INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM DIREITO
MESTRADO EM DIREITO CONSTITUCIONAL

IZABELLY KAROLINE ROMÃO SANTOS

O TRIBUNAL DE CONTAS DA UNIÃO E A LGPD: ESTUDO DE CASO CRÍTICO SOBRE A AUDITORIA DO ACÓRDÃO 1384/2022

BRASÍLIA
2025

IZABELLY KAROLINE ROMÃO SANTOS

O TRIBUNAL DE CONTAS DA UNIÃO E A LGPD: ESTUDO DE CASO CRÍTICO SOBRE A AUDITORIA DO ACÓRDÃO 1384/2022

Dissertação de Mestrado, desenvolvida sob a orientação da Prof.ª Dra. Clara da Mota Santos Pimenta Alves, apresentada para obtenção do título de Mestre em Direito.

BRASÍLIA
2025

Código de catalogação na publicação – CIP

S237t Santos, Izabelly Karoline Romão

O Tribunal de Contas da União e a LGPD: estudo de caso crítico sobre a auditoria do acórdão 1384/2022 / Izabelly Karoline Romão Santos. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2025.

96 f. : il.

Orientador: Profa. Dra. Clara da Mota Santos Pimenta Alves.

Dissertação (Mestrado em Direito Constitucional) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Dados pessoais. 2. Consentimento (segurança da informação). 3. Tratamento dos dados pessoais. I.Título

CDDir 341.2738

Elaborada por Natália Bianca Mascarenhas Puricelli – CRB 1/3439

IZABELLY KAROLINE ROMÃO SANTOS

O TRIBUNAL DE CONTAS DA UNIÃO E A LGPD: ESTUDO DE CASO CRÍTICO SOBRE A AUDITORIA DO ACÓRDÃO 1384/2022

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação Stricto Sensu em Direito Constitucional do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), como requisito final para a obtenção do título de Mestre em Direito Constitucional.

Data da Defesa: 01/07/2025

BANCA EXAMINADORA

_____

Profa. Dra. Clara da Mota Santos Pimenta Alves
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP

_____

Profa. Dra. Tainá Aguiar Junquilho
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP

_____

Prof. Dr. Ricardo Schneider Rodrigues
Centro Universitário Cesmac

DEDICATÓRIA

Dedico esta dissertação a Deus, fonte inesgotável de sabedoria, por me sustentar em cada etapa desta jornada e por me ensinar, em sua Palavra, o valor da perseverança e do propósito. À minha própria jornada, por me ensinar a seguir em frente mesmo quando o caminho parecia incerto e difícil.

À minha família — meus pais e minha irmã — que são meu alicerce, minha segurança e minha inspiração constante. Obrigada por acreditarem em mim, apoiarem cada escolha e celebrarem cada conquista. Essa vitória é, verdadeiramente, nossa.

Ao Professor Ricardo Schneider, cuja visão e generosidade acadêmica abriram portas e iluminaram caminhos desde os primeiros passos da minha trajetória. Primeiro, como orientador do meu projeto de iniciação científica na graduação, foi quem me apresentou aos estudos sobre os Tribunais de Contas. Sua confiança foi essencial para que eu escolhesse o mestrado e definisse, com segurança, o tema que hoje me orgulho em defender.

À minha orientadora, Prof.ª Clara da Mota, por reconhecer o valor deste trabalho desde o início. Obrigada por acreditar em mim, por me incentivar a tratá-lo como prioridade, por compreender os momentos de silêncio e, ainda assim, nunca deixar de me cobrar com firmeza e generosidade. Sua orientação foi fundamental para que eu seguisse em frente com confiança.

E, por fim, às inúmeras instituições e profissionais que me acolheram ao longo da pesquisa. Cada contribuição foi essencial para que este trabalho se tornasse real e relevante.

RESUMO:

A transformação digital da administração pública alterou a forma de tratamento dos dados pessoais, essa mudança ampliou os riscos relacionados à privacidade, como manipulação de informações, fraudes, violações à autonomia individual e ameaças à democracia. Nesse cenário, a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um avanço normativo importante ao estabelecer obrigações específicas ao setor público. Entretanto, o aumento dos incidentes de segurança envolvendo dados pessoais evidencia fragilidades na implementação efetiva da lei. Diante disso, a pergunta que orienta esta pesquisa é: existem limitações e oportunidades de melhoria na auditoria realizada pelo Tribunal de Contas da União (TCU) para a fiscalização da implementação da LGPD nos órgãos públicos federais? Parte-se da hipótese de que a metodologia adotada pelo TCU, especialmente na auditoria que resultou no Acórdão nº 1384/2022, possui um caráter mais preliminar e de sensibilização, não abrangendo plenamente a complexidade e os desafios da proteção de dados pessoais no setor público. O objetivo principal é analisar criticamente essa atuação, identificando contribuições e pontos que podem ser aprimorados para fortalecer a governança e a segurança das informações. Os objetivos específicos incluem: examinar os requisitos da LGPD aplicáveis ao setor público; contextualizar os tipos e limites das auditorias do TCU; analisar o conteúdo da auditoria em questão para identificar lacunas e oportunidades de melhorias. A pesquisa concluiu que a auditoria do TCU possui limitações que comprometem uma fiscalização aprofundada.

Palavras-chave: LGPD; Tribunais de Contas; Setor Público; Fiscalização

ABSTRACT:

La transformación digital de la administración pública ha cambiado la forma de tratamiento de los datos personales; este cambio ha ampliado los riesgos relacionados con la privacidad, tales como la manipulación de información, fraudes, violaciones a la autonomía individual y amenazas a la democracia. En este escenario, la promulgación de la Ley General de Protección de Datos Personales (LGPD) representó un avance normativo importante al establecer obligaciones específicas para el sector público. Sin embargo, el aumento de incidentes de seguridad que involucran datos personales evidencia fragilidades en la implementación efectiva de la ley. Ante esto, la pregunta que orienta esta investigación es: ¿existen limitaciones y oportunidades de mejora en la auditoría realizada por el Tribunal de Cuentas de la Unión (TCU) para la fiscalización de la implementación de la LGPD en los órganos públicos federales? Se parte de la hipótesis de que la metodología adoptada por el TCU, especialmente en la auditoría que resultó en la Resolución nº 1384/2022, posee un carácter más preliminar y de sensibilización, sin abarcar plenamente la complejidad y los desafíos de la protección de datos personales en el sector público. El objetivo principal es analizar críticamente esta actuación, identificando contribuciones y puntos que pueden ser mejorados para fortalecer la gobernanza y la seguridad de la información. Los objetivos específicos incluyen: examinar los requisitos de la LGPD aplicables al sector público; contextualizar los tipos y límites de las auditorías del TCU; analizar el contenido de la auditoría en cuestión para identificar vacíos y oportunidades de mejora. La investigación concluyó que la auditoría del TCU posee limitaciones que comprometen una fiscalización profunda.

Palavras-chave: LGPD; Tribunales de Cuentas; Sector Público; Fiscalización

SUMÁRIO:

INTRODUÇÃO

A discussão jurídica sobre a privacidade começou a ganhar destaque a partir de 1890, quando Louis D. Brandeis e Samuel D. Warren publicaram, na revista *Harvard Law Review*, o artigo "The Right to Privacy". Considerado um marco na história do direito, o texto denunciava que os avanços tecnológicos da época, especialmente a popularização da fotografia e o crescimento da imprensa sensacionalista, estavam permitindo novas formas de invasão da vida privada. Os autores argumentam que tais inovações, combinadas com métodos de negócios cada vez mais agressivos, tornavam obsoleta a proteção tradicional da honra e da reputação, exigindo o reconhecimento de um novo direito: o direito de ser deixado em paz (*the right to be let alone*).

O artigo de Brandeis e Warren é particularmente relevante para compreender as origens do debate contemporâneo sobre a proteção de dados pessoais. Já no final do século XIX, os autores advertiam que o Estado e o direito precisavam evoluir para proteger os indivíduos diante das novas ameaças à sua intimidade, mesmo quando não houvesse prejuízo material ou ofensa à honra pública. Essa concepção inovadora plantou as bases para o desenvolvimento do direito à privacidade como um direito autônomo, que viria a ser reconhecido e ampliado ao longo do século XX e, mais recentemente, consolidado como fundamento da proteção de dados pessoais em legislações como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil.

Em 1948, no contexto da reconstrução global após a Segunda Guerra Mundial, surgiram os primeiros compromissos internacionais voltados à proteção da esfera privada do indivíduo, com a previsão expressa desse princípio no artigo 12 da Declaração Universal dos Direitos Humanos. Esse marco inaugurou uma nova fase na relação entre o ser humano e o tratamento de suas informações pessoais, contribuindo para a formação de um entendimento ético e jurídico.

Danilo Doneda (2019) destaca, em sua obra, três casos emblemáticos que evidenciam a importância da proteção dos dados pessoais, ressaltando o clamor da sociedade por respostas diante de possíveis abusos. Entre esses, sobressai o caso alemão, considerado pioneiro no mundo, que teve início na década de 1970 com a regulamentação do estado de Hassen, voltada inicialmente para dados públicos informatizados. Essa legislação foi

posteriormente substituída pela *Bundesdatenschutzgesetz*, ampliando a proteção aos dados pessoais. A necessidade de revisão da norma surgiu em razão do censo demográfico planejado para 1983, que visava coletar informações pessoais além da simples contagem populacional, provocando forte reação social. A Corte Federal da Alemanha suspendeu temporariamente o censo com base nos princípios constitucionais de proteção à privacidade, autorizando sua continuidade apenas mediante a adoção de medidas para resguardar os dados, como a proibição de compartilhamento de nomes e endereços com outros órgãos públicos.

Naquele período, o romance 1984, de George Orwell, já amplamente difundido, influenciava a percepção pública acerca dos perigos da vigilância estatal e do controle absoluto sobre a vida privada, ao retratar uma sociedade distópica dominada pelo Estado. Nesse cenário, a população vive sob vigilância constante, exercida pelo onipresente "Grande Irmão", que monitora não apenas os espaços públicos, mas também a privacidade nos lares, por meio dos dispositivos conhecidos como "teletelas". A obra evidencia a manipulação e o controle das informações pessoais como ferramentas essenciais para a manutenção do poder estatal, projetando um futuro no qual a privacidade praticamente não existe.

Segundo Souza e Acha (2022), normas atinentes à proteção de dados são uma maneira de proteger a pessoa humana, tendo em vista que os dados pessoais representam algum atributo de uma pessoa, logo, mantém uma ligação concreta com a pessoa titular destes dados, podendo ser considerados uma extensão de sua personalidade, e por isso merecem um tratamento apropriado.

No Brasil, a temática foi regulamentada através da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018), que é aplicável a qualquer tratamento de dados pessoais, realizado por pessoa natural ou jurídica, de direito público ou privado. O presente estudo tem como foco a aplicação dessa lei no âmbito do setor público, conforme disciplinado no Capítulo IV da referida legislação.

É importante destacar que, com a Estratégia Nacional do Governo Digital, instituída pela Lei nº 14.129/2021 e pelo Decreto nº 12.069/2024, iniciou-se um movimento de modernização dos procedimentos realizados pelo poder público no atendimento à população, com a ampliação do uso de serviços digitais. O que antes era controlado de forma física passa a ser realizado também no ambiente virtual, o que intensifica os desafios relacionados à proteção de dados pessoais. No entanto, a necessidade de proteção de dados pelo setor público é anterior e independe do meio utilizado, a digitalização apenas torna ainda mais urgente a sua

efetiva implementação. Sendo assim, não há que se falar em proteção de dados pessoais se o setor público for excluído da adequação.

O volume crescente de informações circulando no ambiente digital afeta diretamente a proteção da privacidade. A coleta e o compartilhamento descontrolado de dados pessoais criam cenários nos quais indivíduos passam a ser alvo de formas sofisticadas de vigilância. No âmbito privado, por sua vez, as empresas utilizam essas informações para desenvolver estratégias comerciais que buscam influenciar comportamentos e maximizar resultados publicitários. Além das finalidades econômicas, a ampla exposição de dados também facilita a atuação de terceiros com interesses ilícitos, ampliando os riscos de uso abusivo das informações.

Embora a proteção de dados pessoais tenha emergido, historicamente, como uma resposta à vigilância estatal e à perseguição de minorias especialmente no contexto das ditaduras do século XX na Europa, é importante reconhecer que, no Brasil, os primeiros marcos legais sobre o tema surgiram na esfera privada, ligados à proteção do consumidor.

O Código de Defesa do Consumidor, por exemplo, já previa o tratamento de dados pessoais por fornecedores e impunha sanções a condutas abusivas, mesmo sem utilizar a expressão "proteção de dados". Nesse cenário, a preocupação central estava voltada à assimetria entre consumidores e empresas, especialmente diante da crescente digitalização das relações de consumo.

SILVA et al. (2021) ressaltam que os consumidores frequentemente enfrentam uma situação de fragilidade diante das empresas, principalmente no ambiente digital, onde a coleta inadequada de dados é facilitada pela pouca familiaridade dos usuários com as práticas adotadas. Os autores trouxeram como exemplo claro dessa realidade o hábito de aceitar termos e condições clicando em “Li e Aceito os Termos”, sem que haja uma leitura detalhada ou entendimento das obrigações e permissões ali contidas. A economia, em grande parte, depende da vigilância intensa e constante dos dados pessoais, que são tratados como um recurso estratégico, o que acaba fragilizando a proteção da privacidade individual.

No entanto, quando se trata da esfera pública, a lógica se altera significativamente. Aqui, não se trata apenas de equilíbrio contratual, mas da efetivação de um direito fundamental, cuja tutela é obrigação direta do Estado. O tratamento de dados por órgãos e entidades governamentais exige não apenas a observância dos princípios da LGPD, mas também o cumprimento de deveres institucionais de transparência, segurança, finalidade e

governança. Nesse contexto, a atuação estatal deve ser pautada por mecanismos formais e estruturados de proteção, uma vez que envolve a confiança do cidadão na administração pública e no uso adequado de suas informações pessoais.

A era do desenvolvimento tecnológico destaca a relevância dos dados pessoais e da privacidade, especialmente com a implementação da Lei nº 13.709/2018 e o aumento substancial dos ataques cibernéticos direcionados a bancos de dados. Quando se trata do manuseio de informações pessoais por órgãos governamentais, torna-se essencial a observância de diretrizes legais, procedimentos administrativos, medidas de segurança e governança. Isso se deve ao fato de que é um direito fundamental dos titulares de dados terem sua privacidade devidamente garantida.

