

**Controles de proteção de dados pessoais dos povos indígenas implementados na FUNAI:  
uma análise do Acórdão n. 1.384/2022 do Tribunal de Contas da União**

**Felipe Pinheiro Prestes**<sup>1</sup>  

Universidade do Extremo Sul Catarinense, UNESC, Brasil.

E-mail: felipeprestesrs@gmail.com

**Daniel Ribeiro Preve**<sup>2</sup>  

Universidade do Extremo Sul Catarinense, UNESC, Brasil.

E-mail: drp@unesc.net

**Marcio Teza de Bona**<sup>3</sup>  

Universidade do Extremo Sul Catarinense, UNESC, Brasil.

E-mail: tezadebona@hotmail.com

**Resumo:** O foco desta pesquisa está na proteção dos dados pessoais tratados pela Fundação Nacional dos Povos Indígenas (FUNAI) sob a ótica do Acórdão n. 1.384/2022 do Tribunal de Contas da União (TCU), referente à auditoria realizada na organização, a fim de obter dados de sua adequação à Lei Geral de Proteção de Dados (LGPD). Portanto, a problemática de pesquisa é justamente saber se a FUNAI está satisfatoriamente adequada à LGPD por meio dos resultados da auditoria. Nesse sentido, em um primeiro momento, buscou-se demonstrar a evolução e adequação da tutela da privacidade dos dados pessoais em um contexto histórico se perfectibilizando em um direito fundamental referente ao tema. Em seguida, foram tratados conceitos legais da LGPD aplicáveis ao estudo, bem como feita a caracterização dos dados pessoais do indígena. Por fim, deu-se especificamente a análise do referido acórdão do TCU, sendo apontadas algumas críticas necessárias, dada a sensibilidade do tema estudado. Neste trabalho, foi adotada a metodologia exploratória e descritiva documental, em conjunto com o método hipotético-dedutivo. Como resultado, evidencia-se o descompasso da FUNAI à LGPD, bem como a evidente possibilidade de riscos de grande monta à população indígena em caso de incidentes de segurança da informação, mas há possibilidade de melhoria nas lacunas encontradas na pesquisa, na FUNAI.

---

1 Mestrando em Direito pelo Programa de Pós-Graduação em Direito da Universidade do Extremo Sul Catarinense-UNESC, Criciúma, Santa Catarina, Brasil. Pesquisador do Núcleo de Pesquisas em Direitos Humanos e Cidadania (NUPEC – UNESC). ORCID: <https://orcid.org/0009-0000-6196-1241>. Currículo Lattes: <http://lattes.cnpq.br/5749567663987781>. E-mail: felipeprestesrs@gmail.com.

2 Doutor em Direito. Professor e Pesquisador Permanente do Programa de Pós-Graduação - Mestrado em Direito da Universidade do Extremo Sul Catarinense - UNESC, Criciúma, Santa Catarina, Brasil. Líder e pesquisador do Grupo de Pesquisa em Direito à Cidade e Políticas de Sustentabilidade Urbana e Ambiental (GPDUC/UNESC). Advogado. ORCID: <https://orcid.org/0000-0002-6231-8466>. Currículo Lattes: <http://lattes.cnpq.br/9200020665014823>. E-mail: drp@unesc.net

3 Mestrando em Direito pelo Programa de Pós-Graduação em Direito da Universidade do Extremo Sul Catarinense-UNESC, Criciúma, Santa Catarina, Brasil. Pesquisador do Grupo de Pesquisa em Direito à Cidade e Políticas de Sustentabilidade Urbana e Ambiental (GPDUC/UNESC). ORCID: <https://orcid.org/0009-0000-4294-1464>. Currículo Lattes: <http://lattes.cnpq.br/4113580313290967>. E-mail: tezadebona@hotmail.com

**Palavras-chaves:** Direitos Humanos; Fundação Nacional dos Povos Indígenas; Lei Geral de Proteção de Dados; Povos indígenas; Tribunal de Contas da União.

**Personal data protection controls for indigenous peoples, implemented at FUNAI:  
an analysis of Ruling n. 1.384/2022 by Federal Court of Auditors**

**Abstract:** The focus of this research is on the protection of personal data processed by the National Foundation for Indigenous Peoples (FUNAI) from the perspective of Judgment n. 1.384/2022 of the Federal Court of Auditors (TCU), referring to the audit carried out on the organization to obtain data on its compliance with the General Data Protection Law (LGPD). Therefore, the research problem is precisely whether FUNAI is satisfactorily complying with the LGPD through the results of the audit. In this sense, we first sought to demonstrate the evolution and adequacy of the protection of personal data privacy in a historical context, that became a fundamental right on the subject. This was followed by a discussion of the legal concepts of the LGPD applicable to the study, as well as a characterization of indigenous people's personal data. Finally, the TCU ruling was specifically analyzed, and some necessary criticisms were pointed out, given the importance of the topic studied. In this work, the exploratory and descriptive documentary methodology was adopted, along with the hypothetical-deductive method. As a result, FUNAI's failure to comply with the LGPD is evident, as well as the obvious possibility of major risks to the indigenous population in the event of information security incidents, but there are possibilities to improve the gaps found in FUNAI.

**Keywords:** Federal Court of Auditors; General Data Protection Law; Human Rights; Indigenous peoples; National Foundation for Indigenous Peoples.

**Sumário:** 1. Introdução 2. Síntese histórica da evolução do direito à privacidade e proteção de dados pessoais como direito fundamental 3. A LGPD e a sua aplicação ao titular de dados indígenas 4. Análise do Acórdão n. 1.384/2022 do TCU 5. Conclusão.

## 1. INTRODUÇÃO

A privacidade começou a ganhar relevância em meados de 1890, quando Louis D. Brandeis escreveu um artigo para a revista “*Harvard Law Review*”, mencionando que métodos de negócios e invenções recentes daquela época poderiam ameaçar a proteção das pessoas e o direito à privacidade.

Após a Segunda Guerra Mundial, no ano de 1948, o tema “privacidade de dados pessoais” começou a ganhar importância no cenário internacional, sendo abordado e garantido como direito por meio do artigo 12 da Declaração Universal dos Direitos Humanos (UNICEF BRASIL, 2022). Nas décadas seguintes, foi possível experimentar novos institutos normativos, com a intenção de tutelar a privacidade das pessoas, inclusive dos seus dados, conforme explorado no primeiro

capítulo, por meio de três casos de diferentes países, quais sejam: Estado Unidos, França e Alemanha.

Nesse sentido, é interessante destacar que foi constatada, no ano de 1970, com início da popularização de aplicação da Tecnologia da Informação e Comunicação, bem como com o aumento do comércio transfronteiriço europeu, a necessidade da adoção de mecanismos que permitissem maior gestão das informações pessoais, para garantir que os indivíduos pudessem exercer controle de seus dados sem que houvesse impactos indesejáveis no desenvolvimento econômico. Tal desafio foi tratado em 1995 pela Diretiva 95/46/CE do Parlamento Europeu, visando harmonizar as legislações europeias no que tange ao tratamento de dados pessoais e à livre circulação destes.

A referida Diretiva se mostrou insuficiente, pois cada país da Europa possuía diferentes leis para tratar do tema. Dessa forma, no ano de 2016 entrou em vigor o Regulamento Geral de Proteção de Dados no continente europeu, legislação que influenciou a criação da Lei Geral de Proteção de Dados (LGPD), colocando o Brasil em patamar semelhante ao de outros países que tutelam o direito à privacidade e proteção dos dados.

