, por isso, deve ser estimulado e ampliado no setor público, de modo que informações podem ser utilizadas como insumos para o cumprimento das funções públicas;
7. O crescente número de políticas públicas multissetoriais e transversais, envolvendo diversos entes da federação, enseja a necessidade do compartilhamento de informações entre as instituições de diferentes poderes e entes e, para tanto, deverão observar o disposto nos artigos 25 a 27 da LGPD.

Acerca dos impactos da LGPD nas atividades fiscalizatórias dos Tribunais de Contas, explica Moises Maciel:

No que concerne às cortes de contas, a nova Lei Geral de Proteção de Dados Pessoais brasileira não gera impactos negativos, sendo a eles aplicada, consoante o disposto em seu próprio texto legal que, por sua vez, já excetua da obrigatoriedade de observância normativa os casos de exercício das funções fiscalizadoras e sancionadoras, típicas (mas não únicas) dos tribunais de contas. Nesses casos, a lei prevê expressamente a sua inaplicabilidade no sentido de não ser obrigatório o consentimento prévio do titular dos dados pessoais, no entanto determina a observância dos princípios da finalidade, da necessidade, da proporcionalidade, de modo que devem utilizar tais dados com o intuito exclusivo de atender ao interesse público, limitando o seu compartilhamento para fins outros. A finalidade da lei é protetiva e seu impacto perante o exercício das funções dos tribunais de contas se dá no sentido de determinar responsabilidade no tratamento dos dados pessoais, mitigando o direito à privacidade e à intimidade dos indivíduos, a fim de garantir algo maior, qual seja: o bem-estar social.<sup>15</sup>

Em setembro de 2021, o Tribunal de Contas da União publicou documento chamado “Estratégia de Fiscalização do TCU em segurança da informação e segurança cibernética, 2020-2023”<sup>16</sup>, onde traz uma relação de boas práticas com vistas a aprimorar o panorama da Administração Pública Federal nas áreas da segurança da informação e da segurança cibernética, de modo a mitigar riscos e possíveis impactos de ataques cibernéticos.

Neste documento, encontra-se a recomendação de auditoria com vista a conscientizar os gestores, bem como verificar o nível de preparo e de conformidade das diversas instituições públicas às disposições contidas na LGPD, bem como de avaliar a estruturação da Autoridade Nacional de Proteção de Dados (ANPD) por meio de uma abordagem de autoavaliação de controles (*Control Self Assessment*), através do qual deverão ser aplicados, aos gestores, questionários sobre conceitos básicos da lei, tais como princípios, direito dos titulares e bases legais, por exemplo, além das etapas de implantação de um Sistema de Gestão de Proteção de Dados (SGPD).

15 Maciel, Moises. Os tribunais de contas no exercício do controle externo de acordo com nova Lei Geral de Proteção de Dados Pessoais. *Revista Controle: doutrina e artigos*, Vol. XIII, n. 1, jan./jun.2020, p. 41.

16 BRASIL. *Estratégia de fiscalização do TCU em Segurança da Informação e Segurança Cibernética 2020-2023*. Tribunal de Contas da União. 02 set. 2021. Disponível em <https://portal.tcu.gov.br/estrategia-de-fiscalizacao-e-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023.htm>. Acesso em 17 nov. 2021.

Conforme documento supramencionado, os gestores deverão responder os questionários e anexar as evidências, através de documentos que comprovem suas respostas ou, então, as justificativas necessárias para as deficiências apresentadas e todo esse material deverá ser analisado e consolidado para fins de um relatório final.

Essa auditoria objetiva não só avaliar o processo de implantação da LGPD na Administração Pública Federal como, ainda, para servir de conscientização, despertando o interesse para o tema, na busca de uma conformidade total por parte das Cortes de Contas.