Conforme a sociedade da informação avança, um fenômeno notável emerge: as ferramentas tecnológicas estão se tornando cada vez mais acessíveis e econômicas para um número cada vez maior de pessoas. Esse avanço tecnológico tem conduzido a uma disseminação generalizada de dados em uma escala nunca antes vista. No entanto, nesse ambiente de alta conectividade e compartilhamento constante, surge uma preocupação crescente em relação à possibilidade de violações dos direitos individuais, especialmente no que diz respeito à invasão da intimidade e da privacidade de outras pessoas. Esse receio é agravado pelo fato de que muitas vezes não há clareza suficiente sobre a natureza e a extensão das informações que são controladas por terceiros, conforme exposto por Manna Bellasalma et al. (2024).

Nos últimos anos, tornou-se cada vez mais comum observar notícias sobre grandes vazamentos de dados na esfera pública, muitas vezes resultantes de ataques de hackers. Esses incidentes revelam a vulnerabilidade de sistemas de informações governamentais e geram preocupações sobre a segurança de dados sensíveis dos cidadãos.

Para obter uma visão quantitativa da situação, foi realizada uma consulta ao site do CTIR Gov – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. Na seção intitulada “CTIR Gov em Números”, iniciativa criada com o objetivo de disponibilizar estatísticas gerais de interesse público relacionadas a incidentes cibernéticos que afetam órgãos e entidades da administração pública, é possível acessar dados consolidados sobre a frequência, a tipologia e a evolução desses incidentes ao longo do tempo (BRASIL, 2025).

A pesquisa qualitativa sobre os incidentes de segurança cibernética registrados em órgãos públicos brasileiros no ano de 2025 revela um cenário preocupante: foram contabilizados 1.994 vulnerabilidades e 4.859 incidentes, totalizando 6.853 registros relacionados a problemas de segurança da informação. Esse volume expressivo evidencia o aumento das ameaças e fragilidades nos sistemas governamentais, reforçando a necessidade de investimentos em prevenção e resposta a incidentes.

É importante, após a apresentação dos dados, esclarecer a diferença entre vulnerabilidades e incidentes de segurança da informação. As vulnerabilidades correspondem a fragilidades identificadas nos sistemas, com caráter preventivo, servindo como alerta para adoção de medidas corretivas antes que ocorram danos (BRASIL, 2025). Já os incidentes são eventos adversos, confirmados ou suspeitos, que indicam uma violação em curso ou já materializada na segurança dos sistemas ou redes (BRASIL, 2025). Enquanto as vulnerabilidades sinalizam potenciais riscos, os incidentes representam a efetiva ocorrência de problemas que exigem resposta imediata.

Ao analisar a natureza dos incidentes, observa-se que o vazamento de dados foi a ocorrência mais frequente, com 3.001 registros, seguido por abuso de sítio web 1.163 e exploração de software vulnerável 759. Também se destacam casos de ataques de negação de serviço (DRDoS), páginas falsas e tentativas de phishing, além de vulnerabilidades de criptografia e abuso de serviços de e-mail. Esses números refletem não apenas a variedade de vetores de ataque, mas também a exposição crescente das instituições públicas brasileiras a ameaças cibernéticas sofisticadas, que exigem uma resposta rápida e estratégica por parte do governo.

A ampla cobertura midiática sobre ataques cibernéticos contra órgãos públicos, facilmente acessível em fontes jornalísticas disponíveis online, evidencia a relevância e a atualidade da problemática. Um deles ocorreu na Prefeitura de Poços de Caldas, De acordo com reportagem do *G1 Sul de Minas* (2023), houve uma tentativa de invasão ao sistema eletrônico que resultou no vazamento de informações confidenciais, tanto de funcionários quanto da própria administração municipal. O sistema, operado por uma empresa terceirizada com sede em Uberlândia (MG), foi alvo de um ataque em que os invasores exigiram um resgate de R$15 milhões para a devolução dos dados. Como consequência, a prefeitura ficou temporariamente sem a emissão de alguns documentos e guias de forma online, orientando a população a buscar atendimento presencial para a realização desses serviços.

Além dos ataques cibernéticos, uma outra vertente dessa problemática envolve o uso criminoso desses dados. De acordo com a Polícia Federal (2024), operações frequentemente têm desmantelado organizações criminosas dedicadas à obtenção e comercialização de informações sigilosas. Um exemplo significativo está na obtenção e venda de dados confidenciais do Instituto Nacional do Seguro Social (INSS), revelando um mercado clandestino que compromete a privacidade dos dados dos segurados e expõe cidadãos a potenciais fraudes.

Quanto a esse ponto, para aprofundar o tema, foi realizada uma pesquisa no site da Autoridade Nacional de Proteção de Dados (ANPD), especificamente na seção "Documentos e Publicações", em "Outras Publicações". Foi possível localizar o Relatório de Monitoramento, que revelou que, no primeiro semestre de 2023, o setor mais demandado em relação a denúncias de descumprimento da legislação foi o Poder Executivo, com 25 denúncias registradas. Esse dado reforça a relevância e a necessidade de uma pesquisa aprofundada sobre o tema (BRASIL, 2023).

O setor público é um grande controlador de dados pessoais, engloba serviços de Cadastro de Pessoas Físicas (CPF), Cadastro de Imóveis Rurais (Cafir), Certidão de Registro de Imóveis Urbanos, Nota Fiscal Eletrônica (NF-e), sistema de emissão de Certidão de Regularidade Fiscal perante a Fazenda Nacional, entre outros.

A justificativa para o acesso do Estado aos dados pessoais repousa no pressuposto que a administração pública eficiente é aquela que tem profundo conhecimento das características da população, o que justificaria, inclusive, em certas situações, o estabelecimento de regras compulsórias para a comunicação de determinadas informações aos órgãos estatais. (DONEDA, 2006, p. 13-14).

O governo federal é composto por 42 órgãos de administração direta, 125 autarquias e 43 fundações públicas. Além disso, o Brasil possui 26 estados, o Distrito Federal e 5.570 municípios, cada um com sua própria estrutura administrativa, o que resulta em uma grande quantidade de entidades responsáveis pela execução dos serviços públicos (BRASIL, 2025; IBGE, 2025).

Para facilitar a visualização da diversidade de instituições e os diferentes tipos de dados tratados por elas, apresentamos a seguir uma tabela que classifica os órgãos federais, tipo de administração: direta ou indireta, poder: Executivo, Legislativo ou Judiciário, exemplos concretos de instituições e os tipos de dados pessoais com os quais operam, veja-se:

Tabela 1 - Classificação dos Órgãos Públicos Federais e a Diversidade no Tratamento de Dados Pessoais

Âmbito	Tipo de Administração	Poder	Exemplos de Órgãos	Tipos de Dados Pessoais Tratados
Federal	Direta	Executivo	Ministério da Saúde, Ministério da Educação, Ministério do Esporte, etc.	Dados de saúde (SUS), estudantes, atletas, beneficiários de programas federais, etc.
	Indireta	Executivo	INSS, ANVISA, IBGE, Caixa Econômica Federal, etc.	Previdenciários, sanitários, estatísticos e bancários, etc.
	Direta/ Indireta	Legislativo	Câmara dos Deputados, Senado Federal	Dados de servidores, visitantes, consultados em consultas públicas, etc.
	Direta/ Indireta	Judiciário	STF, STJ, CNJ, TRFs	Dados processuais, criminais, biométricos, de menores, vítimas, etc.

Fonte: elaborado pela autora

Importante destacar que a estrutura aqui apresentada, baseada no recorte federal, repete-se de forma semelhante nos âmbitos estaduais, distrital e municipais. A tabela acima evidencia a pluralidade institucional que compõe a administração pública e, consequentemente, a heterogeneidade dos dados pessoais tratados por esses entes. Cada órgão possui finalidades distintas e riscos específicos relacionados ao tratamento de dados.

A Constituição da República Federativa do Brasil, de 05 de outubro de 1988, prevê, em seu artigo 71, que os Tribunais de Contas, juntamente com o Congresso Nacional, atuarão no exercício do controle externo, realizando a fiscalização e auditoria contábil, financeira, orçamentária, operacional e patrimonial.

Os Tribunais de Contas desempenham um papel fundamental na fiscalização da administração pública, garantindo a correta aplicação da legislação, dos recursos públicos e

promovendo a transparência e a accountability. Para alcançar esse objetivo, utilizam-se mecanismos de auditoria, tais como a auditoria operacional, de conformidade e financeira.

A auditoria operacional busca contribuir para a melhoria da gestão pública, avaliando o desempenho com foco em economia, eficiência, eficácia e efetividade. O auditor utiliza critérios como normas legais, boas práticas e experiências, analisando se as atividades são executadas da melhor forma possível. Exige um perfil de gestor flexível e empreendedor e demanda conhecimento em ciências sociais e análise de políticas.

Já a auditoria de conformidade verifica se o gestor atua conforme normas aplicáveis, enquanto a auditoria financeira busca garantir a confiabilidade das demonstrações financeiras, assegurando que estejam livres de distorções materiais. Ambas se baseiam na conformidade com procedimentos e normas legais, mas a financeira foca em estruturas contábeis e regulatórias. A conformidade exige conhecimento jurídico, enquanto a financeira demanda expertise em contabilidade. Em resumo, cada tipo de auditoria atende a objetivos distintos, mas complementares, dentro do controle e da transparência da gestão pública e financeira, e será detalhado melhor em capítulo próprio.

Através desses mecanismos, é possível verificar se os princípios que regem a Administração Pública, quais sejam, legalidade, impessoalidade, moralidade, publicidade e eficiência, estão sendo devidamente aplicados. Adicionalmente, com foco na proteção de dados, esses mecanismos servem para avaliar se a norma está sendo implementada corretamente, se está sendo conduzida de maneira adequada e identificar os riscos e dificuldades presentes. O objetivo é garantir a efetividade das políticas públicas, assegurando que elas atinjam sua finalidade, que é a proteção do direito fundamental debatido no presente trabalho.

Nessa perspectiva, será analisada a Auditoria nº 1384/2022/TCU, cujo objetivo foi diagnosticar o grau de implementação da LGPD na administração pública federal. O trabalho avaliou 382 organizações pertencentes a diferentes Poderes da República, com distintas temáticas e desafios institucionais. O questionário utilizado foi estruturado em nove dimensões. O resultado do Acórdão apresentou tanto dados globais sobre o nível geral de implementação quanto dados detalhados por pergunta, permitindo uma visão geral e segmentada da aplicação da LGPD pelos órgãos auditados.

O surgimento de normas como a LGPD decorre da necessidade de garantir direitos fundamentais diante de novas realidades sociais, tecnológicas e econômicas. Nesse sentido, a

norma foi criada para oferecer uma resposta jurídica adequada aos riscos decorrentes do uso massivo de dados pessoais, buscando criar salvaguardas que garantam não apenas o cumprimento formal de obrigações, mas a efetiva proteção dos direitos dos titulares de dados.

Entretanto, a rápida evolução tecnológica e o avanço da sociedade da informação impuseram novas complexidades à administração pública, o processo de digitalização dos serviços públicos aumentou os riscos associados à segurança da informação. A administração pública moderna, com estruturas organizacionais complexas e fluxos de dados cada vez mais dinâmicos e conectados, demanda mecanismos de fiscalização que consigam acompanhar esse novo cenário. A mera verificação formal de documentos e procedimentos declarados pelos órgãos auditados já não são suficientes para garantir que os direitos assegurados pela LGPD estejam sendo, de fato, efetivados.

Diante desse cenário, a atuação do TCU ganha relevância como um possível instrumento de indução e estímulo à implementação da LGPD nos órgãos públicos, por meio de suas auditorias. Contudo, observa-se uma lacuna na literatura quanto à existência de estudos que abordem de forma sistemática as ações fiscalizatórias do TCU no processo de adequação dos órgãos públicos à LGPD.

Com o intuito de confirmar essa lacuna, foram realizadas buscas no Catálogo de Teses e Dissertações da Plataforma CAPES, utilizando os descritores “LGPD”, “Tribunal de Contas da União”, “TCU”, “auditoria” e “Acórdão 1384/2022”. As pesquisas não retornaram resultados, o que indica a ausência de trabalhos acadêmicos que tratem especificamente da fiscalização exercida pelo TCU sob a perspectiva da proteção de dados pessoais.

Este trabalho está vinculado à linha de pesquisa Estado, Constituição e Democracia, mais especificamente à sublinha Constitucionalismo, Direitos Fundamentais e Acesso à Justiça. A escolha se justifica pelo fato de que a proteção de dados pessoais, conforme reconhecido pela Emenda Constitucional nº 115/2022, constitui um direito fundamental diretamente relacionado à dignidade da pessoa humana e à autodeterminação informativa.

A vinculação deste trabalho à linha de pesquisa, especialmente à sublinha Direitos Fundamentais, decorre da compreensão de que a proteção de dados pessoais representa uma dimensão essencial do exercício da cidadania no contexto da sociedade da informação. A análise da atuação do Tribunal de Contas da União permite problematizar como os mecanismos de controle e fiscalização estatais podem contribuir, ou falhar, na consolidação

prática de direitos fundamentais reconhecidos constitucionalmente, como o direito à proteção de dados, recentemente incluído no rol de direitos fundamentais.

Nesse contexto, a análise crítica da atuação do Tribunal de Contas da União como órgão de controle externo na fiscalização da implementação da LGPD nos órgãos públicos contribui para o debate sobre os mecanismos institucionais de garantia de direitos fundamentais, promovendo uma reflexão acerca dos desafios constitucionais relacionados à proteção da privacidade e à governança de dados no setor público. Diante disso, este trabalho propõe-se a preencher uma lacuna na literatura por meio de uma análise crítica da atuação do TCU, com foco no estudo de caso da auditoria que resultou no Acórdão nº 1384/2022.

A presente pesquisa apresenta impactos relevantes em diferentes dimensões. No campo acadêmico, contribui para a ainda escassa produção científica sobre a atuação dos tribunais de contas na efetivação de direitos fundamentais, especialmente no contexto da proteção de dados pessoais. No plano institucional, oferece subsídios para o aprimoramento das metodologias de auditoria aplicadas pelo TCU e demais órgãos de controle em matéria de proteção de dados, estimulando reflexões sobre o papel fiscalizador na implementação de políticas públicas sensíveis à privacidade e à autodeterminação informativa.

A escolha do TCU como objeto de estudo também se justifica por sua centralidade no sistema de controle externo brasileiro. Embora não exista, formalmente, um órgão de uniformização entre os tribunais de contas, a Constituição estabelece, por simetria, que os demais devem observar os parâmetros definidos pelo TCU. Ainda que essa padronização não se concretize plenamente, o Tribunal funciona, na prática, como uma vitrine institucional, influenciando a atuação dos demais e moldando padrões nacionais de fiscalização.

Nesse sentido, a ausência de uniformização entre os 33 Tribunais de Contas brasileiros é analisada por Ricardo Schneider Rodrigues na obra *Os 35 anos do Superior Tribunal de Justiça – Volume I – Direito Público*. O autor observa que, diferentemente do Poder Judiciário, o sistema de controle externo opera de forma descentralizada, sem uma instância responsável por consolidar entendimentos.