Mais tarde, também, no Brasil, foi reconhecido um direito Fundamental à Proteção de Dados, sendo inserido na Constituição Federal no seu artigo 5.º, inciso LXXIX, evolução tratada no primeiro capítulo da presente análise.

No capítulo seguinte, considerando-se o direito fundamental acima arrolado e a existência da LGPD, faz-se uma análise dos conceitos legais necessários para a compreensão do tema debatido no Acórdão n. 1.384/2022 do Tribunal de Contas da União (TCU), das características dos dados pessoais da pessoa indígena, tratados pela Fundação Nacional dos Povos Indígenas (FUNAI) e da forma como devem legalmente ser conceituados, dada a origem racial, étnica, suas convicções religiosas, filosóficas e dados genéticos, além de haver a necessidade de observação, com olhares atentos, dos riscos à população nacional pertencente aos povos originários.

No terceiro capítulo, enfim, é analisado o referido Acórdão, bem como tecida alguma crítica referente ao resultado obtido, notadamente considerando a relevância e sensibilidade do tema quando vinculado à população indígena.

## **2. SÍNTESE DA EVOLUÇÃO DO DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS COMO DIREITOS FUNDAMENTAIS**

O presente capítulo aborda os principais aspectos conceituais a respeito da LGPD, com uma breve síntese histórica evolutiva do assunto que culminou na referida legislação e o mais recente direito fundamental, reconhecido e inserido na Constituição Federal, notadamente o direito fundamental à proteção de dados pessoais.

De fato, não se trata de tarefa fácil resumir a evolução histórica da importância da privacidade na sociedade, contudo ela é necessária, devido à aplicação da tecnologia no contexto social, tal como se constata na atualidade, mesmo que de forma resumida.

Nesse sentido, primeiramente, é importante pontuar que a história ensina que a privacidade começou a ser juridicamente tratada por iniciativa da doutrina no final do século XIX, por meio dos estudos de Warren e Brandeis (1890), porém, só mais recentemente é que recebeu os contornos

atualmente conhecidos (Limberger, 2020). Contudo, foram, no decorrer do século XX, os principais acontecimentos que evidenciaram a necessidade de tutela dos dados pessoais, notadamente, se tornando tema relevante em tratados internacionais e atos internos.

Nesse sentido, no ano de 1948, a Declaração Universal dos Direitos Humanos trouxe, no artigo 12, o direito à privacidade e intimidade nos seguintes moldes, informando que ninguém “será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem o direito à proteção da lei contra tais interferências ou ataques”.

Interessante também pontuar que, segundo Santos (2005), a Declaração Universal dos Direitos Humanos, nos moldes em que é conhecida na atualidade, pacifica princípios que vinham sendo concebidos na história do mundo ocidental há muito tempo. Com o passar das décadas e o avanço tecnológico, novos desafios se apresentaram, colocando a privacidade do cidadão em xeque. Dessa forma, Danilo Doneda (2019) aponta três notórios casos que trouxeram ao protagonismo a necessidade da proteção dos dados da população, inclusive com forte apelo da sociedade por uma significativa resposta para possíveis abusos que seriam cometidos.

Nessa perspectiva, o primeiro acontecimento é datado na década de 1965, o caso do *National Data Center*<sup>4</sup>, um evento paradigmático, que demonstra a súbita reação de alguns grupos da sociedade quanto aos efeitos da utilização da informática no processamento de dados pessoais (Doneda, 2019). No ocorrido, o Escritório de Orçamento dos Estados Unidos apresentou uma proposta que originalmente aparentava ser simples e natural, em razão da inerente evolução na estrutura administrativa do Estado, tornando possível, com a utilização da computação, a construção de uma central única de armazenamento de dados pessoais em um único banco de dados, pois justamente a fragmentação das informações da sociedade trazia incômodo para a eficiência governamental (Doneda, 2019).

Entretanto, os idealizadores da referida proposta, muito aparentemente cegados pela eficiência de sua ideia ou, então, por desconsiderar esse cenário pouco explorado na época, não levaram em conta as implicações que poderiam surgir, em especial, referente à privacidade do cidadão estadunidense, provocando reações, já que se percebia certo temor pela introdução dos primeiros computadores no tecido social (Doneda, 2019).

O Congresso Nacional dos Estados Unidos da América não endossou a medida debatida, decidindo que nada deveria ser feito em relação à construção de um banco de dados nacional, sem que fosse observada a proteção da privacidade, decisão tomada depois de uma série de audiências que se deram após a discussão em âmbito científico e consultas à opinião pública acerca do tema (Doneda, 2019).

Servindo como prólogo para futuras discussões em outros Estados, o caso do *National Data Center* influenciou e foi exemplo para decisões semelhantes nas décadas posteriores. Assim, a segunda situação, determinante para a evolução do direito de privacidade de dados pessoais, foi o caso do *Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*<sup>5</sup>

4 Tradução livre: Centro Nacional de Dados

5 Tradução livre: Sistema Automatizado para Arquivos Administrativos e Diretório de Indivíduos.

(SAFARI), que aconteceu na França, na década de 1970, época em se tornou pública a intenção do *Institut National de la Statistique*<sup>6</sup> de transferir para sistemas informatizados todos os dados pessoais dos cidadãos franceses que estavam em posse da Administração Pública. Um dos principais objetivos do referido projeto era a identificação do sujeito por meio de um número de *Sécurité Sociale*<sup>7</sup> que lhe seria atribuído desde o nascimento, sendo invariável durante toda a sua vida (Doneda, 2019).

Da mesma forma do ocorrido na década anterior nos Estados Unidos, o projeto francês seria de ordem técnica, para tão somente melhorar a eficiência administrativa governamental, não sendo feita necessária análise jurídica dos direitos da população francesa, sem desconsiderar que também era plano que possuía raízes em pretensões pautadas em um governo discriminatório da República de Vichy (Doneda, 2019).

É interessante destacar, nesse ponto, o enfoque dado por Danilo Doneda (2019) ao se debruçar no desenvolvimento do seu estudo, sublinhando um governo discriminatório ao interseccionar com a abordagem sobre a privacidade dos dados pessoais. Em síntese, é focal que a má utilização ou o tratamento de dados pessoais de forma irresponsável pode ser direcionado para atos discriminatórios, ponto que é sensível para a pesquisa em desenvolvimento no presente artigo, haja vista tratar-se de análise dos dados pessoais daqueles que fazem parte de populações indígenas, dados sensíveis por natureza, como ainda será caracterizado em capítulo adiante.

Feita a consideração do parágrafo anterior, retorna-se à situação do Estado francês, assinalando que a repercussão do referido projeto não ocorreu da forma esperada, tampouco eficaz, sendo que o então primeiro-ministro, por meio de medida administrativa, interditou todos os tipos de transações de dados pessoais entre ministérios, conseqüentemente encerrando o projeto SAFARI e, após a constituição da comissão *Informatique et libertés*<sup>8</sup>, resultou na Lei n. 78-17, de 6 de janeiro de 1978, conhecida como *Loi Informatique, Fichiers et Libertés* (França, 1978)<sup>9</sup>.

Outras discussões que se assemelham ao caso francês também ocorreram em outros países, sendo que muitos adaptaram os seus ordenamentos, a fim de equipararem-se à nova realidade.

O terceiro caso se trata da legislação alemã sobre proteção de dados pessoais, sendo de suma importância salientar que o governo da Alemanha trata o tema com notória importância, sendo a primeira nação do mundo a tutelar sobre o direito de proteção de dados por meio do estado de Hassen ainda em 1970, a qual contemplava apenas dados públicos informatizados (Mendes; Sarlet; Coelho, 2015). Posteriormente, o texto fora substituído pela *Bundesdatenschutzgesetz*<sup>10</sup>, encarregada da proteção tanto dos dados públicos quanto dos pessoais. O marco que deu início para que fosse feita a alteração das legislações foi o censo demográfico proposto pelo governo alemão (Limberger, 2000).