O documento prevê, ainda, a realização de outras auditorias como “Auditoria em sistema crítico” (buscando avaliar regras de negócio e SegInfo) e “Auditoria sobre *backup*” (já realizada nos períodos entre 15/10 e 13/11, em parceria entre a Sefti e outras 12 unidades técnicas da Segecex do TCU, aguardando a expedição de relatório final a ser publicado), com vistas a avaliar se os procedimentos de *backup* e *restore* das organizações da Administração Pública federal estão sendo suficientes e adequados para assegurar a continuidade dos serviços prestados.

Além destas, estão relacionadas, também, fiscalização do tipo “acompanhamento” para obtenção de dados, com vistas a avaliar a adoção de controles críticos para a gestão de SegCiber pela Administração Pública Federal, a “Auditoria sobre identidade e assinaturas Digitais” e, ainda, a “Auditoria no processo de resposta a incidentes cibernéticos”, buscando avaliar a capacidade de resposta a tais incidentes, por parte dos órgãos da Administração Pública Federal.

A finalidade do documento mencionado consiste, dentre outras coisas, em divulgar a visão do TCU e replicar esse trabalho para os Tribunais de Contas Estaduais, através de capacitações, com o intuito de compartilhar experiências, técnicas e ferramentas e, ainda, na elaboração de materiais de divulgação a fim de orientar os gestores públicos.

Neste diapasão, é perceptível o desafio dos Tribunais de Contas no sentido de desenvolver conhecimentos de governança pública voltados para a proteção de dados, para no exercício da função pedagógica, orientar os gestores públicos na efetivação de políticas públicas baseadas na LGPD.

No mesmo sentido, cumpre a realização de uma atualização das matrizes de auditoria, que conduzem a atividade fiscalizatória do controle externo, além de estabelecer pontos de controle da governança pública pertinentes aos dados pessoais, sem esquecer do aprimoramento, primordial, de uma cultura de privacidade junto aos servidores destas instituições.

Agir de maneira proativa, orientando os jurisdicionados no tocante ao cumprimento do disposto na LGPD e se estruturando no mesmo sentido, é uma determinação constitucional para as Cortes de Contas: cumprir e fazer cumprir o princípio da legalidade.

## 4 Conclusão

A LGPD já está impactando profundamente no funcionamento e organização das empresas e agentes privados e do próprio Poder Público, inclusive os Tribunais de Contas.

Esses últimos, como órgãos técnicos e independentes, responsáveis, dentre outras coisas, pela fiscalização das contas públicas, precisarão demonstrar cumprimento íntegro aos mandamentos das normativas em relação à proteção de dados, juntamente com a transparência

cujos requisitos são intrínsecos aos postulados do Poder Público, no que concerne ao tratamento dos muitos dados que se encontram sob seu poder.

A adequação já vem ocorrendo em todo o Brasil, e, por se tratar de um processo que demanda um relativo tempo de adaptação, vale ressaltar uma das funções exercidas pelos Tribunais de Contas, qual seja, no exercício de suas competências constitucionais: a função pedagógica.

Na sociedade contemporânea, que se organiza na complexidade de um sem-número de informações, a dificuldade em se discriminar os fatos de inverdades, somada à manipulação e construção de notícias inverídicas - *fake news* -, a confiança vem despontando como um legitimador do cotejo de fatos e dados sobre seu objeto, com apurados e sistemáticos filtros. A responsabilidade dos Tribunais de Contas no exercício de sua função pedagógica, primeiramente se otimizando a fim de dar o exemplo como órgão público que trata os dados pessoais com respeito, responsabilidade e transparência e, ainda, como responsável pela orientação técnica de seus jurisdicionados, alcança uma importância considerável e que precisa ser não só debatida, como reconhecida e devidamente aplicada.

Compete aos Tribunais de Contas, dentre suas diversas funções e competências, reconhecidas e amparadas pela Constituição da República brasileira, exercer a devida orientação dos seus jurisdicionados, com relação aos passos que estes deverão observar para a implementação eficaz e eficiente do disposto na lei de proteção de dados brasileira, possibilitando que o tratamento de dados, por eles realizados, se dê de forma consciente, legítima e adequada. Para tanto, será preciso que essa orientação esteja acompanhada de uma fiscalização adequada, a fim de avaliar o seu real cumprimento.