Essa constatação reforça a relevância de estudar o TCU como referência nacional. Ao analisar criticamente a metodologia de auditoria adotada no Acórdão nº 1384/2022, este trabalho contribui para o debate sobre o papel institucional do Tribunal na efetivação de direitos fundamentais da proteção de dados.

O problema que norteou esta pesquisa parte da constatação de que, embora o Tribunal de Contas da União exerça um papel essencial na fiscalização da implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no setor público, ainda são escassos os estudos críticos que analisem, de forma aprofundada, os critérios e a metodologia empregados na Auditoria nº 1384/2022. Essa lacuna compromete a compreensão mais precisa sobre o alcance, os impactos e os limites da atuação do TCU no acompanhamento da conformidade dos órgãos públicos federais com a LGPD. Diante disso, a presente pesquisa busca responder: a auditoria do TCU, conforme o Acórdão nº 1384/2022, apresenta limitações e oportunidades de aprimoramento na fiscalização da implementação da LGPD nos órgãos públicos federais?

Assim, esta dissertação tem como objetivo geral analisar os elementos que compõem a atuação do Tribunal de Contas da União na auditoria de implementação da LGPD, a partir do estudo do Acórdão nº 1384/2022, identificando potenciais contribuições e limitações dessa atuação. Nesse sentido, adota-se o método de abordagem hipotético-dedutivo, que permite partir de uma hipótese inicial e testá-la por meio da análise de dados e evidências. Para alcançar esse propósito, foram definidos os seguintes objetivos específicos:

1. Construir a fundamentação teórica e normativa necessária para a análise crítica da atuação fiscalizatória do TCU, por meio da apresentação dos conceitos essenciais da proteção de dados pessoais, da estrutura legal da LGPD no setor público, dos riscos associados ao tratamento inadequado de dados e da atuação dos órgãos competentes. Trata-se, portanto, de estabelecer os elementos estruturantes que servirão de base para a avaliação realizada nos capítulos seguintes.
2. Contextualizar os tipos de auditoria realizados pelo Tribunal de Contas da União, com foco em suas finalidades, metodologias e limites institucionais, a fim de fornecer o referencial necessário para a análise crítica da auditoria objeto desta pesquisa.
3. Analisar criticamente o conteúdo, a estrutura e as limitações da auditoria realizada pelo Tribunal de Contas da União no Acórdão nº 1384/2022, verificando se ela contempla adequadamente os requisitos da LGPD e se permite avaliar, com consistência, as ações adotadas pelos órgãos auditados.

Diante do recente contexto de vigência da LGPD à época da realização da Auditoria nº 1384/2022, é possível que o TCU tenha adotado uma metodologia de fiscalização orientada mais à sensibilização e ao levantamento preliminar de conformidade do que à exigência de

adequações estruturais e aprofundadas. Essa abordagem, ainda que relevante para o estágio inicial de implementação normativa, pode ter apresentado limitações quanto à abrangência dos critérios utilizados e ao direcionamento das recomendações, evidenciando desafios a serem enfrentados na consolidação de uma política pública de proteção de dados no setor público.

Ademais, a estrutura da dissertação se dará da seguinte forma: o primeiro capítulo tem como objetivo apresentar os conceitos fundamentais que sustentam o tema central da pesquisa. Nesse sentido, serão explorados os fundamentos da LGPD com foco no setor público, com destaque para os princípios e diretrizes que a tornam um marco regulatório essencial na garantia do direito à proteção de dados pessoais, como direito fundamental atribuído pela nossa Constituição. Esse panorama inicial busca contextualizar as interseções entre o TCU e a LGPD, servindo como base para as discussões mais aprofundadas no capítulo terceiro.

No segundo capítulo, foi analisada a atuação do Tribunal de Contas e os diferentes tipos de auditoria por ele realizadas, para contextualizar o papel dessas auditorias no âmbito da fiscalização da administração pública. A partir desse panorama, aliado à análise do primeiro capítulo, cria-se a base conceitual e metodológica que permitirá, no capítulo seguinte, a avaliação crítica da auditoria realizada pelo Tribunal de Contas da União especificamente em matéria de proteção de dados pessoais.

Na apresentação desses dois capítulos, será adotada uma metodologia de procedimento monográfico com análise descritiva, uma vez que serão expostos os conceitos, princípios e diretrizes fundamentais da LGPD e TCU, fornecendo a base teórica necessária para o desenvolvimento da pesquisa.

Segundo Pinheiro (2019) essa fase é fundamental para o pesquisador, pois é nesse momento que ele tem a oportunidade de aprofundar sua base teórica, a qual constituirá todo o suporte conceitual do seu trabalho. Desenvolvida a partir da consulta a livros, artigos científicos e diversos outros materiais, esta técnica de pesquisa contribui para a ampliação do universo de pesquisa, já que permite ao sujeito pesquisar dados construídos *a priori*.

O terceiro capítulo realiza uma análise crítica da auditoria conduzida pelo Tribunal de Contas da União, que resultou no Acórdão nº 1384/2022. O objetivo é verificar se essa auditoria abrange todos os requisitos previstos na LGPD e se está estruturada de forma a

contribuir efetivamente para garantir a segurança das informações pessoais tratadas pelos órgãos públicos.

Por fim, a conclusão apresentará uma síntese dos principais achados da pesquisa, com foco em responder à pergunta de pesquisa, bem como confrontar as hipóteses e premissas estabelecidas, destacando as contribuições para a área, as limitações do estudo e sugestões para pesquisas futuras.

1. LEI GERAL DE PROTEÇÃO DE DADOS NO SETOR PÚBLICO

A proteção de dados pessoais consolidou-se como uma das principais preocupações da sociedade contemporânea, especialmente diante da intensificação do uso de tecnologias digitais e da crescente virtualização dos serviços públicos e privados. A transição para o ambiente online ampliou significativamente os riscos relacionados ao tratamento de informações pessoais, expondo os cidadãos a novas formas de vulnerabilidade, como fraudes, manipulação de informações, discriminações indevidas e violações da privacidade.

Nesse contexto de crescente preocupação social e jurídica, a promulgação da Lei nº 13.709/2018, representou um marco normativo fundamental na consolidação de direitos relacionados à privacidade e à proteção de dados no Brasil. Posteriormente, com a Emenda Constitucional nº 115/2022, a proteção de dados pessoais foi alçada ao status de direito fundamental, reforçando a centralidade do tema na agenda pública e jurídica nacional.

O objetivo deste capítulo é oferecer ao leitor uma análise sobre a aplicação da LGPD no setor público brasileiro, uma vez que o tratamento de dados por órgãos e entidades públicas apresenta especificidades que o diferenciam do setor privado, sobretudo em razão dos princípios constitucionais que regem a Administração Pública e da própria finalidade pública dos tratamentos realizados.

Ao longo da exposição, será apresentada uma contextualização inicial dos principais conceitos relacionados à proteção de dados pessoais, com destaque para os fundamentos normativos e constitucionais que sustentam o direito à privacidade. Nesse primeiro momento, serão abordados também os riscos associados ao tratamento inadequado de dados, incluindo exemplos de ataques cibernéticos e o caso emblemático da Cambridge Analytica, que evidenciam as potenciais ameaças à segurança informacional e à autonomia dos indivíduos. Em seguida, proceder-se-á à análise normativa da aplicação da LGPD no âmbito da

Administração Pública, com especial atenção ao papel da ANPD como órgão regulador e fiscalizador, refletindo-se sobre suas atribuições, competências e limitações.

Além disso, serão discutidos os mecanismos de sanção e fiscalização aplicáveis ao Poder Público, questão que desperta relevantes debates, inclusive no âmbito dos Tribunais de Contas, instituições responsáveis pela fiscalização da Administração Pública. Outro ponto de destaque será a análise da relação entre a LGPD e a LAI, tema de extrema relevância para o controle externo, considerando que, à primeira vista, as duas normas podem aparentar conflito, ao estabelecerem, respectivamente, limites e deveres quanto ao acesso e à proteção das informações públicas e pessoais.

Por fim, as reflexões apresentadas neste capítulo buscarão oferecer ao leitor uma compreensão inicial e estruturada da temática da proteção de dados no setor público, estabelecendo as bases conceituais e normativas que nortearão os debates dos capítulos seguintes.

1.1. Fundamentos da proteção dos dados pessoais: noções introdutórias

O avanço acelerado das tecnologias digitais provocou uma profunda transformação nas dinâmicas sociais, criando um ambiente no qual pessoas de diferentes partes do mundo permanecem conectadas em tempo real por meio de redes virtuais. Essa nova realidade favoreceu a circulação massiva de informações nesses espaços digitais, resultando na formação de grandes bases de dados pessoais. Nesse contexto, compreender os direitos fundamentais relacionados à proteção de dados demanda, inicialmente, uma análise clara e objetiva do que se entende por "dados pessoais", conceito que será abordado a seguir (SOUZA; ACHA, 2022).

Dado pessoal é toda informação que permite identificar uma pessoa natural, direta ou indiretamente. Isso inclui dados básicos como: nome, CPF, endereço, telefone, dados biométricos, dados fácil, localização, registros de saúde, características físicas, entre outros. A LGPD foi criada justamente para estabelecer uma metodologia sobre o tratamento desses dados no Brasil. A lei dispõe sobre os princípios, direitos, deveres e responsabilidades que devem ser observados tanto por empresas quanto por órgãos públicos ao coletar, armazenar, processar e compartilhar dados pessoais.

Após a promulgação da LGPD, o Supremo Tribunal Federal passou a reconhecer expressamente a proteção de dados pessoais como um direito fundamental. Isto é, antes da aprovação da Emenda Constitucional que formalizou tal entendimento, o Plenário do STF já havia concedido medida cautelar na Ação Direta de Inconstitucionalidade - ADI nº 6387/DF. Nessa decisão, a Corte reforçou a necessidade de interpretar a Constituição Federal de forma atualizada, de modo a alinhar seus preceitos às novas demandas surgidas com o avanço das tecnologias (BRASIL, 2020).

Segundo Mendes et al. (2023), a Constituição Federal de 1988, embora faça referência, no art. 5°, XII, ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas), passou a contemplar expressamente um direito fundamental à proteção de dados pessoais, inclusive em meios digitais, a partir da promulgação da EC 115, aprovada em fevereiro de 2022 pelo Congresso Nacional.

A elevação da proteção de dados pessoais à condição de direito fundamental, reconhecida pelo Supremo Tribunal Federal e posteriormente consolidada com a Emenda Constitucional n.º 115/2022, é essencial porque confere um nível maior de proteção jurídica a esse direito. Isso significa que a proteção de dados passa a ser um dever prioritário do Estado e um limite às práticas de empresas e instituições. O uso malicioso ou irresponsável de dados pessoais pode gerar graves consequências, como fraudes financeiras, roubo de identidade, discriminação, invasão de privacidade, perseguição, risco a democracia e demais.

A proteção de dados pessoais vem sendo reconhecida como um direito fundamental com autonomia própria, sustentada por fundamentos jurídicos que a inserem no campo do Direito Constitucional e do Direito Civil. No âmbito constitucional, a sua vinculação está diretamente relacionada ao princípio da dignidade da pessoa humana, previsto no artigo 1º, inciso III, da CF, o qual orienta a interpretação de diversos direitos fundamentais. Já no campo civil, a proteção de dados se conecta à tutela dos direitos da personalidade. Essa conexão decorre da compreensão de que a dignidade da pessoa humana não é apenas um princípio abstrato, mas sim um valor que permeia e fundamenta os demais direitos assegurados ao indivíduo. No entanto, apesar de sua centralidade no ordenamento jurídico, a dignidade da pessoa humana não pode ser utilizada de forma genérica como solução para qualquer conflito levado ao Judiciário, sob o risco de perder seu conteúdo normativo e sua força conceitual. (CALISSI; FRANCO NEME; ALBERTO MAIA, 2024, p. 203).

Souza e Acha (2022) destacam que a crescente digitalização das relações pessoais, comerciais e profissionais tem levado as pessoas a compartilharem diariamente uma grande quantidade de dados pessoais em diversas plataformas, como cadastros online, aplicativos de mensagens e redes sociais. Eles apontam que essa exposição frequente, que abrange desde interações familiares até operações financeiras e contratações, aumenta os riscos relacionados à privacidade e à intimidade dos usuários. Exemplos de vazamentos e usos inadequados de dados demonstram as ameaças reais enfrentadas por muitos indivíduos no ambiente digital.

É importante trazer essas ameaças para o debate, uma vez que o conhecimento dos riscos envolvidos contribui para uma análise mais aprofundada da auditoria, não apenas em relação ao cumprimento formal da conformidade, mas sobretudo quanto à efetiva segurança no tratamento dos dados que realmente importam.

Doneda (2020) ressalta que as ameaças podem ser compreendidas como uma combinação entre o ator e o ataque. Nesse sentido, abordaremos inicialmente os aspectos relacionados aos atores, para, em seguida, explorar os ataques que podem ser efetivamente desencadeados.

Quanto ao primeiro ponto, os atores podem ser divididos em dois grupos: de um lado, os *hackers* e de outro, os *insiders*. Enquanto os primeiros são agentes externos, os *insiders* correspondem a agentes internos de uma instituição e/ou empresa vítima de um incidente de segurança. Antes de esclarecer as formas de atuação desses atores e de abordarmos as diversas categorias de *hackers*, é importante destacar que, apesar da conotação frequentemente negativa atribuída ao termo, um *hacker* é, na essência, alguém que busca entender profundamente os mecanismos e sistemas, a fim de solucionar problemas.

A obra de Doneda (2020) apresenta diversas categorias de hackers, classificando-os conforme seus propósitos e atuações. Entre essas categorias, destacam-se o white hat, hacker ético focado em segurança dos sistemas; o black hat, que utiliza seus conhecimentos para fins criminosos; e o grey hat, que invade sistemas por diversão, sem causar danos. Também são mencionados o blue hat, contratado por empresas para identificar vulnerabilidades; o hacktivista, que emprega suas habilidades para apoiar causas sociais, políticas, ideológicas ou religiosas; e os nation states hackers, hackers vinculados a governos e envolvidos em grupos de guerra cibernética.

Já os *insiders* são, em geral, funcionários descuidados ou insatisfeitos e/ou ex-funcionários em busca de vingança. Por estarem inseridos na instituição e/ou empresa,

esses indivíduos possuem acesso legítimo aos dados, o que aumenta significativamente o risco de incidentes. Nesse contexto, a melhor forma de prevenção é a implementação de mecanismos eficazes de controle de acesso.