No entanto, diversas reclamações constitucionais foram ajuizadas por diferentes grupos da sociedade com a intenção de impugnar a lei federal editada no ano de 1982, uma vez que, no texto

6 Tradução livre: Instituto Nacional de Estatística.

7 Tradução livre: Seguro Social.

8 Tradução livre: Computação e Liberdade.

9 Tradução livre: Lei de Proteção de Dados, Arquivos e Liberdades.

10 Tradução livre: Lei Federal de Proteção de Dados.

legal, previa-se para 1983 a realização de um recenseamento demográfico da população, por meio do qual não seria feito um levantamento referente ao número de habitantes, mas, sim, a coleta de dados pessoais dos cidadãos (Mendes; Sarlet; Coelho, 2015).

A Corte Federal da Alemanha suspendeu os efeitos da Lei do Recenseamento pela interpretação de regras constitucionais, contidas nos artigos 1.1 e 1.2 da Lei Fundamental (Limberger, 2000). Porém, fora permitido que o ato governamental fosse praticado desde que as medidas fossem tomadas, com o intuito de resguardar os dados pessoais da população, como, por exemplo, a proibição de coleta de nomes e endereços para transferência para outros órgãos (Mendes; Sarlet; Coelho, 2015).

Tão importante quanto interessante é observar que o receio do cidadão alemão dos primeiros anos da década de 1980 em relação ao recenseamento, de fato, se tratava de algo real, visto que a contextualização história e social se tornara elemento influenciador daquela sociedade. Nesse sentido, um dos prováveis fatores influenciadores para a onda de protestos contra o censo pode ser o fato de a data aproximar-se das previsões contidas na obra de 1984, de George Orwell. Frisa-se que não apenas o ano destacado no romance estava próximo às manifestações, mas também que, na história, contida no livro, seria o Estado o responsável por exercer o controle sobre a população, pela constante vigilância do Grande Irmão, e de suas informações pessoais, inclusive dentro de suas próprias casas por meio dos dispositivos chamados “teletelas”. Outrossim, o desenvolvimento dos computadores da época apenas permitia que os dados fossem armazenados em grandes centros informatizados e não, de forma fracionada em máquinas situadas em diferentes locais, na forma que a *Internet* atualmente permite. Ademais, não pode ser descartado o receio que o cidadão alemão tinha do Estado, uma vez que este espionava os cidadãos na Alemanha Oriental (Mendes; Sarlet; Coelho, 2015).

Ainda, a decisão do Tribunal Alemão fora um fato muito impactante, visto que se tornou um marco na proteção de dados, uma vez que fixou diretrizes relacionadas à disciplina, as quais serviram para influenciar outras legislações e a doutrina. Além disso, ocorrera naquele momento o reconhecimento do direito denominado “autodeterminação informativa”, integrando o direito geral de personalidade, desenvolvido desde a década de 1950 pelo Tribunal Constitucional Alemão (Doneda, 2019).

Assim, foram observados, a partir dos três casos estudados que surgiram no mundo, ainda no século XX, os primeiros dispositivos a tutelarem o direito de privacidade quanto à proteção dos dados pessoais e, há pouco mais de uma década atrás, fora constitucionalmente reconhecido o direito fundamental alemão sobre o tema, conforme ensina Doneda (2019), derivado ainda do primeiro instituto mundial, dedicado exclusivamente ao assunto, evidenciando a evolução da legislação da Alemanha, o que também demonstrou a tendência no crescimento da importância para tratar da privacidade de dados pessoais.

Nesse sentido, Rodatà (2008) evidência que não é apenas o cenário tecnológico que avança para o futuro, o qual vai se transformando, mas também a profunda mudança no contexto jurídico institucional, uma vez que se extrapolam os problemas relacionados à tutela da intimidade individual, estabelecendo-se novo critério de base para a legalidade, o qual se refere às mudanças ocorridas principalmente por meio do censo alemão.

No ano de 1995, o desafio de tutelar a privacidade dos dados pessoais foi tratado de forma mais ampla, o que foi realizado pela publicação da Diretiva 95/46/CE do Parlamento Europeu, como tentativa de harmonizar as legislações da Europa sobre o tratamento de dados pessoais e a livre circulação destes (Maldonado; Blum, 2019). Contudo, apesar da aludida Diretiva, os países europeus possuíam leis distintas, a fim de tutelar o tema. Frente a isso, a União Europeia publicou, no ano de 2016, o Regulamento Geral de Proteção de Dados, uma legislação uníssona para todos os países do bloco, buscando unificar e reforçar a proteção de dados para todos os indivíduos no continente. Também, pela necessidade comercial econômica, diversos países que não possuíam legislação própria tiveram que se adequar ao regimento do colonizador, inclusive influenciando o legislador brasileiro na criação da LGPD que, além de garantir o direito à tutela estatal sobre as informações pessoais, faz com que o Estado se alinhe a *standarts*<sup>11</sup> internacionais referentes à matéria, possibilitando comercialização de diversos serviços e produtos (Pinheiro, 2019).

A LGPD brasileira foi promulgada no dia 14 de agosto de 2018, passando a vigorar somente em setembro de 2020, colocando o Estado brasileiro dentre aqueles que tutelam a proteção de dados por meio de legislação infraconstitucional (Brasil, 2018).

Todavia, frente ao mundo do *big data* e de um volume de dados jamais visto na história, no qual, em tempo algum, havia sido processo volume tão grande de informações por organizações privadas e públicas (Maldonado; Blum, 2019), se mostrou fundamental também um olhar mais crítico não somente por meio de uma legislação principiológica, conforme aponta Pinheiro (2019), como ainda, pela atualização de direitos fundamentais.

Dessa forma, em fevereiro de 2022, por meio da Emenda Constitucional 115/22, foi reconhecida a inserção do direito fundamental à proteção de dados pessoais na Constituição Federal, presente no artigo 5.º, inciso LXXIX.

Nesse sentido, destaca-se que o direito à privacidade se trata essencialmente de um direito fundamental, definição do Pós-positivismo, tanto de Dworkin (2011) quanto de Alexy (2008). A partir dessa definição, origina-se a ideia de proteção aos dados que surge como uma norma, decorrente do aprofundamento do direito fundamental à defesa e promoção da privacidade, sem que ocorra a perda da natureza de princípio. Nessa perspectiva, elevou-se o Brasil ao patamar de países que não só tutelam a privacidade dos dados pessoais por meio de instrumento infraconstitucional, como ainda reconhecem um direito fundamental à proteção de dados pessoais, conferindo ao cidadão proteção e notório reconhecimento da importância que o tema tem na sociedade da informação.

Portanto, tem-se que o assunto se configura em sua importância, sendo referenciado, no presente capítulo, por meio de uma tentativa célere de demonstrar a evolução da legislação que aborda a temática de proteção e privacidade dos dados pessoais de cada cidadão. Logo, com o intuito de adentrar mais no tema, o próximo capítulo abordará, de forma mais aprofundada, a norma brasileira – a LGPD – bem como conceituará o dado pessoal do indígena dentro dos limites normativos, para que, em última análise, no capítulo final, seja objetivamente demonstrada a necessidade de análise da auditoria, realizada na FUNAI, organização federal que tem como objetivo a proteção desse povo de cultura e história ímpares.

---

<sup>11</sup> Tradução livre: Padrões.