Desta forma, com a LGPD, surge para os Tribunais de Contas mais uma responsabilidade, de atuar como fiscalizadores, ao lado da Autoridade Nacional de Proteção de Dados, em primeiro lugar orientando, para, em seguida, avaliar o cumprimento das exigências contidas na referida legislação, objetivando um tratamento de dados pelo poder público que vá ao encontro das expectativas de toda a coletividade, que precisa ter seus dados tratados pelos diversos setores da Administração Pública, mas, mais do que isso, que esse tratamento se dê com respeito, com transparência e com a responsabilidade sempre ansiada por todos.

## Referências

BRASIL. Câmara de Coordenação e Revisão 3. *Roteiro de Atuação*. Sistema Brasileiro de Proteção e Acesso a Dados Pessoais. Análise de dispositivos à lei de acesso à informação, da lei de identificação civil, da lei do marco civil da internet e da lei nacional de proteção de dados. v. 3. Ministério Público Federal. Brasília: MPF, 2019, p. 25. Disponível em <http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3> Acesso em 17 de nov. 2021.

BRASIL.. Decreto nº 10.046 de 2019. Disponível em [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/decreto/D10046.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm). Acesso em 17 de nov. 2021.

BRASIL. *Estratégia de fiscalização do TCU em Segurança da Informação e Segurança Cibernética 2020-2023*. Tribunal de Contas da União. 02 set. 2021. Disponível em <https://portal.tcu.gov.br/>

tcu.gov.br/estrategia-de-fiscalizacao-do-tcu-em-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023.htm. Acesso em 17 nov. 2021.

BRASIL. Lei nº 13.709/2018 – LGPD. Disponível em [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em 17 nov. 2021.

BRASIL. TCU e a Lei Geral de Proteção de Dados – LGPD. *Tribunal de Contas da União*. 2021. Disponível em: <https://portal.tcu.gov.br/lgpd/> Acesso em 17 nov. 2021.

INSTITUTO RUI BARBOSA. Anexo. Nota Técnica 01/2019. ATRICON. 2019. Disponível em <https://www.atricon.org.br/wp-content/uploads/2019/11/NOTA-TECNICA-ANEXO-I.pdf>. Acesso em 17 nov. 2021.

Maciel, Moises. Os tribunais de contas no exercício do controle externo de acordo com nova Lei Geral de Proteção de Dados Pessoais. *Revista Controle: doutrina e artigos*. Vol. XIII, n. 1, jan./jun.2020, pp. 20-45.

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

PORTUGAL. *Resolução 3/2018 – PG*. do Tribunal de Contas. 2018. Disponível em <https://www.tcontas.pt/pt-pt/NormasOrientacoes/Resolucoes/Documents/2018/res003-2018-pg.pdf> Acesso em 17 nov. 2021.

SILVEIRA. Luís Novais Lingnau da. O Direito à proteção de dados pessoais. *Comissão Nacional de Protecção de Dados*. Disponível em [https://apdsi.pt/wp-content/uploads/prev/2.11\\_luis%20silveira\\_070626.pdf](https://apdsi.pt/wp-content/uploads/prev/2.11_luis%20silveira_070626.pdf) Acesso em 17 de nov. 2021.

UNIÃO EUROPEIA. *Regulamento (UE) 2018/1725*. Considerando nº 25. 2018. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725> Acesso em 17 nov. 2021.

XAVIER, Fábio Correa. Tribunais de Contas avançam na implementação da LGPD. *Equipe Instituto Rui Barbosa*. 21 jun. 2021. Disponível em <https://irbcontas.org.br/tribunais-de-contas-avancam-na-implementacao-da-lgpd/>. Acesso em 17 de nov. 2021.