Após contextualizar os principais aspectos relacionados aos autores, passa-se à análise dos principais tipos de ataques cibernéticos e suas características, que ameaçam a integridade das informações pessoais, quais sejam, engenharia social, *data exfiltration, shoulder surfing, dumpster diving, phising, spear phising, whaling, sniffing, ransomware.*

A engenharia social é um método que utiliza técnicas de persuasão e manipulação psicológica para induzir pessoas a fornecerem informações confidenciais. Por sua vez, a *data exfiltration* ocorre quando um agente malicioso realiza a transferência não autorizada de dados. Já o *shoulder surfing* consiste na obtenção de informações sensíveis por meio da observação direta, enquanto a vítima digita ou escreve dados confidenciais.

Dumpster diving é uma prática onde criminosos vasculham o lixo de empresas ou órgãos públicos em busca de informações e dados que possam facilitar a invasão e/ou fraude, isso decorre do descarte irregular de documentos e/ou dispositivos eletrônicos que contém dados.

Phishing consiste em um golpe virtual em que atacantes buscam enganar usuários para obter dados pessoais ou financeiros. Para isso, utilizam estratégias de engenharia social, enviando mensagens eletrônicas disfarçadas de comunicações oficiais, geralmente de grandes empresas. Essas mensagens, por sua vez, direcionam a vítima para páginas falsas ou solicitam a inserção de informações confidenciais, induzindo o usuário a agir de maneira imprudente.

O *spear phishing* e o *whaling* são variantes do *phishing* que se diferenciam principalmente pelo foco do ataque. No *spear phishing*, o alvo é um indivíduo ou instituição específica, com o conteúdo do e-mail personalizado para aumentar a eficácia do golpe. Já no *whaling,* o alvo são pessoas de alto escalão (como executivos ou autoridades), com ataques ainda mais sofisticados e personalizados para explorar seu acesso privilegiado a informações e sistemas.

Sniffing é a leitura ou interceptação de dados por meio da captura do tráfego de rede, a maior preocupação consiste no fato de que muitos dados trafegam sem ser criptografados, e por isso facilita o acesso a dados sensíveis. O *ransomware* é um tipo de *malware* que criminosos utilizam para extorquir dinheiro, ele vai criptografar e manter os dados reféns enquanto não houver um pagamento.

Além dos ataques cibernéticos, não podemos esquecer o contexto histórico da Guerra Fria, quando dois grandes impérios: os Estados Unidos e a extinta União Soviética, disputavam continentes. Nesse cenário, encontraram na desinformação, operações de influência política e na espionagem seu principal método, pois era fundamental saber com antecedência onde, como, quando e em que local o inimigo pretendia agir.

Práticas de manipulação da informação, que antes pareciam restritas aos bastidores da geopolítica, hoje fazem parte do nosso cotidiano digital. Campanhas de desinformação, criação de narrativas e tentativas de minar a confiança nas instituições democráticas continuam a ser usadas, com novos recursos e um alcance sem precedentes.

Podemos citar como exemplo as alegadas interferências nas eleições presidenciais dos Estados Unidos de 2016, em que a Cambridge Analytica esteve envolvida no escândalo que usou dados pessoais de usuários do facebook, para prever a personalidade de cada adulto, através de testes, e influenciar eleitores que podem ter ajudado a eleger Trump nos Estados Unidos, a influência se dava através da propagação de anúncios produzidos sob medida e direcionados para eleitores de acordo com o traços de suas personalidades, obtidas e armazenados no banco de dados, visando provocar a exata reação emocional pela qual o cliente estava pagando, controlando assim o processo de tomada de decisão, conforme notícias veiculadas pela imprensa (GLOBO, 2018).

A utilização dos dados pela Cambridge Analytica insere-se no contexto da chamada sociedade informacional, na qual informações pessoais se tornaram um verdadeiro *commodity*, amplamente explorado no âmbito privado para a criação de perfis detalhados de personalidade e comportamento. Empresas e plataformas digitais coletam, analisam e comercializam esses dados com o objetivo de direcionar produtos e serviços, personalizar experiências e maximizar lucros. No caso específico do escândalo envolvendo o Facebook, tais perfis não foram apenas utilizados para fins comerciais, mas empregados estrategicamente para manipular eleitores, influenciando suas decisões no processo eleitoral. Nesse sentido, compromete-se a autonomia individual e representa uma ameaça à integridade do sistema democrático.

Frazão (2023) destaca que dados, informações e referências pessoais tornaram-se elementos centrais na economia global, servindo como matéria-prima para a obtenção de ganhos tanto na eficiência empresarial quanto na atuação governamental. Contudo, o uso

desses mesmos dados também gera abusos e distorções, tema que vem sendo amplamente discutido em círculos acadêmicos, empresariais e entre formuladores de políticas públicas.

Segundo Valadares (2024), a coleta constante de dados pessoais é uma consequência inevitável da modernidade, já que muitos serviços essenciais à vida econômica e cidadania dependem hoje de plataformas digitais. Isso inclui desde transações bancárias até processos de contratação e compra de passagens, que exigem o fornecimento frequente de informações pessoais, transformando o mundo em um grande banco de dados. Embora esses avanços ampliem as capacidades tecnológicas e administrativas, eles também trazem riscos pouco percebidos pela maioria das pessoas, pois a exposição contínua dos dados pode afetar a dignidade humana, limitando a autonomia e a forma como cada indivíduo constrói sua identidade.

A dignidade da pessoa humana, no contexto da proteção de dados pessoais, está diretamente relacionada à capacidade do indivíduo de exercer sua autonomia, ou seja, de fazer suas próprias escolhas de maneira consciente e livre, tanto nas escolhas do dia a dia quanto no controle sobre seus dados pessoais. Tal autonomia é um pressuposto para o exercício da autodeterminação informativa, que permite à pessoa decidir como, quando e em que medida suas informações pessoais serão utilizadas.

Os autores Calissi, Franco Neme e Maia escreveram o artigo “A proteção de dados e o princípio da dignidade humana: uma compreensão acerca da autodeterminação informativa”, que propôs avaliar a relação entre a proteção de dados pessoais e o princípio da dignidade da pessoa humana, enfatizando a autodeterminação informativa como elemento essencial dessa relação. Nesse sentido, concluíram que:

> No âmbito da proteção de dados, compreendida como Direito Fundamental Autônomo, a intertextualidade das perspectivas de Hesse no século XX e de Rodotá no Século XXI, são convergentes, tanto no plano do Direito Interno, quanto do Direito Internacional. Neste sentido, pode-se afirmar, também, a natureza dúplice supra-positiva e positiva do princípio da Dignidade da Pessoa Humana, e seu aspecto universal, que tanto no plano interno, quanto internacional colocam a pessoa no centro do ordenamento jurídico em consonância com a perspectiva personalista propugnada por Rodotá (CALISSI; FRANCO NEME; ALBERTO MAIA, 2024, p. 218).

Diante da constatação de que a proteção de dados pessoais constitui um direito fundamental, cuja relevância se acentua no contexto da sociedade informacional, e considerando os riscos inerentes ao tratamento massivo e indiscriminado de dados, a

aplicação da teoria da dimensão objetiva dos direitos fundamentais revela-se especialmente pertinente.

A teoria objetiva dos direitos fundamentais representa uma evolução no entendimento sobre sua função dentro do ordenamento jurídico. Ela amplia a ideia tradicional de que os direitos fundamentais servem apenas para proteger o indivíduo contra abusos do Estado. Conforme explicam Mitidiero et al. (2023), essa concepção reconhece que tais direitos também possuem uma função estruturante, voltada à conformação da ordem jurídica como um todo. Ou seja, os direitos fundamentais não apenas garantem liberdades individuais, mas também impõem deveres e orientações para toda a atuação estatal, inclusive de forma independente da provocação de um sujeito específico.

Mendes (2012), ao tratar da tradição constitucional alemã, destaca que essa dimensão objetiva impõe ao Estado obrigações positivas, como proteger os indivíduos contra ameaças que possam vir de terceiros. Essa responsabilidade ativa do Estado transforma sua posição: ele deixa de ser visto apenas como um possível violador e passa a ser considerado um agente necessário na promoção e na salvaguarda dos direitos fundamentais. Essa virada teórica influencia diretamente o modo como os órgãos públicos devem operar, exigindo que suas ações estejam pautadas por uma postura proativa e garantidora desses direitos.

Nessa linha, Hachem (2016) destaca que o artigo 5º, §1º, da CF ao afirmar que os direitos e garantias fundamentais têm aplicação imediata, não limita essa eficácia à sua dimensão subjetiva. Pelo contrário, obriga a Administração Pública a atuar também no plano objetivo, promovendo e estruturando suas práticas administrativas de forma a dar efetividade a esses direitos. Isso inclui, por exemplo, o dever de agir preventivamente, mesmo sem provocação específica, especialmente quando se trata de temas sensíveis como a proteção de dados pessoais.

Reconhecendo que a proteção de dados pessoais é um direito fundamental que se relaciona diretamente com a dignidade da pessoa humana, é possível afirmar que o Estado, por meio de todos os seus órgãos, inclusive os Tribunais de Contas, tem o dever de assegurar sua efetividade. A partir da teoria objetiva, não basta que o Estado se abstenha de violar dados pessoais; ele deve implementar mecanismos, fiscalizar condutas e desenvolver políticas públicas voltadas à sua proteção. Isso significa que a atuação dos Tribunais de Contas ganha uma nova centralidade nesse processo.

Os Tribunais de Contas, enquanto órgãos de controle externo da Administração Pública, possuem não apenas a possibilidade, mas o dever jurídico-constitucional de atuar na fiscalização da conformidade das práticas administrativas com os direitos fundamentais, inclusive no que se refere à proteção de dados. Com base em sua competência constitucional, esses tribunais devem verificar se os órgãos públicos estão adotando medidas adequadas de governança de dados, segurança da informação e conformidade com a LGPD. Ao assim procederem, contribuem para a consolidação de uma cultura institucional de respeito à privacidade e à autodeterminação informativa.

Essa atuação é ainda mais relevante diante da natureza transversal da proteção de dados, que afeta áreas como acesso à informação, igualdade de tratamento, liberdade de expressão e segurança jurídica. Conforme aponta Frazão (2023), a proteção de dados não é um tema isolado, mas se interconecta com diversos outros direitos fundamentais. Dessa forma, a fiscalização exercida pelos Tribunais de Contas fortalece não apenas a efetividade da LGPD, mas a própria estrutura normativa da Constituição, cumprindo o papel de garantir que a Administração Pública atue em consonância com os valores fundamentais do Estado Democrático de Direito.

Portanto, a partir da teoria objetiva dos direitos fundamentais, a proteção de dados pessoais deve ser compreendida como um dever estatal de promoção ativa e contínua. Os Tribunais de Contas, nesse cenário, assumem uma posição estratégica ao acompanhar, induzir e exigir o cumprimento da legislação de proteção de dados nos entes públicos, colaborando para a construção de uma administração pública mais transparente, responsável e alinhada aos princípios constitucionais.

1.2 A aplicação da LGPD na administração pública

A LGPD dispõe de um capítulo específico para abordar o tratamento de dados pelo poder público, especificamente o Capítulo IV da Lei nº 13.709/2018. No entanto, primeiramente é importante destacar que o tratamento de dados é definido como “toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (BRASIL, 2018).

Nesse sentido, esta seção tem como objetivo estudar o referido capítulo da lei, uma vez que a finalidade do tratamento de dados realizado por empresas privadas difere daquela dos órgãos públicos. O entendimento desta seção é fundamental para o desenvolvimento do presente trabalho, por se tratar de um aspecto central, e servirá como base para a análise da auditoria.

A legislação optou por estabelecer uma distinção no tratamento de dados realizado pelos órgãos públicos, se aplicando a qualquer órgão ou entidade pública, empresas públicas e sociedade de economia mista, considerando a natureza desse tratamento, que deve ser conduzido para atender a uma finalidade pública, visando alcançar o bem coletivo e executar competências legais, conforme o que dispõe o art. 23, *caput*, Lei 13.709/2018. Por outro lado, a legislação não se aplicará ao poder público nos casos que envolvam: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais (BRASIL, 2018).

A LGPD não traz disposições específicas sobre políticas públicas. Em pesquisas realizadas para identificar possíveis regulamentações por parte da ANPD, verificou-se que, até o momento, não foi editada nenhuma normativa sobre o tema. No entanto, a mesma publicou um guia orientativo para o tratamento de dados pelo poder público. A partir desse documento, pode-se concluir que, para caracterizar uma política pública, dois aspectos devem ser considerados: (i) a existência de um ato formal que institua a política pública, seja por meio de ato normativo (lei ou regulamento) ou; (ii) ajustes contratuais (contratos, convênios e instrumentos congêneres).

É possível compreender políticas públicas como qualquer iniciativa governamental formalizada por meio de atos normativos ou contratuais como: leis, regulamentos ou ajustes que envolvam, de forma estruturada, a definição de objetivos, metas, prazos e os meios para sua execução (ANPD, 2023). Essa interpretação mais ampla permite abarcar diferentes formas de atuação do Estado voltadas à concretização de direitos e ao atendimento do interesse público.

Ao analisar a legislação, verifica-se que, quando o tratamento de dados é realizado por órgãos públicos, é necessário consultar e analisar outras normas correlatas para sua correta aplicação, especialmente no que se refere aos prazos e procedimentos para o exercício dos direitos do titular, conforme artigo 23, § 3º da LGPD.

O encarregado pelo Tratamento de Dados Pessoais surge por meio do art. 5º, inciso VIII, da LGPD o conceituou como a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". (BRASIL, 2018).

Além da legislação, a Autoridade Nacional de Proteção de Dados aprovou o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais por meio da Resolução CD/ANPD nº 18, de 16 de julho de 2024. Esse regulamento estabelece diretrizes sobre quem pode exercer a função, como deve desempenhá-la e a forma de formalização da indicação.

No que se refere à atuação do encarregado no setor público, o primeiro passo é a escolha da pessoa designada para a função. De modo geral, a resolução dispõe que o encarregado pode ser tanto um profissional interno quanto externo. No entanto, quando trata especificamente dos órgãos públicos, determina que a indicação deve recair preferencialmente sobre servidores ou empregados públicos de reputação ilibada. Dessa forma, a oficialização deste ato deverá ser divulgada no Diário Oficial da União, do Estado, do Distrito Federal ou do Município.

A legislação trata do compartilhamento de dados pessoais realizado pelos órgãos públicos, permitindo a transferência de bases de dados para outro ente público ou para entidades privadas, desde que com o objetivo de atender a uma finalidade pública. A legislação enfatiza a obrigatoriedade de atender à finalidade pública. No entanto, na prática, na análise concreta da situação, apenas atingir essa finalidade não é suficiente para a realização dos atos administrativos relacionados à LGPD, é preciso atrelar a outras determinações da legislação.