### 3. A LGPD E A SUA APLICAÇÃO AO TITULAR DE DADOS INDÍGENAS

O direito à privacidade e proteção dos dados pessoais, como já explorado no capítulo anterior, remonta ainda da década de 1890, entretanto o seu desenvolvimento se deu de forma mais concreta depois da segunda metade do século XX, principalmente após a Segunda Guerra Mundial, pela Declaração Universal de Direitos Humanos (UNICEF, 2022) e irresignação da sociedade com medidas governamentais que objetivavam mais a celeridade de processos administrativos do que a proteção das informações do cidadão em si, nos termos dos casos abordados acima.

Em continuidade, o presente capítulo procura classificar os dados pessoais da pessoa indígena nos termos da LGPD, para uma melhor proteção destes tanto pela necessidade imposta na Lei como pela importância e capacidade lesiva que o mal tratamento de dados dessa população pode causar para o seu modo de vida e patrimônio cultural e social. Também, sua finalidade é demonstrar a importância e relevância do Acórdão n. 1.384/2022 do TCU, ponto final e focal do presente estudo, para o tema da proteção dos dados dos povos indígenas.

Como dito, a LGPD é a versão brasileira do Regulamento Geral de Proteção de Dados Pessoais da Europa, uma legislação principiológica (Pinheiro, 2019), conceitual que estabelece regime jurídico para o tratamento de dados pessoais (Teixeira; Armelin, 2021).

Nesse sentido, primeiramente, é importante apontar que a LGPD dispõe sobre o tratamento de dados pessoais, inclusive em meio digital e, por conseguinte, em meios físicos, tanto por pessoa natural quanto jurídica, tendo como objetivo a proteção de direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da pessoa natural e sua personalidade, conforme artigo 1.º (Brasil, 2018).

Com o intuito de assegurar mais clara compreensão do que se aborda no presente trabalho, enfatiza-se, de acordo com artigo 5.º, inciso X da LGPD, que o tratamento de dados pessoais é caracterizado como qualquer “operação realizada com dados pessoais”, desde a coleta ao descarte, englobando classificação e transmissão por qualquer meio, bem como o arquivamento e a modificação dos dados pessoais etc.

Outrossim, é importante destacar os incisos VI, VII e IX também dos mesmos artigos, os quais se referem aos agentes de tratamento. O primeiro (VI) se trata do controlador, o qual pode ser “pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento dos dados pessoais”. Ou seja, é quem determina qual dado pessoal será coletado e a hipótese para que isso ocorra, dando a devida finalidade para cada informação que obtiver do sujeito, tendo também responsabilidades para que não ocorra situação de descumprimento dessas decisões ou incidentes de segurança da informação (Pinheiro, 2019).

No que se refere à figura do operador, inciso VII, esse pode ser “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. Em outras palavras, é a empresa ou a pessoa física escolhida pelo controlador para operar os dados coletados por este, de acordo com a finalidade também apontada pelo segundo, incorrendo em riscos de responsabilidade pelo descumprimento de qualquer finalidade previamente contratada (Pinheiro, 2019).

Porém, no mesmo artigo 5.º, um pouco mais acima, no inciso II, tem-se o conceito legal de

dados pessoais, sendo estes “a informação relacionada à pessoa natural identificada ou identificável”. Nesse ponto, a doutrina de Teixeira e Armelin (2021) notadamente acerta, ao ensinar que a Lei não está se referindo somente à pessoa natural identificada, mas também, à pessoa identificável, o que possibilita inúmeras interpretações a depender do caso concreto, estando todas sob a tutela da Lei.

Explica-se: é provável que o leitor tenha uma falsa interpretação que dados pessoais são somente aqueles diretos, como o nome e o número dos documentos pessoais. No entanto, alguns outros dados são capazes de identificar uma pessoa, dependendo do contexto e das circunstâncias em que estão inseridos, como a posição geográfica, por exemplo, que, a princípio, não é um dado pessoal, mas que, em determinado momento, pode levar à identificação de um indivíduo (Teixeira; Armelin, 2021). Inclusive, dependendo da pessoa que o posicionamento geográfico identificar, esse dado pode ser conceituado como de natureza sensível. Aliás, reza a lei:

Art. 5º Para os fins desta Lei, considera-se:

[...]

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Nesse sentido, explica-se que esses dados são denominados “sensíveis” por encontrarem, na LGPD, um tratamento diferenciado, com uma tutela mais rígida, devido ao seu alto grau de lesão em caso de incidentes de informação, no caso do presente estudo, principalmente, o vazamento de dados ou o desvio da finalidade da coleta. Ademais, os dados pessoais de natureza sensível demandam um maior rigor na coleta e no controle do tratamento, conforme apontado acima, fazendo com que a LGPD positive rol taxativo para que possam ser tratados, como ensinam Teixeira e Armelin (2021), o que é feito por meio do artigo 11 da referida Lei.

Ou seja, o referido artigo indica as bases legais para o tratamento dos dados pessoais de natureza sensível, da mesma forma que existem as hipóteses de tratamento para dados de natureza comum no artigo 7.º da LGPD (Brasil, 2018). Nessa perspectiva, qualquer que seja o dado pessoal de natureza sensível, este só poderá ser coletado e tratado quando devidamente fundamentado no inciso I ou nas alíneas do inciso II (Brasil, 2018).

No caso de sujeitos que sejam pertencentes a grupos de povos originários, seus dados comumente podem ser encaixados como dados pessoais de natureza ordinária, contudo é o que se reproduz, por meio inclusive da própria LGPD, ao possibilitar considerar-se dado pessoal, a depender do contexto, como dado pessoal de natureza sensível.

No caso do inciso I do referido dispositivo da LGPD, colacionado acima, fica claro que, no tratamento de dados pessoais de natureza sensível, é possível o titular de dados pessoais consinta o seu uso, de forma específica e destacada, para finalidades específicas (Brasil, 2018). Ou seja, quando determinado sujeito permitir que algum dado pessoal sensível seja tratado para determinada finalidade, sob hipótese alguma, este poderá ser desvinculado desse fim para uso em qualquer outro assunto senão aquele que permitiu que o agente de tratamento obtivesse tal informação do indivíduo (Teixeira; Armelin, 2021).

Entretanto, o inciso II do artigo 11 da LGPD deixa clara a possibilidade de que é possível

o tratamento de dados pessoais sem o consentimento, mas deve ser obedecida uma das hipóteses da alínea *a* até a alínea *g*. Em outras palavras, sem o consentimento se justifica a utilização desses dados pessoais pelo bem do próprio titular ou da coletividade, desde que essas informações sejam indispensáveis para isso (Teixeira; Armelin, 2021).

Dessa forma, considerando a natureza e a missão institucional da FUNAI – criada pela Lei n. 5.371, de 5 de dezembro de 1967 – ela se concretiza em proteger e promover os direitos dos povos indígenas no Brasil. A atuação dessa organização é orientada por diversos princípios, destacando-se o reconhecimento da organização social, os costumes, as línguas, crenças e tradições desses povos, buscando não somente a sua plena autonomia, mas também, a sua autodeterminação (FUNAI, 2020). Pode-se dizer que, quando a FUNAI estiver tratando dos dados pessoais do cidadão indígena, estará fazendo uso de dado pessoal de natureza sensível. Por conseguinte, deve proceder com cautela e em consonância com o artigo 11, inciso II, alíneas *b* e *c*, da LGPD, dependendo do contexto do tratamento, uma vez que as informações dos sujeitos dirão respeito ao contexto social no qual estão inseridos em suas comunidades e como pertencentes aos povos originários, nos termos do artigo 5.º, inciso II, da mesma legislação, pois são dados relacionados à origem racial ou étnica, convicção religiosa, de organização caráter religioso, filosófico ou político e genético (Brasil, 2018).

A hipótese, referente ao tratamento de dados pessoais pelo Poder Público para execução de políticas públicas, possui alto risco para os povos originários e o seu patrimônio. Nesse ponto, assinala-se, como exemplo, a situação ocorrida no Estado de São Paulo, onde foi promulgada a Lei n. 16.758, em 08 de junho de 2018, tornando obrigatória a informação sobre a cor ou a identificação racial em todos os cadastros, bancos de dados e registros de informações assemelhados, privados ou públicos no Estado (São Paulo, 2018). Segundo a idealizadora do Projeto de Lei, a Deputada Estadual Leci Brandão, tais dados serão coletados, os quais têm por finalidade a coleta para mapeamento do estado e a melhoraria das políticas públicas em regiões com maior concentração de pessoas negras. Entretanto, o risco existente é o de um possível vazamento de dados pessoais, o que geraria riscos incalculáveis para os titulares de dados, haja vista a possibilidade de discriminação por condição racial (Teixeira; Armelin, 2021).

Nesse cenário, com o olhar atento voltado ao indígena, pode-se citar problemáticas relacionadas a questões originárias, com o risco advindo de tratamento dos seus dados de forma errônea ou irresponsável, porque não somente o sujeito está à mercê dos danos, mas também, todo o seu modo de vida e cultura, além do seu espaço geográfico e direitos, como pertencente aos povos originários. Por exemplo, pode inclusive ser citado o vazamento de dados pessoais a respeito de determinada comunidade posicionada em região de interesse do garimpo ilegal. Ou seja, sendo de conhecimento dos invasores o número de pessoas e de possíveis ameaças para o seu negócio, são capazes de articular a invasão de terras indígenas, a fim de afastá-los de sua região para explorar o local, entre inúmeras outras possibilidades que poderão colocar em risco esse povo.

Aliás, conforme menciona Sérgio Amadeu da Silveira, alguns povos indígenas têm se mobilizado em defesa da governança de seus dados, convertendo o tema em verdadeira agenda de reivindicação política (Silveira, 2023):

‘Gida’ é uma palavra basca e significa guia. Em julho de 2019, foi realizado no

país Basco, na cidade de Oñati, um workshop para discutir os direitos dos povos indígenas. Uma das resoluções desse encontro foi a constituição da GIDA, the *Global Indigenous Data Alliance*, que pode ser traduzido em português como Aliança Global de Dados Indígenas. Estavam presente sete nações indígenas que consideraram necessário uma articulação internacional para disseminar leis, regulamentos e padrões coletivos de proteção e soberania de dados. A articulação se coloca como um guia da proteção e governança dos dados dos povos indígenas, uma vez que as leis ocidentais de proteção de dados são voltadas ao indivíduo. Um dos povos indígenas que integram a GIDA são os Māori, que vivem na atual Nova Zelândia. Para eles, os dados são recursos valiosos que “uma vez perdido o controle, é difícil recuperá-lo”. Dados coletados pelo seu povo, sobre seu povo e sobre os ambientes onde vivem são taonga, palavra maori que pode ser entendida como propriedade coletiva. Os Māori possuem uma rede de defesa da soberania de dados. A rede chamada Te Mana Raraunga reuni pesquisadores Māori e um dos seus slogans é ‘Nossos Dados, Nossa Soberania, Nosso Futuro’.

Um ponto interessante referido pelo autor diz respeito a estudo levado a efeito pela pesquisadora indígena Linda Tuhiwai Smit, que em 1999 publicou o livro *Decolonizing Methodologies: Research and indigenous people*. Nessa obra, a autora lançou “uma crítica a forma colonialista de pesquisar e de extrair informações das populações indígenas”.

Assim, segundo Silveira (2023):

O livro de Tuhiwai Smith teve boa repercussão e, se não trouxe a expressão soberania de dados em suas páginas, exibiu as bases para a crítica de como as informações quantificadas, os dados, podem discriminar, desvirtuar, descaracterizar a cultura e a cosmovisão dos povos. Também questionou se um pesquisador não-indígena teria o direito de extrair dados de um povo sem consultá-lo e sem dizer quais os objetivos, as finalidades das pesquisas. Essa crítica dos pesquisadores indígenas à supremacia epistemológica do neocolonialismo abria o caminho para soluções de enfrentamento e superação do problema. “Ao trabalhar para descolonizar os dados nos tempos modernos, o lugar para começar é a Soberania de Dados Indígenas” (ROBERTS; MONTOYA, 2022).

Portanto, fica o alerta e a preocupação com a segurança de dados, especialmente diante do impacto que o mau uso deles pode ocasionar aos povos tradicionais.

A esse propósito, ainda é pertinente fazer referência à pesquisa desenvolvida por Pedro Brandão, que culminou na publicação de valiosa obra, intitulada “Colonialidade do Poder, biodiversidade e direito”, onde o autor tratou de temas comumente afetos à biopirataria, apontado-a como a mais nova “descoberta do colonialismo”.

Discorrendo sobre a temática em ensaio homônimo ao seu livro, que foi publicado no site Outras palavras em novembro de 2023, o autor trouxe dados impressionantes e dignos de registro:

Para se ter uma ideia do que está em jogo nessa discussão e todos os potenciais interesses envolvidos, o Brasil é o país com a maior biodiversidade e sociobiodiversidade do mundo. São mais de 300 povos indígenas e inúmeras comunidades tradicionais que cultivam o conhecimento tradicional coletivo. De acordo com dados do Ministério do Meio Ambiente, o país abriga mais de 20% de todas as espécies da terra. Além do Brasil, países como México, China, Colômbia, Indonésia, Quênia, Peru, Venezuela, Equador, Índia, Costa Rica e África do Sul representam em torno de 70% da diversidade biológica global. São números inigualáveis, que nos colocam na posição de país mais megadiverso do mundo, de maneira que a biodiversidade se transforma num lugar de disputa central da economia política.

Por outro lado, a indústria farmacêutica e a indústria de sementes movimentam

bilhões de dólares. Nos Estados Unidos, de acordo com o Banco Mundial, somente o mercado de fármacos produzidos através da medicina tradicional rendeu mais de US\$ 32 bi, sendo que mais da metade dos remédios receitados no ocidente são produzidos a partir de florestas tropicais localizadas na região equatorial e no hemisfério Sul, enquanto três quartos das informações utilizadas na produção de medicamentos são derivadas dos conhecimentos tradicionais. Dados mais atualizados também apontam que o mercado de produtos biotecnológicos gira, no mundo, em torno de 500 bilhões de dólares e, no Brasil, aproximadamente US\$ 500 milhões.

Ainda, deixou assentado que “o uso da sociobiodiversidade por empresas capitalistas parece tratar de uma expropriação do conhecimento que, de um lado, o condena simplesmente ao lugar de pertencente ao passado; e, de outro, o valoriza apenas para a reprodução da visão mercantil”. Por conta disso, concluiu que,

Assim, o conhecimento comunitário está duplamente localizado na lógica da colonialidade do poder: ou pela sua negação completa, através do epistemicídio; ou pela sua validação somente vinculada à lógica do lucro, isto é, como um saber meramente instrumental ao mundo capitalista.