No caso do compartilhamento de dados, é necessário observar os seguintes requisitos, segundo a ANPD: a) formalização e registro; b) definição do objeto e da finalidade; c) base legal; d) duração do tratamento; e) transparência e garantia dos direitos dos titulares; f) medidas de prevenção e segurança (BRASIL, 2023).

À primeira vista, essa operação pode parecer simples. No entanto, trata-se de um processo altamente desafiador, pois exige a atuação de uma equipe multidisciplinar para assegurar que o compartilhamento atenda à finalidade pública sem comprometer os princípios da proteção de dados, especialmente no que se refere à segurança. Esse é um tema que pode ser objeto de estudo acadêmico mais aprofundado.

Para exemplificar a complexidade, podemos analisar a Medida Provisória nº 954, de 2020, que tinha como objetivo determinar que empresas de telecomunicações disponibilizasse ao Instituto Brasileiro de Geografia e Estatística - IBGE, dados pessoais, quais sejam: nome, número telefone e endereço dos consumidores, para a produção de estatísticas oficial. De uma análise da legislação mencionada, percebe-se que a mesma proporciona o devido formalismo, no entanto, não previu questões essenciais que determinasse o devido tratamento e segurança que a LGPD dispõe.

Como resultado, foi instaurada Ação Direta de Inconstitucionalidade - ADI nº 6.387, ao Supremo Tribunal Federal - STF, para contestar a constitucionalidade da medida, que em sede de medida cautelar foi deferida, suspendendo a eficácia da Medida Provisória, a fim de prevenir danos irreparáveis à intimidade de milhares de usuários dos serviços de telefonia, tendo em vista que apesar de preencher os requisitos formais, a medida ultrapassa os limites de proporcionalidade e razoabilidade, bem como não preenche os requisitos do ponto de vista material.

A decisão proferida na ADI nº 6.387 pelo STF trouxe à tona a complexidade envolvida no compartilhamento de dados pessoais por órgãos da Administração Pública. Embora a medida em questão tenha buscado atender a uma finalidade legítima, ou seja, a produção de estatísticas oficiais pelo IBGE, a falta de salvaguardas adequadas para a privacidade e segurança dos dados pessoais dos cidadãos levou à sua suspensão.

Duas grandes questões foram levantadas para suspender a medida, a saber: razoabilidade e proporcionalidade, uma vez que seriam compartilhados aproximadamente mais de 200 (duzentos milhões) de dados de cidadãos. Além disso, argumentou-se que as medidas de segurança deveriam ser implementadas antes do compartilhamento dos dados, com o objetivo de prevenir possíveis danos decorrentes de um vazamento. Na decisão em questão, várias consequências foram mencionadas como possíveis, caso um indivíduo mal-intencionado obtivesse acesso a esses dados. Entre essas, foram destacadas as possibilidades de fraudes financeiras e referências ao caso da Cambridge Analytica.

Por fim, a legislação prevê a criação de uma autoridade nacional, responsável por garantir a aplicação e orientar sua implementação, tema que será aprofundado melhor na próxima seção. No entanto, no que se refere ao setor público, essa autoridade possui a competência de requisitar informações sobre o tratamento de dados realizado por órgãos e entidades, além de emitir pareceres técnicos para assegurar a conformidade com a legislação.

Além disso, cabe a ela estabelecer diretrizes complementares sobre a comunicação e o compartilhamento de dados pessoais entre entes públicos, conforme previsto na própria LGPD.

1.2.1 A Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados (ANPD) foi instituída pela LGPD, se consolidando como autarquia de natureza especial, com autonomia técnica e decisória, conforme art. 55-A da Lei 13.709/2018., após a terceira alteração legislativa, por meio da redação dada pela MP 1.124/2022, convertida em na Lei 14.460/2022.

Lima (2020, p. 45) ressalta que "a regulação exercida pela ANPD é exercida de forma transversal não só em relação à Administração Pública, notadamente no que se refere a políticas públicas exercidas diretamente ou indiretamente, como também sobre os setores econômicos que realizam tratamento e compartilhamento de dados pessoais, sejam atividades puramente privadas ou de interesse público, de tal forma que deve haver um necessário equilíbrio nas competências normativas do regulador".

Ao analisar a trajetória da criação da ANPD, observa-se que o processo de sua institucionalização foi influenciado por modelos internacionais bem-sucedidos e também por peculiaridades do contexto brasileiro. Nesse sentido, Frazão (2023, p. 703) destaca:

> é possível dizer, então, que a defesa da criação de uma Autoridade Nacional de Proteção de Dados replicou, de um lado, aprendizados de um modelo de amplo sucesso internacional e, de outro, dado o diagnóstico brasileiro, atacou problemas que lhe eram especificamente inerentes. De forma a garantir independência e técnica, almejou congregar em um único ente uma série bastante ampla de funções. Em rol longo, porém não exaustivo, viu-se a Autoridade potencial responsável pela normatização, pela implementação, pela formulação, pelo fomento, pela sanção, pela educação e pela oitiva da sociedade. As atividades específicas que o debate lhe sugeriu variaram desde uma ampla capacidade normativo-regulatória até competências de auditoria e de gerenciamento de transferência internacional.

Nesse sentido, foi realizada uma pesquisa das competências atribuídas à ANPD, conforme estabelecido no artigo 55-J da LGPD. A partir da identificação dessas competências, procedeu-se à sua reorganização em grupos, de acordo com a natureza de cada uma. A estrutura adotada foi apresentada em colunas, indicando a natureza da competência, o

inciso correspondente e observações complementares que contribuíssem para o melhor entendimento das atribuições legais da ANPD, conforme segue:

Tabela 2 - Classificação das Competências da ANPD

Natureza	Competências Associadas	Informações Adicionais
Normativa	III, XIII, XVIII, XX	Refere-se à criação de normas, regulamentos e diretrizes para garantir a conformidade com a LGPD.
Fiscalizatória	IV, XI, XVI, XXII, XXIII	Relacionada à supervisão e imposição de sanções em caso de descumprimento da legislação.
Sancionatória	IV, XX, XXI, XXII	Trata da aplicação de penalidades administrativas e encaminhamento para providências judiciais.
Consultiva/Orientativa	I, II, XIV, XX	Engloba a interpretação da legislação e a prestação de esclarecimentos sobre a LGPD.
Educativa	VI, VII, VIII, XIX	Relacionada à promoção do conhecimento e capacitação da sociedade e empresas sobre proteção de dados.
Cooperativa	IX, XIV, XXIII	Abrange parcerias e articulações com outros órgãos e entidades nacionais e internacionais.
Administrativa/Gestão	XII, XV, XVII, XXIV	Relacionada à organização e gestão interna da ANPD, incluindo arrecadação e processos administrativos.

Fonte: Elaborada pela autora.

Dentre as competências abordadas na tabela anterior, é importante detalhar 02 (duas) naturezas da competência que têm impacto direto na atuação do poder público em observância à LGPD, quais sejam: fiscalizatória e educativa.

A função fiscalizatória será abordada minuciosamente na seção seguinte onde abordaremos sobre as sanções aplicadas a órgãos públicos, no entanto, merece considerações iniciais, a saber: (i) a autoridade poderá aplicar penalidades a órgãos públicos que descumprir, embora haja limitações quanto à imposição de multas; (ii) monitoramento contínuo aos órgãos públicos, através de solicitação de informações sobre o tratamento de dados realizado pelo

poder público; (iii) submissão dos órgãos públicos a auditorias; (iv) comunicação aos órgãos de controle interno o descumprimento da LGPD por órgãos públicos para medidas corretivas.

Quanto à função educativa, compete: (i) a capacitação contínua de servidores e órgãos públicos da correta implementação da legislação; (ii) editar regulamento e diretrizes específicas para o setor público, adequando as regras à realidade da administração pública.

De acordo com as competências expostas e o texto da lei, a ANPD é a figura central na aplicação da legislação, sendo que os agentes de tratamento, tanto públicos quanto privados, estão sujeitos à sua atividade regulatória.

1.2.2 Sanções aplicáveis ao tratamento de dados realizados por órgãos públicos

A legislação prevê a responsabilização em caso de descumprimento de suas diretrizes. As sanções estão previstas especificamente no Capítulo VIII - Da Fiscalização e têm como objetivo garantir a conformidade por parte dos agentes de tratamento de dados, prevenindo e desencorajando infrações.

O rol do art. 52 da Lei 13.709/2018, dispõe sobre diversas sanções administrativas. No corpo do texto, incluímos apenas as que estão vigentes e grifamos as sanções aplicáveis ao poder público, conforme mencionado no §3º do referido artigo. No entanto, mantivemos as duas sanções que não se aplicam a órgãos públicos, pois são as únicas que preveem sanções financeiras, onde faz parte de uma das hipóteses discutidas no presente estudo. Vejamos:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)
> **I - advertência, com indicação de prazo para adoção de medidas corretivas;**
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> **IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;**
> **V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;**
> **VI - eliminação dos dados pessoais a que se refere a infração;**
> (...)
> **X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)**
> **XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)**

> **XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019) (*grifo nosso*)**

A partir da análise das infrações no âmbito do poder público, constatam-se as seguintes questões: i) não há previsão de multa pecuniária; ii) parte das sanções são corretivas e impactam apenas a imagem da gestão; iii) há possibilidade de suspensão do banco de dados e/ou do exercício da atividade por prazo determinado, bem como de proibição parcial ou total do exercício da atividade.

Isto é, ao analisar as alternativas sancionatórias mais coercitivas à ausência de multa pecuniária, surge um problema mais grave do ponto de vista da população: a possibilidade de suspensão do tratamento de dados ou até mesmo da atividade desempenhada pelo órgão. A consequência lógica de tal medida é o comprometimento de serviços essenciais à população, especialmente em setores que lidam com políticas públicas fundamentais, como saúde, educação e assistência social.

Enquanto sanções meramente corretivas podem servir como um mecanismo de ajuste sem comprometer a continuidade dos serviços públicos, a suspensão de atividades gera um efeito colateral severo. Diante disso, surge um questionamento essencial: Será que sem a imposição de uma sanção corretiva é capaz de assegurar a aplicação? Será que a suspensão de possíveis políticas públicas, quando se trata de um direito fundamental, é uma medida razoável diante do impacto direto à população?

A legislação estabelece o papel da Autoridade Nacional, já abordada na seção anterior deste estudo, tanto na regulamentação das sanções administrativas (art. 53 da LGPD) quanto no exercício da atividade fiscalizatória, por meio de processo administrativo que assegure o respeito ao contraditório e à ampla defesa (art. 53, § 1º).

A ANPD informou no seu site oficial que o objetivo é criar um ambiente estimulador de comportamentos e tomada de decisões em conformidade com a LGPD. Para isso, a atuação fiscalizatória é pautada por princípios como cooperação, eficiência, racionalidade, proporcionalidade e transparência. Esses são os elementos fundamentais da regulação responsiva.

Para aprofundar o estudo, foi realizada uma pesquisa no site oficial da ANPD com o objetivo de analisar as regulamentações que possuem relação com o tema abordado nesta seção. Para isso, acessou-se a seção "Acesso à Informação", seguida das opções "Institucional" e "Atos Normativos". Nessa área, são disponibilizados atos normativos

inferiores a decretos editados pela ANPD, sendo selecionada a opção "Regulamentações da ANPD".

Dentre as regulamentações o presente estudo abordará apenas as que tratam sobre o objeto proposto, quais sejam: (i) Resolução CD/ANPD nº 1, de 28 de outubro de 2021 que trata sobre o processo de fiscalização e administrativo sancionador; (ii) Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, que regulamenta a dosimetria e aplicação de sanções administrativas.

Quanto às sanções impostas ao poder público, regulamentadas pela ANPD na Resolução CD/ANPD nº 4/2023, prevê a possibilidade de aplicação de advertência, publicização da infração e/ou proibição total ou parcial do exercício de atividades relacionadas a tratamento de dados. No entanto, tais penalidades não interferem nas determinações previstas em legislações correlatas, como a Lei de Acesso à Informação, Improbidade Administrativa e o Regime Jurídico dos Servidores Públicos.

Paralelamente, buscou-se a localização dos processos administrativos em andamento e foi possível constatar dois procedimentos distintos onde o primeiro é de monitoramento e o segundo de fiscalização, ambos em andamento, com vários agentes de tratamento submetidos ao procedimento. No entanto, no presente momento da pesquisa, o estudo se restringe à análise dos tipos de sanções aplicáveis ao tratamento de dados realizado por órgãos públicos.

Embora a ANPD desempenhe um papel fundamental na fiscalização e monitoramento, é importante ressaltar que os órgãos públicos também podem ser submetidos à fiscalização realizada por outras entidades de controle, como, por exemplo, o TCU e os Tribunais de Contas Estaduais, que, em sua função de controle externo, têm realizado auditorias nos órgãos públicos para avaliar o grau de cumprimento da LGPD.

Superada a análise das sanções em âmbito administrativo, é importante destacar a possibilidade de acionamento do Poder Judiciário para ajuizamento de processos judiciais visando à reparação de danos decorrentes do descumprimento da norma sobre tratamento de dados. Nessa seara, não se exclui a possibilidade de o poder público ser condenado pecuniariamente por danos causados.

No entanto, quanto a esse ponto, é importante esclarecer que o Superior Tribunal de Justiça (AREsp 2.130.619, Rel. Ministro Marco Buzzi, julgado em 10/03/2023) possui entendimento consolidado de que o simples vazamento de dados pessoais não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo

necessária a demonstração, por parte do titular dos dados, de prejuízo efetivo decorrente da exposição das informações. Situação distinta ocorre no caso de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa.

Nesse sentido, quando órgãos públicos realizam o tratamento de dados pessoais de maneira contrária aos parâmetros legais e constitucionais, incluindo a divulgação de informações fora das situações excepcionais de sigilo previstas na Constituição, o Estado poderá ser responsabilizado civilmente pelos prejuízos causados aos indivíduos. Nesses casos, será possível o exercício do direito de regresso contra os agentes públicos ou políticos envolvidos, desde que comprovada a existência de dolo ou culpa.

1.2.3 A relação entre a LGPD e a LAI

Antes de adentrarmos no tema propriamente dito, é válido destacar que, apesar da existência de diversas normativas que tratam de dados na administração pública, o presente trabalho fez um recorte para analisar apenas a LAI e a LGPD. Essa escolha se justifica pelo fato de essas leis serem as mais debatidas e utilizadas no âmbito dos Tribunais de Contas e órgãos públicos. Além disso, seu estudo é fundamental para alcançar o objetivo proposto.