Para a ativista indiana Vandana Shiva, está em curso um novo projeto de colonização, concentrado na apropriação da natureza e dos conhecimentos tradicionais, que se materializa na concessão de patentes e nos direitos de propriedade intelectual. Seria o que ela denomina a “segunda chegada de Colombo”, já que “a biopirataria é a ‘descoberta’ de Colombo 500 anos depois de Colombo”. E “as patentes ainda são o meio de proteger essa pirataria da riqueza dos povos não-ocidentais como um direito das potências ocidentais” (Brandão, 2023).

Nessa perspectiva, a proteção dos dados dos povos indígenas diz diretamente com a preservação de suas terras, de sua cultura, de seu modo de vida e de sua própria existência. Além disso, “os dados retirados de um povo podem ser utilizados para submetê-lo e para explorá-lo, para encontrar seus pontos frágeis e quebrar suas resistências” (Silveira, 2023).

Em síntese, no presente capítulo, possibilitou-se ao leitor a análise de pontos determinantes para demonstrar a classificação dos dados pessoais sensíveis do indígena no contexto de políticas públicas, notadamente do que diz respeito àquelas desenvolvidas pela FUNAI, bem como o risco que pode advir de vazamento de dados pessoais e/ou da má condução dos processos internos para proteção da população indígena e do seu patrimônio cultural e social tal como originariamente é dentro das possibilidades atuais.

#### **4. ANÁLISE DO ACÓRDÃO N. 1.384/2022 DO TCU**

Nos capítulos anteriores, foram abordados temas, como o desenvolvimento da privacidade até a criação de legislações de proteção de dados pessoais que encontram maior eficácia e proteção com a criação de direito fundamental que aborda o assunto. Em continuidade, foram conceituados, por meio do texto da LGPD, o que são dados pessoais sensíveis e como os dados pessoais dos indígenas podem ser caracterizados de natureza sensível dentro das políticas públicas, na FUNAI.

No presente e último capítulo, será feita a análise da adequação da FUNAI à LGPD por meio do Acórdão n. 1.384/2022 do TCU, o qual tem por base a auditoria realizada na organização

da Administração Pública Federal, entre novembro de 2020 e maio de 2021, para avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio dos controles naquela época implementados na Fundação (Brasil, 2022).

Nesse sentido, conforme bem indica o relatório do referido acórdão, o Brasil, no ano de 2019, ocupou somente a 70.<sup>a</sup> posição do Índice Global de Cibersegurança que fora publicado pela União Internacional de Telecomunicações (Brasil, 2022).

Portanto, com a evidenciada necessidade de estimular a implantação de uma cultura de segurança da informação e proteção de dados pessoais nas entidades que fazem parte da Administração Pública Federal, o TCU conduziu auditoria, a qual teve como relator o Ministro Augusto Nardes, com o intuito de analisar a adequação de 382 organizações públicas federais à LGPD. A referida auditoria teve como propósito examinar as ações governamentais e os riscos à proteção de dados pessoais, utilizando um diagnóstico sobre os controles implementados nas organizações públicas federais (BRASIL, 2022).

O método empregado para a coleta de dados nas organizações foi o autoavaliativo, que ocorreu por meio de um questionário eletrônico, para que os gestores preenchessem as respostas que mais adequadamente representassem a situação da respectiva organização em relação aos controles relacionados à LGPD. Tal método fora composto por 60 questões, organizadas em duas diferentes perspectivas, em nove dimensões (Brasil, 2022), bastante semelhante ao Sistema de Gestão da Informação do ISO 27.001, bem como dos campos de adequação presentes na obra de Maldonado e Blum (2019).

Das 60 questões assinaladas, foi separado um subconjunto de 42 destas para compor um indicador elaborado, visando a resumir as respostas fornecidas por cada organização. Esse indicador considerou possíveis respostas de cada questão, atribuindo nota para cada uma delas. Dessa forma, as respostas indicadas são dadas em uma palavra, quais sejam, “Sim”, “Parcialmente” e “Não”, sendo para elas atribuídas as notas 1, 0,5 e 0, respectivamente. A nota da organização é a resposta e a soma de todas as perguntas, divididas por 42 (Brasil, 2022).

Com os valores do indicador, foi possível definir quatro níveis de adequação à LGPD, o que permite classificar cada organização de acordo com a sua harmonização com a Lei. O primeiro nível de adequação é mais baixo, o “Inexpressivo”, com indicador menor ou igual a 0,015; o segundo nível, o “Inicial”, serve para classificação com nota acima de 0,15 e menor ou igual a 0,5; o terceiro nível, o “Intermediário”, é conferido à organização que tenha obtido coeficiente maior do que 0,5 e menor ou igual a 0,8; e o quarto nível, o “Aprimorado”, fora dado para a organização que demonstrou melhor adequação a Lei, por meio dos indicadores, quando o resultado final apontou a média acima de 0,8 (Brasil, 2022).

Em números gerais, apenas 2,9% das organizações puderam ser classificadas com o nível mais alto, o “Aprimorado, sendo um total de apenas 11. No nível “Intermediário”, os resultados apontaram que, nesse patamar, existem 78 entidades, ou seja, 20,4% das 382. Seguindo, existem 225 das 382 organizações que estão em um nível “Inicial” de adequação à LGPD, perfazendo 58,9% do total das entidades. Contudo, talvez o mais alarmante – dada a situação da complexidade, sensibilidade e risco aos dados pessoais tratados por entidades públicas – é a condição da entidade que alçou nota suficiente para ser enquadrada em qualquer outro indicador que não fosse o

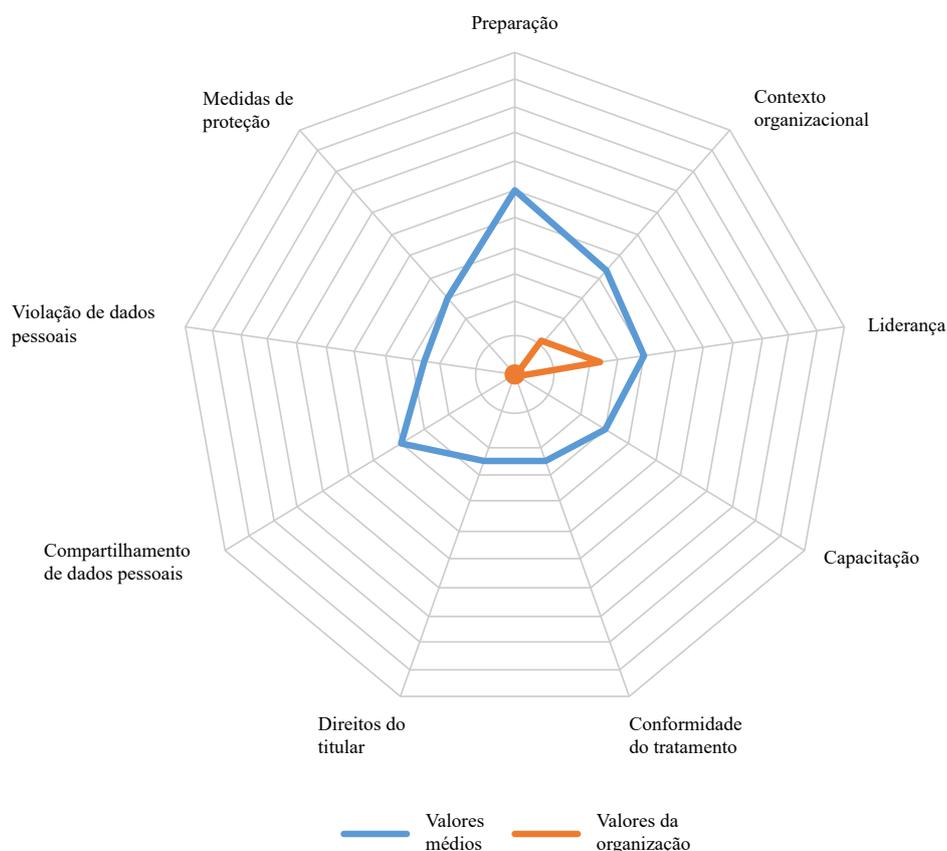
“Inexpressivo”, no qual estão 68 delas, isto é, 17,8% do total (Brasil, 2022).