Com o avanço contínuo das tecnologias da informação e a consolidação de uma sociedade conectada em rede, a atuação do Estado também passou a ser marcada pela intensificação da digitalização de dados e pelo intercâmbio de informações entre órgãos públicos. Muitos desses dados passaram a ser disponibilizados online, acessíveis ao público em geral. Um marco importante nesse processo foi a promulgação da Lei nº 12.527/2011, que regulamenta o acesso à informação e autoriza, por exemplo, a divulgação dos valores pagos a servidores públicos. Diante dessa nova realidade, surge o desafio de equilibrar a transparência administrativa com a garantia de direitos fundamentais como a privacidade e a intimidade, como apontam Ribas do Nascimento e Schorn Rodrigues (2013, p. 193).

Assim, um dos principais pontos de conflito no tratamento de dados por órgãos públicos está na tensão entre os princípios da transparência e da proteção de dados pessoais. De um lado, a publicidade é a regra, e o sigilo da informação, a exceção. Por outro lado, o sigilo é um fator fundamental para a proteção de dados. Nesse sentido, surge o desafio: como garantir a eficácia da lei sem infringir a própria lei?

Frazão (2023) observa que o direito de acesso à informação, seja ela de interesse individual, coletivo ou geral, possui natureza de direito fundamental, ocupando o mesmo patamar constitucional da privacidade. Tal entendimento decorre do artigo 5º, inciso XXXIII, da Constituição Federal, que assegura a todos os cidadãos o direito de obter informações dos órgãos públicos, ressalvadas aquelas cujo sigilo seja essencial para a proteção da sociedade ou do Estado.

A publicidade é condição indispensável para que os atos administrativos gerem efeitos fora da administração, uma vez que sua eficácia perante terceiros depende da sua divulgação. Sem essa publicização, o ato, embora juridicamente válido, pode não produzir resultados concretos. Nesse sentido, a transparência representa o instrumento por meio do qual se viabiliza o princípio da publicidade, previsto no caput do artigo 37 da Constituição Federal de 1988 como um dos pilares da administração pública.

A LAI surge a partir do direito fundamental de acesso à informação, previsto na Carta Magna. Dessa forma, a administração pública tem o dever de publicar seus atos administrativos independentemente de requerimento, garantindo transparência na gestão pública. Ambos os preceitos debatidos possuem origem constitucional, não havendo, portanto, hierarquia entre as normas.

Nesse sentido, Serafini (2023) conclui que as duas legislações não conflitam entre si, uma vez que a LGPD permite que a administração pública trate dados pessoais visando ao interesse coletivo, estabelecendo um certo controle sobre sua utilização, em conformidade com o princípio da finalidade pública. Além disso, a LGPD também atua nas áreas de exceção ao acesso à informação previstas na LAI.

Costa (2023) também concluiu, por meio de estudos empíricos, que o conflito entre as normas não é real, mas apenas aparente. A controvérsia em torno da disponibilização dos dados deve ser abordada no sentido de garantir o tratamento adequado dessas informações, e não sua indisponibilidade. Um ponto que merece destaque é a ênfase dada à necessidade de capacitação contínua dos servidores, bem como à atuação de uma equipe multidisciplinar para assegurar a correta aplicação das normas.

O artigo 23 da LGPD autoriza o tratamento de dados pessoais pelo poder público, desde que para a realização de políticas públicas ou o cumprimento de obrigações legais, com expressa menção à LAI. Isso evidencia a intenção de alinhamento entre as duas legislações,

permitindo que, quando o interesse público estiver em pauta, o tratamento de dados pessoais seja permitido.

Além da LGPD, a LAI também se preocupa com a privacidade, na medida em que determina que os órgãos públicos devem proteger a informação pessoais, bem como garantir que o tratamento dessas informações sejam com respeito à intimidade, vida privada, honra e imagem das pessoas. Além disso, o artigo 31, § 3º, inciso V da LAI e o artigo 7º, § 3º da LGPD apresentam uma harmonia: permitem a dispensa de consentimento para o tratamento de dados pessoais quando o interesse público justificar a sua divulgação ou tratamento. De um lado, a LAI facilita o acesso às informações pessoais quando for necessário para garantir um interesse público, de outro lado, a LGPD estabelece que dados de acesso público podem ser tratados sem consentimento, justificando sua disponibilização.

Enquanto a LAI busca garantir tanto o acesso ativo quanto passivo às informações públicas, além de resguardar os dados pessoais, a LGPD tem como foco principal assegurar que os titulares possam obter informações claras, objetivas e acessíveis sobre seus dados e sobre as práticas adotadas em seu tratamento, ou seja, incorporando diretrizes voltadas à transparência.

Nesse sentido, cabe ao profissional assegurar a correta aplicação das legislações, na medida em que o caso concreto surja, definindo quais dados estarão sujeitos a restrições de acesso e de que forma isso ocorrerá, em favor da transparência pública. Verifica-se uma questão central importante para o estudo acadêmico, superando a análise do conflito entre as normas uma vez que elas não são conflitantes, surge a necessidade de identificação através de pesquisa empírica se a LGPD está sendo utilizada como mecanismo para ocultar informações de interesse público nos pedidos de acesso à informação da LAI.

Assim, conclui-se que a correta aplicação das duas normativas está diretamente relacionada ao grau de maturidade dos órgãos públicos. Esse nível de maturidade pode ser verificado por meio das auditorias realizadas pelo Tribunal de Contas da União, que serão objeto de estudo na presente dissertação. No entanto, o tema abordado nesta seção é fundamental para a construção do objeto proposto neste trabalho.

1.3 Lições extraídas

A partir do reconhecimento da proteção de dados pessoais como direito fundamental, emergem consequências importantes para a Administração Pública, especialmente para os

órgãos que atuam como controladores desses dados. A digitalização crescente dos serviços públicos, que antes ocorriam em formato físico e agora são amplamente realizados por meios eletrônicos, trouxe inúmeras facilidades para o cidadão, como a possibilidade de acessar serviços e realizar transações diretamente de dispositivos digitais. Contudo, essa transformação também ampliou significativamente a exposição a riscos cibernéticos, evidenciando novas vulnerabilidades que precisam ser cuidadosamente gerenciadas.

No contexto dos órgãos públicos, este capítulo evidenciou os diversos agentes que podem atuar como vetores de ataques, que vão desde hackers externos até servidores internos, além dos variados tipos de ataques, como engenharia social (phishing e spear phishing), ransomware, exfiltração de dados, entre outros. O conhecimento dessas ameaças é fundamental para aprimorar as auditorias e desenvolver estratégias que minimizem as vulnerabilidades mais frequentes.

Diante da diversidade e sofisticação das ameaças, é imprescindível que as instituições públicas adotem medidas preventivas robustas e integradas, que incluem tanto soluções tecnológicas avançadas, como criptografia, firewalls e sistemas de detecção, quanto a promoção de uma cultura organizacional de segurança da informação. Práticas como: o treinamento contínuo dos servidores, controle rigoroso de acesso, campanhas internas de conscientização, políticas eficazes de descarte e backup, e monitoramento de tráfego de dados são essenciais para mitigar os riscos e garantir a integridade dos dados pessoais.

As auditorias realizadas pelos Tribunais de Contas devem, portanto, contemplar esses aspectos de forma integrada, buscando identificar lacunas nos controles de segurança e recomendar medidas corretivas eficazes. Essa atuação fiscalizatória assume papel central na proteção dos dados pessoais, reforçando a responsabilidade estatal vinculada ao respeito aos direitos fundamentais, como a privacidade, a dignidade, a liberdade de expressão e a autodeterminação informativa dos cidadãos.

Além disso, o papel do encarregado de proteção de dados, previsto pela legislação e regulamentado pela ANPD, emerge como um elemento-chave para a governança e conformidade dos órgãos públicos. A auditoria deve verificar a formalização e atuação desse profissional, garantindo que seu trabalho esteja alinhado com as diretrizes estabelecidas e com os princípios da LGPD.

O estudo também evidenciou uma lacuna importante entre as normas e sua aplicação prática, como ilustrado pelo compartilhamento de dados pelo IBGE. Embora existam

requisitos técnicos definidos, a observância dos princípios da razoabilidade e proporcionalidade implica uma análise caso a caso, o que torna desafiadora a métrica objetiva dessa ponderação em auditorias. Esse aspecto revela uma complexidade que merece aprofundamento acadêmico, pois impacta diretamente a efetividade da proteção de dados no setor público.

Outro ponto importante é a relação entre a LGPD e a LAI. Conclui-se que essas legislações não são conflitantes, mas complementares, e sua correta aplicação requer que o órgão público possua um grau adequado de maturidade em governança da informação. Essa maturidade envolve a capacidade de avaliar e balancear princípios como transparência e proteção de dados pessoais, respeitando os limites legais e os direitos dos cidadãos.

Para a auditoria, isso implica a necessidade de ir além da verificação formal do cumprimento normativo, adotando uma abordagem que avalie o nível de maturidade da instituição, sua capacidade de gestão de riscos e sua cultura organizacional. A auditoria deve buscar identificar não apenas falhas pontuais, mas também a existência de processos robustos que permitam a tomada de decisões ponderadas e alinhadas às exigências legais.

2. A LGPD E O PAPEL DO TRIBUNAL DE CONTAS DA UNIÃO

A elevação da proteção de dados pessoais ao status de direito fundamental, consolidada com a promulgação da Emenda Constitucional nº 115/2022, ampliou de maneira significativa as responsabilidades do Estado na garantia desse direito. Conforme abordado no capítulo anterior, a garantia dos direitos fundamentais não se limita à sua dimensão subjetiva, voltada à proteção individual de cada cidadão. Pelo contrário, a teoria da dimensão objetiva dos direitos fundamentais, impõe ao Poder Público o dever de implementar políticas e mecanismos institucionais que assegurem a concretização desses direitos de forma ampla.

Dentro desse contexto, os Tribunais de Contas, enquanto órgãos de controle externo, assumem papel central na fiscalização da efetividade da proteção de dados no setor público. A sua atuação transcende a simples verificação de legalidade formal, exigindo desenvolvimento de atividades fiscalizatórias proativas.

Para compreender o alcance da atuação do TCU em relação à proteção de dados pessoais, faz-se necessário compreender previamente sua estrutura organizacional, suas competências, funções institucionais e os principais instrumentos de fiscalização disponíveis. Neste primeiro momento a análise será desenvolvida de forma mais abrangente, apresentando

o contexto geral de atuação do TCU. Em seguida, nos subcapítulos serão realizadas abordagens individuais sobre cada tipo de auditoria, com o objetivo de identificar suas características, finalidades e potenciais aplicações na implementação da LGPD no setor público.

Essa análise preliminar será fundamental para, no capítulo seguinte, verificar qual modalidade de auditoria foi efetivamente utilizada pelo tribunal no acompanhamento da proteção de dados e, com base nos parâmetros discutidos anteriormente, avaliar qual seria a abordagem fiscalizatória mais adequada para esse contexto.

O reconhecimento da proteção de dados como tema relevante de governança também se refletiu na agenda institucional do TCU. A inclusão da matéria nas ações estratégicas demonstra a preocupação em acompanhar a evolução e induzir o aprimoramento das práticas administrativas relacionadas à proteção de dados.

Um exemplo concreto é a inserção, no Plano Anual de Trabalho (PAT) 2024 da Rede Integrar, da Ação 29, cujo objetivo é verificar a evolução do cumprimento da legislação pelos órgãos e entidades da Administração Pública. Essa nova auditoria, no entanto, será conduzida em parceria com Tribunais de Contas Estaduais, o que permitirá ampliar o escopo da avaliação.

Ao final deste capítulo, será possível extrair lições fundamentais: (i) o Tribunal de Contas da União dispõe de instrumentos adequados e consolidados para a fiscalização da implementação da LGPD no setor público; (ii) A escolha da metodologia de auditoria: operacional, de conformidade ou financeira, dependerá dos objetivos específicos de cada fiscalização, aspecto que será aprofundado no capítulo seguinte.

2.1 Tribunal de Contas da União: Noções introdutórias

A relação entre o Estado e os dados pessoais dos cidadãos é marcada por um notável desequilíbrio de poder. Esse descompasso resulta, de um lado, da autoridade conferida ao ente público, detentor de prerrogativas típicas do poder estatal, e, de outro, da condição estrutural de concentrar grandes volumes de informações pessoais em suas bases, em razão das funções que desempenha. Não raro, tais dados possuem natureza sensível, o que eleva os riscos envolvidos e amplia a responsabilidade do Estado na sua gestão.

O exercício da atividade administrativa é inerente à própria ideia de Estado. Ao assumir a missão de organizar a vida em sociedade, o Estado assume também a

responsabilidade de gerir recursos públicos: dinheiro, bens e valores, em prol do interesse coletivo. Esse gerenciamento é feito por meio da Administração Pública, que executa políticas públicas e presta serviços essenciais à população.

Diante dessa ampla gama de atribuições e do impacto direto de suas ações sobre os direitos individuais, especialmente no tratamento de dados pessoais, torna-se indispensável a existência de mecanismos eficazes de controle contra a atuação estatal. O regular funcionamento do Estado de Direito, conforme concebido nas democracias modernas, pressupõe que todo o poder seja fiscalizado e limitado por outros poderes e instituições de controle. Trata-se da consagração do princípio dos freios e contrapesos, desenvolvido por Montesquieu, segundo o qual "o poder deve frear o poder", evitando abusos e garantindo o equilíbrio institucional.

A noção de Estado de Direito está diretamente vinculada à existência de mecanismos de controle, pois para que o Estado efetivamente exista, é imprescindível a criação de instituições e instrumentos que assegurem o cumprimento das normas legais pelos agentes públicos. Nessa perspectiva, Mello Junior (2001, p. 153) ressalta que “a relevância do controle exercido sobre o poder estatal está relacionada tanto à sua indispensabilidade quanto à eficiência e regularidade com que é realizado”.

Há diversas formas de classificar os mecanismos de controle da Administração Pública, levando-se em consideração aspectos como o órgão responsável por sua execução, o momento em que é realizado, a maneira como se inicia, a abrangência e a profundidade do controle, entre outros critérios. Contudo, para manter o foco na proposta central deste trabalho, a análise será restrita à classificação baseada na posição institucional dos entes envolvidos no processo de fiscalização, abordando apenas as modalidades de controle interno e externo.

O controle interno corresponde à fiscalização realizada pela própria Administração Pública sobre seus atos. Por outro lado, o controle externo é exercido por órgãos independentes, situados fora da estrutura administrativa responsável pela execução do ato, tendo como finalidade a supervisão e o controle das ações administrativas por entidades com competência constitucional para tal, como é o caso dos Tribunais de Contas e do Poder Legislativo.

Nesse contexto de fiscalização e limitação do poder estatal, os Tribunais de Contas surgem como órgãos constitucionais especializados, que auxiliam o Poder Legislativo no

controle externo da Administração Pública. Sua função vai além da simples verificação da correta aplicação dos recursos públicos, abrangendo também o exame da legalidade, legitimidade e eficiência dos atos administrativos, contratos, licitações e políticas públicas implementadas. Por meio de auditorias, os Tribunais de Contas promovem a transparência, a responsabilização e a proteção do interesse público em suas múltiplas dimensões.

Essa competência está prevista no art. 70 da Constituição Federal de 1988, o qual estabelece que: *"A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder."*

A Corte de Contas é um tribunal administrativo, responsável pela fiscalização dos gastos públicos. Órgão colegiado, é formado, no âmbito Federal, por 09 (nove) Ministros, indicados pelo Congresso Nacional e pelo Presidente da República, dentre os quais há integrantes oriundos das carreiras dos auditores e membros do *Parquet* de Contas, conforme art. 73 da Carta Magna.

Situa-se no ordenamento jurídico-constitucional como órgão público especializado e independente, que colabora com o Poder Legislativo prestando-lhe auxílio técnico, bem como aos demais poderes, visando resguardar a probidade e eficiência da Administração Pública. “Sendo assim, o Tribunal de Contas é uma das garantias institucionais da liberdade, pois garante os direitos fundamentais, em razão de sua singularidade no quadro institucional do país” (COSTA, 2005, p. 56).

É relevante enfatizar que o conceito de auxílio, no contexto da atuação dos Tribunais de Contas, deve ser interpretado como um exercício de cooperação institucional, desvinculado de qualquer ideia de subordinação administrativa ou hierárquica. Na prática, o Tribunal atua de maneira colaborativa junto aos três Poderes da República, mantendo-se, entretanto, com plena independência, tanto em sua estrutura organizacional quanto na condução de suas funções típicas de controle.

Moreira Neto (2002) entende que o princípio jurídico é uma norma de caráter indicativo, cuja principal finalidade é apontar valores ou objetivos que devem ser genericamente buscados por todas as normas do ordenamento jurídico, independentemente do grau de concretização alcançado em cada caso. Em outras palavras, os princípios atuam como

diretrizes superiores que orientam a criação, a interpretação e a aplicação das regras jurídicas, permitindo que órgãos de controle, como os Tribunais de Contas, desempenhem suas funções com foco na proteção do interesse público e na efetivação dos fins constitucionais.

Os princípios que norteiam a atuação dos Tribunais de Contas estão expressamente previstos no art. 70 da CF, quais sejam: os princípios da legalidade, legitimidade e economicidade. Tais princípios possuem força normativa cujo grau de incidência pode variar, exigindo, em muitos casos, um processo gradual de concretização por meio de regramentos infraconstitucionais que lhes atribuam a densidade necessária para garantir coerência e legitimidade ao ordenamento jurídico, ainda assim, reconhece-se que detêm aplicabilidade direta e imediata.

O princípio da legalidade impõe à Administração Pública a obrigação de atuar conforme os limites estabelecidos pela legislação. No entanto, como observa Costa (2005, p. 70), é fundamental compreender que a atuação dos Tribunais de Contas vai além de um controle meramente formal e documental. Segundo o autor, deve-se considerar que "a ação dos Tribunais de Contas não está jungida tão-somente ao controle documental e burocrático dos atos levados a efeito pelo administrador público", mas deve também analisar se a aplicação da norma legal, no contexto social em que se insere, realmente atende aos objetivos do interesse público. Para tanto, é necessário levar em conta o conjunto de princípios que orientam a Administração Pública, superando uma visão puramente legalista do controle.

O princípio da economicidade orienta a Administração Pública a buscar a melhor relação entre custo e benefício na aplicação dos recursos públicos, evitando desperdícios e promovendo a eficiência na execução das políticas e serviços destinados à sociedade. Já o princípio da legitimidade complementa essa diretriz ao exigir que todos os atos administrativos estejam não apenas em conformidade com a lei, mas também alinhados aos valores constitucionais, à moralidade, à ética e ao interesse público, garantindo que a atuação estatal seja justa, adequada e comprometida com os fins sociais para os quais o poder público foi instituído.

As competências do Tribunal de Contas, plasmadas no texto constitucional de 1988 (art.71), visam efetivar o controle da Administração Pública. Esse controle é próprio dos Estados de Direito e, principalmente, democráticos, e tem o propósito de se proceder à verificação, quanto à observância dos princípios e das normas constitucionais, em todo universo de atuação administrativa, a qual deve estar sempre focada na satisfação do interesse

público, que reflete fator de proteção não só para os cidadãos, como também para a própria Administração Pública (COSTA, 2005, p. 14).

Quanto à função consultiva, considera-se o exame de consultas elaborado por autoridade competente elencadas em seu artigo 216, do Regimento Interno, e Art. 71, I, da CF, a respeito da dúvida suscitada na aplicação de dispositivo legal, sendo de caráter normativo e constitui prejulgamento da tese, ou seja, não há em relação ao caso concreto.

Ao analisar o contexto histórico, observa-se o surgimento da função fiscalizadora nos diversos textos constitucionais. Outrossim, percebe-se que, com o advento da Constituição de 1988, houve uma ênfase maior nas competências da Corte, abrangendo a conformidade com as normas e princípios, assegurando, inclusive, os direitos fundamentais.

Além disso, vale destacar que a ampliação da atuação resulta na competência por parte do TCU, referente à auditoria de natureza contábil, financeira, orçamentária, operacional e patrimonial, conforme estabelecido no artigo 71, inciso IV, da Constituição Federal, bem como pelo art. 1, II, da Lei n 8.443/92, Orgânica do Tribunal de Contas da União.

Sobretudo, é no contexto da atividade de controle que as Cortes de Contas assumem especial relevância, sobressaindo a missão conferida a esta pelo Constituinte. Denota-se, por conseguinte, embasado no artigo 70, que a norma estabelece o controle externo mediante auditoria, levantamento de auditoria, inspeções e acompanhamento.

Segundo Braga (2025, p. 275), “no âmbito da proteção de dados, é possível identificar tipos de processos aptos a bem atuar na defesa do direito fundamental.” Esses processos, disciplinados a partir do artigo 230 do Regimento Interno do TCU, podem se originar de diferentes fontes, como iniciativa do próprio tribunal, solicitações do Congresso Nacional, ou ainda por meio de representações e denúncias. Dependendo da metodologia adotada, classificam-se em diferentes formatos, tais como auditorias, inspeções, levantamentos, monitoramentos e acompanhamentos.

Já a função informativa, surge para assegurar que as competências do TCU estão sendo devidamente cumpridas, através da prestação de informações ao Congresso Nacional. Com relação à função jurisdicional, observa-se que é uma das funções mais importante, visto que decorre do princípio fundamental da ordem constitucional brasileira, sendo obrigatória a prestação de contas por parte da administração pública, obedecendo assim os preceitos estabelecidos.

A função corretiva baseia-se na competência do mesmo para deliberar prazo para a correção de irregularidades e sustar atos, quando for constatada a inércia do Parlamento. Por outro lado, a função sancionadora consiste na aplicação das sanções previstas na Lei Orgânica, decorrente de ilegalidade de despesa e irregularidade nas contas, por parte dos responsáveis.

Por fim, a função normativa consiste na expedição de instruções e atos normativos, sendo obrigatório o cumprimento dos mesmos, sob pena de responsabilização do infrator. Outrossim, a função de ouvidoria, que surgiu no texto da Constituição atual, compreende os processos julgados pelo TCU, a título de denúncia ou representação, ligados ao controle social da gestão pública.

Diante desse contexto, cabe ao TCU verificar se as práticas adotadas pelas unidades jurisdicionadas para o tratamento de dados pessoais estão alinhadas aos parâmetros de controle já mencionados ao longo deste estudo. Essa verificação não se limita a um aspecto específico, abrangendo diferentes dimensões da gestão de dados. Entre os pontos que podem ser objeto de análise estão: a existência de normas internas sobre o tema, as medidas de segurança da informação implementadas, a estrutura dos sistemas utilizados para tratamento e compartilhamento de dados, os critérios estabelecidos para escolha e capacitação dos agentes responsáveis, os procedimentos para comunicação de incidentes de segurança e, ainda, as formas de relacionamento e transparência com os próprios titulares dos dados.

2.2 Auditoria no controle externo do tribunal de contas

Abordaremos neste estudo os tipos de auditoria externa, realizada no âmbito do setor público. Trata-se de um processo conduzido por profissionais qualificados e independentes em relação ao órgão auditado, garantindo imparcialidade na fiscalização. Conforme demonstrado, no Brasil, essa estrutura é regulamentada pela Constituição Federal e exercida pelos Tribunais de Contas e demais órgãos de controle.

Segundo ARAÚJO (2008, p.15) “é do conhecimento de todos os que labutam com o tema, o termo *auditoria,* etimologicamente falando, origina-se do latim *audire*, “ouvir”. Inicialmente os ingleses o traduziram como *auditing* para designar, exclusivamente, o conjunto de procedimentos técnicos para a revisão de registros contábeis”.

As Normas Brasileiras de Auditoria do Setor Público (NBASP)[1] foram desenvolvidas com base nas diretrizes da Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), passando por um processo de adaptação para atender às especificidades do sistema jurídico e administrativo brasileiro.

Segundo a INTOSAI (2024, p. 1), "normas e diretrizes profissionais são essenciais para a credibilidade, a qualidade e o profissionalismo da auditoria do setor público." Nesse contexto, as ISSAI foram elaboradas com o objetivo de assegurar que as instituições de controle exerçam suas funções com independência e eficiência. Elas também fornecem um referencial técnico para que os membros da organização desenvolvam práticas de auditoria alinhadas às suas competências legais e realidades nacionais, respeitando seus marcos normativos internos.

A ISSAI 100 define três tipos de auditoria e seus respectivos objetivos. Além disso, ao pesquisar no portal do TCU, é possível identificar três categorias de auditoria: operacional, de conformidade e financeira.

A seguir, será apresentada uma tabela, elaborada pelo TCU, que tem como propósito apresentar uma visão comparativa entre os principais tipos de auditoria utilizados no âmbito do controle externo: auditoria operacional, auditoria de conformidade e auditoria financeira. Seu objetivo é demonstrar que cada modalidade de auditoria possui características metodológicas distintas, refletindo diferentes finalidades de fiscalização e enfoques de análise.

Para isso, a tabela organiza os elementos essenciais que diferenciam essas auditorias, como os conceitos-chave, o objetivo principal, o papel esperado do auditor, as áreas de conhecimento predominantes, os critérios utilizados na avaliação, o funcionamento esperado do objeto auditado e o perfil do gestor, veja-se:

Tabela 3 - Quadro comparativo entre tipos de auditoria

Característica	**Auditoria Operacional**	**Auditoria de Conformidade**	**Auditoria Financeira**
Conceitos-chave	Economia, eficiência, eficácia, efetividade	Conformidade com leis e regulamentos	Materialidade, demonstrações financeiras livres de erros materiais

[1] As Normas Brasileiras de Auditoria do Setor Público (NBASP) são emitidas pelo Instituto Rui Barbosa (IRB), do qual são membros o TCU e os demais Tribunais de Contas brasileiros.

Objetivo	Contribuir para a melhoria da gestão pública	Verificar se o gestor atuou de acordo com normas aplicáveis	Aumentar o grau de confiança nas demonstrações por parte dos usuários previstos.
Papel do auditor	Avaliar o desempenho	Verificar se há discrepância entre a situação encontrada e a lei ou norma	Expressar opinião quanto a estarem as informações financeiras livres de distorções relevantes devido a fraude ou erro
Principais áreas de conhecimento do auditor	Ciências sociais, análise de políticas	Direito	Contabilidade
Critérios	Normas legais, boas práticas, valores profissionais, modelos, experiências	Normas, que incluem leis e regulamentos, resoluções, políticas, códigos, termos acordados ou princípios gerais	Estrutura de relatório financeiro aplicável (normas contábeis) e marco regulatório aplicável
Funcionamento esperado do objeto auditado	Atividades executadas da melhor maneira possível	Atividades, transações, informações aderentes às normas aplicáveis	Demonstrações financeiras de acordo com a estrutura de relatório financeiro aplicável
Perfil do gestor	Flexível, empreendedor	Conformidade com procedimentos	Conformidade com procedimentos

Fonte: Tribunal de Contas da União

O propósito de uma auditoria de natureza financeira é proporcionar maior credibilidade às informações contábeis apresentadas pela organização avaliada. Durante a execução desse processo, cabe ao auditor reunir evidências suficientes que permitam concluir que as demonstrações financeiras não contêm distorções relevantes, seja por falhas intencionais ou equívocos. Ao final, o profissional responsável irá emitir um parecer, indicando se os registros analisados foram preparados em conformidade com as normas contábeis pertinentes.

Segundo Costa e Dutra (2014, p. 54), “o papel da auditoria financeira na estrutura de governança das instituições públicas é estabelecido em padrões internacionais de auditoria governamental emitidos pela Organização Internacional de Entidades de Fiscalização Superior (Intosai)”.

Além da auditoria financeira, o TCU apresenta, na seção "Controle e Fiscalização" de sua página institucional, diversas áreas de atuação do controle externo. Ao acessarmos a categoria "Tecnologia da Informação", é possível encontrar informações sobre a "Auditoria

sobre LGPD", que trata da fiscalização referente à implementação da Lei Geral de Proteção de Dados na União, Estados e Municípios, foco principal do presente estudo, que será detalhado em capítulo específico.

Compreender a distinção entre os diferentes tipos de auditoria é essencial para a adequada delimitação do objeto desta pesquisa. Algumas auditorias possuem caráter preventivo e orientador, enquanto outras têm um enfoque corretivo, buscando identificar irregularidades e propor soluções, cada qual com suas funções e metodologias específicas.

De forma intencionalmente sucinta, foram apresentados os principais aspectos de cada tipo de auditoria na tabela anteriormente exposta, com o objetivo de oferecer um panorama geral das modalidades existentes no âmbito do controle externo. Essa análise permitiu verificar que a auditoria financeira não se alinha ao escopo central desta pesquisa. Por essa razão, os próximos subcapítulos concentrarão a análise nas auditorias operacional e de conformidade, por serem mais relevantes à fiscalização da implementação da LGPD no setor público e, consequentemente, mais alinhadas aos objetivos deste estudo.

Um ponto de reflexão relevante, considerando a temática abordada nesta pesquisa, é que não apenas os serviços oferecidos aos cidadãos passaram a ser digitalizados, como também o próprio serviço público começou a adotar tecnologias visando maior eficiência na prestação de seus serviços. Antes, as auditorias eram realizadas de forma manual, baseadas na materialidade e na experiência do auditor. Com o avanço tecnológico, especialmente com o surgimento da inteligência artificial, passou-se a contar com o auxílio de ferramentas automatizadas para aprimoramento das suas funções.