Enfatiza-se que o número de organizações em situação de adequação “Inexpressivo” é mais de seis vezes superior ao das entidades em estágio “Aprimorado”. Em síntese, isto significa que organizações, vinculadas à Administração Pública, estão com os seus processos de harmonização com a LGPD atrasados, ainda mais quando considerado que a Lei entrou em vigor dois anos após a sua publicação (Teixeira; Armelin, 2021), bem como por possuir capítulo exclusivamente dedicado ao tratamento de dados pessoais pelo setor público, positivado dos artigos 23 ao 32 da referida norma (Brasil, 2018).

Após o questionário ter sido respondido pela chefia da FUNAI, bem como suas respostas terem sido devidamente analisadas por meios dos indicadores e questões pertinentes para obtenção do coeficiente da Organização à legislação, constatou-se que a FUNAI obteve o valor de 0,04 para indicar a sua adequação total à LGPD correspondente ao nível “Inexpressivo” (Brasil, 2022).

Nesse sentido, de acordo com o Gráfico abaixo, retirado do Acórdão n. 1.384/2022 do TCU, é possível comparar os indicadores em cada dimensão que foram calculados para FUNAI, comparado aos valores médios, calculados em conjunto das 382 organizações públicas federais avaliadas, da seguinte forma.

Gráfico: Comparação dos indicadores em cada dimensão, calculados para a FUNAI, em comparação com as 382 organizações públicas federais avaliadas:



Fonte: TCU (2022, p. 112)

Nesse sentido, explicando o gráfico supra, nas duas questões relacionadas à dimensão de

“Preparação”, a FUNAI não pontuou, pois, na época da auditora, não havia sido conduzido nenhum ato de iniciativa para adequar ou elaborar plano de adequação. Em relação ao vetor “Contexto Organizacional”, concernente à revisão e identificação de normativas correlatas à proteção de dados pessoais, a entidade pontuou em apenas um quesito do total de nove (Brasil, 2022).

Já no que se refere ao vetor “Liderança”, que também possui nove questões respondidas pela Organização, a FUNAI pontuou, de forma máxima, ou seja, 1 ponto, em apenas dois quesitos, visto que, na época, possuía Política de Segurança da Informação ou instrumento interno correlato, bem como já havia nomeado o seu encarregado para o tratamento de dados pessoais nos termos do artigo 42, § 2.º da LGPD, porém não o havia publicizado de acordo com o que está positivado na norma (Brasil, 2022).

Em relação aos vetores “Conformidade do Tratamento”, “Capacitação”, “Direitos do Titular”, “Compartilhamento de Dados Pessoais”, “Violação de Dados Pessoais” e “Medidas de Proteção”, a Organização obteve um total de zero pontos (Brasil, 2022).

Dessa forma, pelos resultados obtidos, é possível ver que estatisticamente – e em termos legais da LGPD – a FUNAI ficou abaixo de outras organizações da Administração Pública Federal auditadas quanto à adequação à LGPD, eis que ocupa posição no indicador “Inexpressivo”, com poucas ações, inclusive iniciais, com a intensão de se adequar à referida norma.

Consequentemente, os dados da população indígena, tratados pela FUNAI, podem estar em risco, em razão do seu nível de proteção implementado, ainda mais considerado com o alto grau de risco de dano à parcela indicada da população em caso de incidentes de segurança da informação, notadamente aqueles que possuem intenção maliciosa sobre bens da cultura e sociedade dos povos originários, como terras, por exemplo.

Entretanto, uma ressalva deve ser feita, visto que, segundo o Sistema de Gestão de Segurança da Informação, inclusive bem desenhado pela doutrina (Maldonado; Blum, 2019), presente inclusive em guias mais práticos (Donda, 2020), percebe-se que existem informações conflitantes nos resultados obtidos na auditoria realizada na FUNAI. Isto posto, frisa-se que as entidades receberam as questões para que respondessem, mas há somente orientação redigida, sem um especialista para melhor respondê-las.

Ainda, outro ponto conflitante existente é que, na época, esse Órgão possuía um encarregado nos termos legais, porém não indicado no sítio eletrônico da organização, evidenciando-se, assim, importantes passos para a adequação. Ademais, há resposta positiva no que diz respeito à existência de Política de Segurança da Informação, embora não haja nenhuma outra espécie de normativa interna, a fim de assegurar a confidencialidade, integridade e disponibilidade dos dados.

Também, apontam-se alguns aspectos, como o fato de a gerência ter respondido como “Não se Aplica” à pergunta sobre revisão de contratos com operadores ou avaliação, se havia controladores conjuntos, o que demonstra, na verdade, maior desconhecimento da norma, o que pode influenciar as respostas no sentido negativo, ou pelo fato de a LGPD ter entrado em vigor sem que fosse difundida de forma eficaz, com mais informações a respeito dela, o que inclusive abrindo espaço para tecer algumas críticas.

Com efeito, atualmente (julho de 2024) ainda se observa da página *online*<sup>12</sup> da FUNAI, que não houve a aplicação de melhorias/avanços quanto a uma adequação mais assertiva à Lei Geral de Proteção de Dados, visto que somente consta acesso à decisão do TCU, ora estudada, e acesso à informação de contato e como contatar a Encarregada de proteção de dados da entidade, essa recentemente atualizada em 21 de junho de 2024.

Todavia, mesmo que *per si* não se demonstre grandes avanços de conformidade com a Lei por esses aspectos, no mínimo evidencia certa transparência ao titular de dados interessado em obter informações quanto ao tratamento desses pelo órgão, contudo permanece latente a necessidade de rápida e efetiva medida de *compliance* à LGPD por parte da FUNAI, que desde 2022 foi sinalizada sua inexpressividade perante citada norma.

## 5. CONSIDERAÇÕES FINAIS

Pode-se constatar, a partir do exposto, que o direito à privacidade teve seus primeiros esboços ainda na década de 1890. No entanto, foi após o término da Segunda Guerra Mundial, por meio da Declaração Universal dos Direitos Humanos de 1948, que o tema ganhou notória importância no cenário internacional.

No decorrer das décadas seguintes, ainda no século XX, ocorreram irresignações populares em diferentes países frente as medidas administrativas relacionadas ao tratamento de dados pessoais por parte do Estado, o que permitiu o surgimento dos primeiros direitos internos que trataram da privacidade de dados pessoais.

Nesse contexto, no âmbito da Europa, a partir da evolução tecnológica, com a popularização de sistemas de processamento de dados informatizados, iniciado na década de 1970, concretizou-se a Diretiva 95/46/CE do Parlamento Europeu que, mais tarde, auxilia na criação do Regulamento Geral de Proteção de Dados e uniformiza o tema naquele bloco econômico. Essa legislação serviu de modelo para a LGPD brasileira que ganha mais importância por meio do direito fundamental à proteção de dados pessoais, anexado à Constituição Federal de 1988.

Ainda, foram abordados termos da LGPD, necessários para a melhor compreensão da Lei brasileira aplicada à FUNAI, sem desconsiderar a natureza de dados pessoais sensíveis do sujeito indígena que são tratados na Instituição, inclusive, por meio dos riscos à população originária em caso de incidentes de segurança da informação.

Ao final do trabalho, foi analisado o Acórdão n. 1.384/2022 do TCU. Nesse ponto, foi observado que a FUNAI, na época da auditoria, possuía nível “Inexpressivo” de adequação à LGPD, pois obteve nota equivalente a 0,04. Foi possível, entretanto, constatar que ela não é a única organização nesse patamar e que provavelmente o resultado da pesquisa poderia ter sido, em parte, diferente, haja vista que faltou conhecimento por parte da gerência da referida Instituição sobre a norma, o que gerou conflito de respostas nos questionários. Em se tratando dos resultados baixos, percebidos na pesquisa, é possível direcionar a atuação da FUNAI para suprimir esses espaços inexistentes de aplicação da LGPD na organização. Assim, por se tratar também de legislação

<sup>12</sup> GOVERNO FEDERAL. Fundação Nacional do Índio. Política de privacidade e proteção de dados. Disponível em: <https://www.gov.br/funai/pt-br/acesso-a-informacao/privacidade-e-protecao-de-dados-1>. Acesso em: 27 ago. 2024.

recente, o resultado inicial servirá de comparativo para uma próxima avaliação, bem como de guia dos pontos a serem melhorados.

## REFERÊNCIAS

ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiro, 2008.

BRANDÃO, Pedro. Colonialidade do poder, biodiversidade e Direito. Outras palavras. 11 nov. 2023. Disponível em: <https://outraspalavras.net/descolonizacoes/colonialidade-do-poder-biodiversidade-e-direito/>. Acesso em 17 jul. 2024.

BRANDÃO, Pedro. Colonialidade do Poder, Biodiversidade e Direito. 2024.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 25 ago. 2023.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 14 agosto 2018. 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: 1 ago. 2023.

BRASIL. Lei n.º 5.371, de 5 de dezembro de 1967. Autoriza a instituição da "Fundação Nacional do Índio" e dá outras providências. Diário Oficial da União, Brasília, DF, 5 de dezembro de 1967. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/1950-1969/15371.htm](http://www.planalto.gov.br/ccivil_03/leis/1950-1969/15371.htm). Acesso em: 27 ago. 2023.

BRASIL. Tribunal de Contas da União. Auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. Acórdão 1.384/2022-TCU-Plenário de relatoria do Ministro Augusto Nardes. Relatório de Feedback, 2022. Disponível em: [https://www.gov.br/mcom/pt-br/aceso-a-informacao/transparencia-e-prestacao-de-contas/privacidade-e-protecao-de-dados-pessoais/2022\\_relatoriofeedback\\_tcu-mcom.pdf](https://www.gov.br/mcom/pt-br/aceso-a-informacao/transparencia-e-prestacao-de-contas/privacidade-e-protecao-de-dados-pessoais/2022_relatoriofeedback_tcu-mcom.pdf). Acesso em: 4 ago. 2023.

DONDA, Danilo. Guia prático de implementação da LGPD: conheça estratégias e soluções para adequar sua empresa em conformidade com a Lei. São Paulo: Labrador, 2020.

DONEDA, Danilo. Da privacidade à proteção de dados: fundamentos da Lei Geral de Proteção de Dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters, E-book. 2019.

DWORKIN, Ronald. Levando os direitos a sério. Tradução de Nelson Boeira. São Paulo: Martins Fontes, 2011.

FRANÇA. Lei n.º 78-17, de 6 de janeiro de 1978. Relative à l'informatique, aux fichiers et aux libertés. Légifrance, République Française. Disponível em: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vig>. Acesso em: 25 ago. 2023.

FUNDAÇÃO NACIONAL DOS POVOS INDÍGENAS (FUNAI). Atualização de 27 de novembro,

2020. Disponível em: <https://www.gov.br/funai/pt-br/aceso-a-informacao/institucional/Institucional>. Acesso em: 27 ago. 2023.

LIMBERGER, Têmis. A Informática e a Proteção à Intimidade. *Revista de Direito Constitucional e Internacional*, São Paulo, pp. 110-124, out./dez. 2000.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). *Lei Geral de Proteção de Dados Comentada*. São Paulo: Thomson Reuters Brasil, E-book. 2019.

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (Coords.). *Direito inovação e tecnologia*. São Paulo: Saraiva, v.1, 2015.

ORWELL, George. 1984. São Paulo: Companhia das Letras, 2009.

PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. *Revista dos Tribunais*, São Paulo, v. 1000, pp. 309-323, fev. 2019. Disponível em: [https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/186011/2021\\_pinheiro\\_patricia\\_nova\\_lgpd.pdf?sequence=1&isAllowed=y](https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/186011/2021_pinheiro_patricia_nova_lgpd.pdf?sequence=1&isAllowed=y). Acesso em: 24 ago. 2023.

RODATA, Stefano. *A Vida na sociedade da vigilância: A privacidade hoje*. Tradução de Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTOS, Sílvio Coelho dos. Direitos humanos e os direitos dos povos indígenas. *Revista de Antropologia Ilha da Universidade Federal de Santa Catarina, Florianópolis*, v. 7, n. 1, 2, p. 73-82, jan. 2005. Disponível em: <https://periodicos.ufsc.br/index.php/ilha/article/view/1561/1357>. Acesso em: 26 ago. 2023.

SÃO PAULO. Lei n.º 16.758, em 08 de junho de 2018. Projeto de Lei n.º 304, de 2012, da Deputada Leci Brandão Â- Pcdob. Assembleia Legislativa do Estado de São Paulo. São Paulo Legislação, SP, 8 de junho, 2018. Disponível em: <https://www.al.sp.gov.br/repositorio/legislacao/lei/2018/lei-16758-08.06.2018.html>. Acesso em: 27 ago. 2023.

SILVEIRA, S. A. Soberania de dados indígenas. *A Terra é redonda*. 18 nov. 2023. Disponível em: <https://aterraeredonda.com.br/soberania-de-dados-indigenas/>. Acesso em: 17 jul. 2024.

TEIXEIRA, Tarciso; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei geral de proteção de dados pessoais: Comentada artigo por artigo*. 3 ed. rev., atual. e ampl. Salvador: JusPodvim, 2021.

UNIÃO EUROPEIA. Directiva 46 do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Relativa à Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Bruxelas: Disponível em: <https://eur-lex.europa.eu/eli/dir/1995/46/oj>. Acesso em: 19 mai. 2023.

UNICEF BRASIL. *Declaração Universal dos Direitos Humanos*. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. 8 de agosto de 2022. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 25 ago. 2023.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review*, [s.l.], v.

4, pp. 2303-2312, 15 Dec. 1890. Disponível em: [http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy\\_brand\\_warr2.html](http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html). Acesso em: 24 jun. 2023.

Recebido em: 24.06.2024

Aprovado em: 05.07.2024

Última versão dos autores: 26.07.2024

#### **Informações adicionais e declarações dos autores (Integridade Científica)**

**Declaração de conflito de interesses:** os autores confirmaram que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de originalidade:** os autores garantiram que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; também atestam que não há plágio de terceiros ou autoplágio.

#### **Como citar (ABNT Brasil):**

Prestes, F. P.; Ribeiro Preve, D.; Teza de Bona, M. Controles de proteção de dados pessoais dos povos indígenas implementados na FUNAI: uma análise do Acórdão n. 1.384/2022 do Tribunal de Contas da União. *JURIS - Revista Da Faculdade De Direito*, 34 (1). <https://doi.org/10.14295/juris.v34i1.17613>



Os artigos publicados na Revista Juris estão licenciados sob a Licença Creative Commons Attribution 4.0 International (CC BY 4.0)