Segundo o Tribunal de Contas da União (2023), em fevereiro de 2023, o Comitê de Gestão de Tecnologia da Informação aprovou a criação de um grupo de trabalho denominado GT ChatGPT, para fomentar o uso seguro dessas tecnologias na Corte, tendo em vista a capacidade deste modelo de linguagem em gerar textos coerentes através de comandos fornecidos pelos usuários, como fruto desse trabalho conjunto, foi lançado o ChatTCU.

O artigo *"A inteligência artificial nos órgãos constitucionais de controle de contas da administração pública brasileira"*, de Bitencourt e Martins (2023), apresentou um mapeamento das iniciativas de uso de inteligência artificial nos Tribunais de Contas brasileiros. O estudo identificou aplicações voltadas ao apoio em diversas funções internas, contudo, constatou-se que, até a data de sua elaboração, não havia registros de uso da IA para a tomada de decisão nos processos de controle externo. Entre as soluções mapeadas,

destacam-se o sistema APTO (Análise dos Portais da Transparência no Tocantins)[2] e o Esmeralda[3], do TCM-GO, por apresentarem maior proximidade com atividades de fiscalização.

Bitencourt e Martins (2023, p. 7) observam que "a gestão tecnológica na Administração Pública possibilita diversos ganhos de produtividade e eficiência." Contudo, os autores alertam que essas transformações tecnológicas também modificam significativamente as formas de atuação dos Tribunais de Contas. Por isso, torna-se necessário um acompanhamento rigoroso e contínuo, com mecanismos de regulação e controle que assegurem o uso responsável dessas ferramentas, em consonância com o interesse público e a proteção dos direitos fundamentais.

Embora seja inegável que a adoção de tecnologias baseadas em inteligência artificial representa um avanço significativo para a eficiência e a qualidade das funções de controle, é importante destacar que este estudo não tem como foco a análise do Tribunal de Contas da União enquanto controlador de dados pessoais. O objetivo central é examinar a atuação do TCU no exercício do controle externo, especialmente na fiscalização da implementação da LGPD por outros órgãos e entidades da Administração Pública.

Ainda assim, é importante reconhecer que, ao utilizar ferramentas baseadas em inteligência artificial, o próprio TCU vivencia na prática os desafios e as exigências legais relacionados ao tratamento de dados pessoais. Essa experiência interna permite que a Corte de Contas, ao exercer sua função de controle externo, consiga estabelecer uma conexão concreta entre a teoria e a prática no uso dessas tecnologias, servindo como referência ao fiscalizar outros órgãos da administração pública que também vêm incorporando soluções de IA em suas rotinas.

Nos próximos subcapítulos, serão exploradas de forma mais detalhada as diferentes modalidades de auditoria mencionadas neste tópico. A intenção é apresentar as características específicas de cada tipo, suas finalidades e como podem ser aplicadas no contexto da fiscalização da implementação da LGPD pelos órgãos e entidades públicas. Essa abordagem permitirá compreender de que maneira cada metodologia de auditoria pode contribuir para uma análise mais eficaz do cumprimento das obrigações legais relacionadas à proteção de dados pessoais.

---

[2] Analisa os portais da transparência do estado, verificando se disponibilizam todas as informações exigidas por lei e se estão disponíveis para o cidadão.

[3] Realiza auditorias, buscando os riscos das licitações.

2.2.1 Auditoria de conformidade

A auditoria de conformidade no setor público tem como função central permitir que as Entidades Fiscalizadoras Superiores (EFS) verifiquem se as ações das instituições públicas seguem as normas que as regulam. Conforme aponta a INTOSAI (2010, p. 6), "isso envolve relatar o grau em que a entidade auditada cumpre com os critérios estabelecidos". Os relatórios resultantes podem apresentar formatos diversos, indo desde opiniões breves até conclusões mais extensas.

Essa auditoria pode abordar tanto a legalidade, que trata da aderência a leis e normas, quanto a legitimidade, que envolve princípios éticos e padrões de boa gestão. Ainda segundo a INTOSAI (2010, p. 6), "a legalidade é o foco principal da auditoria de conformidade", mas a legitimidade também pode ser considerada, especialmente diante das expectativas do setor público. O escopo da auditoria, portanto, pode incluir ambos os aspectos, a depender do mandato da EFS.

Quanto às características da auditoria objeto de análise, percebe-se a flexibilidade uma vez que poderá cobrir uma variedade ampla de áreas ou temas, bem como a utilização de vários critérios e métodos para obtenção de evidências, do formato do relatório, conclusões variadas a depender do contexto e complexidade do trabalho auditado. Além disso, exerce a característica do fortalecimento das práticas de governança, identificando falhas e legitimidade na aplicação da lei, promovendo a transparência e accountability ao reportar violações a normas, refletindo nesse aspecto a sua natureza preventiva e corretiva.

No tocante aos elementos, é dividido em: (i) normas e critérios: a norma é o elemento principal, pois o conteúdo delas fornecem critérios para realizar a auditoria, essas normas podem incluir regras, leis e regulamentos, resoluções, políticas, códigos estabelecidos; (ii) objeto: é definido pelo escopo e pode envolver atividades, transações ou informações.

Em relação aos princípios, dada a grande quantidade de informações e a importância de um entendimento claro e facilitado, especialmente para posterior análise das auditorias realizadas pelo TCU, que será objeto de estudo no capítulo seguinte, optou-se pela organização dos princípios em uma tabela.

Na criação da tabela, os princípios foram organizados em duas colunas: a primeira contém o nome do princípio, enquanto a segunda apresenta uma breve descrição das suas

diretrizes, o objetivo foi facilitar a consulta ajudando na compreensão de como cada um se relaciona com a auditoria de conformidade e sua implementação no contexto do TCU.

Tabela 4 - Princípios da Auditoria de Conformidade

Princípio	**Descrição**
Julgamento e ceticismo profissionais	Significa que o auditor fará uma avaliação crítica, com uma mente questionadora, acerca da suficiência e da adequação das provas coletadas ao longo de toda a auditoria.
Controle de qualidade	Visando assegurar que a auditoria seja realizada em conformidade com as normas aplicáveis.
Gestão de equipes de auditoria e habilidades	Devem possuir conhecimento, experiência prática e compreensão das normas e da entidade auditada.
Risco de auditoria	Refere-se ao risco de que o relatório pode ser inadequado às circunstâncias da auditoria.
Materialidade	É a utilização de julgamento profissional para avaliar a relevância de questões quantitativas e qualitativas, que podem influenciar as decisões dos usuários.
Documentação	Deve ser elaborada considerando critérios, escopo, julgamentos, evidências e conclusões.
Comunicação	Manutenção de uma comunicação eficaz durante todo o procedimento de auditoria.
Escopo de auditoria	O escopo de uma auditoria é influenciado pela materialidade e pelo risco, e determina quais normas e partes delas serão cobertas.
Objeto e critérios	O objeto e os critérios podem ser definidos por lei
Entendendo a entidade	O auditor deve, portanto, estar familiarizado com a estrutura e as operações da entidade auditada e com seus procedimentos para alcançar a conformidade
Entendendo controles internos e o ambiente de controle	O auditor deve considerar se os controles internos estão em harmonia com o ambiente de controle, de modo a assegurar a conformidade com as normas em todos os aspectos relevantes.
Avaliação de risco	A identificação dos riscos de não conformidade e seu potencial impacto nos procedimentos de auditoria
Risco de fraude	Se o auditor se deparar com casos de não conformidade que possam ser indicativos de fraude, ele deve exercer o devido zelo profissional e cautela de modo a não interferir com eventuais procedimentos legais ou investigações futuras

Estratégia de auditoria e plano de auditoria	Os auditores devem desenvolver uma estratégia e um plano de auditoria.
Evidência de auditoria	Os auditores devem reunir evidências de auditoria suficientes e apropriadas para cobrir o escopo da auditoria, considerando tanto a quantidade quanto a qualidade das evidências, de acordo com os critérios, o objeto e o risco da auditoria.
Avaliando evidência e formando conclusões	Os auditores devem avaliar se a evidência de auditoria suficiente e apropriada foi obtida e formular conclusões pertinentes.
Relatando	Os auditores devem preparar um relatório baseado nos princípios de completude, objetividade, tempestividade e contraditório.
Monitorando	Os auditores devem preparar um relatório baseado nos princípios de completude, objetividade, tempestividade e contraditório.

Fonte: elaborado pela autora.

As descrições utilizadas na tabela apresentada foram extraídas do ISSAI 400 - Princípios Fundamentais de Auditoria de Conformidade. O objetivo de descrever e estudar a referida norma fundamenta-se na necessidade de compreender detalhadamente os aspectos práticos aplicados para contribuir na análise das auditorias de conformidade da LGPD, realizadas pelo TCU.

O processo de planejamento da auditoria inicia-se com a definição clara e objetiva do seu propósito central, que deve ser apresentado sob a forma de uma declaração, contendo um verbo de ação que reflita o resultado esperado. Essa delimitação é essencial para assegurar o alinhamento da equipe e orientar todas as etapas subsequentes. Em seguida, o objetivo é desdobrado em questões de auditoria, as quais devem abordar os diferentes aspectos do escopo, estabelecendo os limites, as dimensões e o foco da investigação. Essa etapa permite determinar os caminhos metodológicos a serem seguidos, garantindo que a execução do trabalho permaneça dentro do escopo previsto. Segundo o Tribunal de Contas da União (2024, p. 9), “assim, o enunciado da questão não deve extrapolar o objetivo definido, de forma a não ampliar o escopo previsto para a auditoria. Deve englobar, porém, todos os itens que se quer verificar.”

Nesse contexto, a análise da auditoria realizada sobre a LGPD, que será feita no próximo capítulo, deve verificar se o planejamento contemplou, de forma adequada, todos os itens que se pretendia avaliar com base no objeto previamente definido. Ou seja, é necessário examinar se houve coerência entre o objetivo traçado e as questões formuladas, assegurando que o escopo da auditoria foi suficientemente abrangente para cobrir todos os aspectos

relevantes relacionados à proteção de dados pessoais, sem lacunas ou desvios que comprometam a efetividade do trabalho.

2.2.2 Auditoria operacional

A auditoria operacional é o exame independente, objetivo e confiável que analisa se empreendimentos, sistemas, operações, programas, atividades ou organizações do governo estão funcionando de acordo com os princípios de economicidade, eficiência, eficácia e efetividade e se há espaço para aperfeiçoamento (ISSAI 3000/17).

Considerando esses princípios fundamentais da auditoria operacional, é possível estabelecer uma correlação entre cada um deles e as exigências da proteção de dados pessoais no setor público, especialmente no contexto da implementação e fiscalização da LGPD. A seguir, apresenta-se uma tabela que adapta os conceitos de economicidade, eficiência, eficácia, efetividade e equidade à realidade da proteção de dados, evidenciando como tais dimensões podem ser avaliadas no âmbito da administração pública.

Tabela 5 – Aplicação dos Princípios da Administração Pública na Implementação da LGPD

Princípio	Conceito Geral (Administração Pública / Auditoria)	Conceito Aplicado à LGPD	Exemplo Prático na Administração Pública
Economicidade	Minimização dos custos dos recursos utilizados na execução das atividades, sem comprometimento da qualidade.	Uso racional de recursos (financeiros, tecnológicos e humanos) na implementação das medidas de proteção de dados, assegurando segurança e conformidade sem desperdícios.	Adoção de soluções tecnológicas de proteção de dados com melhor custo-benefício, como softwares de código aberto ou contratação de serviços compartilhados entre órgãos públicos.
Eficiência	Relação entre os produtos gerados e os custos dos insumos utilizados, mantendo padrões de qualidade.	Capacidade de transformar recursos disponíveis (tempo, equipe, tecnologia) em ações concretas e rápidas para garantir a proteção de dados pessoais.	Realização de treinamentos em proteção de dados com otimização de tempo e pessoal, ou implantação de ferramentas de privacidade com o menor custo possível e dentro do prazo estabelecido.

Eficácia	Grau de alcance das metas programadas, independentemente dos custos envolvidos.	Cumprimento das metas previstas no plano de adequação à LGPD, como a implementação de políticas de privacidade, canais de atendimento ao titular, realização de Relatórios de Impacto, entre outros.	Conclusão do inventário de dados pessoais, elaboração do Relatório de Impacto ou implantação de canal de atendimento aos titulares no prazo estabelecido.
Efetividade	Alcance dos resultados pretendidos a médio e longo prazo, considerando os impactos sobre a população-alvo.	Verificação de que as ações de adequação à LGPD resultaram efetivamente em maior proteção aos dados dos cidadãos, com impactos positivos e sustentáveis.	Redução de incidentes de vazamento de dados, maior índice de respostas às solicitações dos titulares dentro do prazo legal, e aumento da confiança dos cidadãos na proteção de seus dados.
Equidade	Garantia de tratamento diferenciado quando necessário, com foco na promoção da justiça social e na ampliação do acesso aos direitos.	Adoção de medidas que assegurem que todos os cidadãos, incluindo os mais vulneráveis, possam exercer seus direitos previstos na LGPD de maneira acessível e justa.	Disponibilização de políticas de privacidade em linguagem simples, criação de canais acessíveis a pessoas com deficiência, e adoção de estratégias para atingir populações em situação de vulnerabilidade digital.

Fonte: elaborado pela autora, com base em BRASIL (2020).

A Tabela foi elaborada com o objetivo de adaptar os princípios tradicionalmente utilizados nas auditorias da administração pública (economicidade, eficiência, eficácia, efetividade e equidade) ao contexto específico da proteção de dados pessoais, considerando as exigências estabelecidas pela LGPD. Inicialmente, os conceitos gerais foram extraídos do *Manual de Auditoria Operacional* do Tribunal de Contas da União (BRASIL, 2020), que apresenta as definições oficiais desses princípios aplicados ao setor público.

Em seguida, foi realizada uma interpretação conceitual para transpor esses princípios ao campo da proteção de dados, buscando estabelecer uma correlação entre cada princípio e as exigências normativas, os desafios de implementação e os aspectos operacionais relacionados à LGPD no setor público. Por fim, foram adicionados exemplos práticos para ilustrar como cada princípio pode ser observado, avaliado ou aplicado pelas organizações públicas no processo de adequação à LGPD, com foco na melhoria da governança e na proteção efetiva dos direitos dos titulares de dados pessoais.

O Ciclo de Auditoria Operacional representa as principais fases metodológicas de uma auditoria voltada para a avaliação de desempenho de políticas públicas, programas ou

atividades governamentais. Segundo o Manual de Auditoria Operacional do Tribunal de Contas da União (2020), o ciclo é composto por oito etapas principais, organizadas de forma sequencial, mas que também podem apresentar retroalimentações a depender dos resultados obtidos, quais sejam, seleção de temas, planejamento, execução, relatório, comentário do gestor, apreciação, divulgação e monitoramento.

Um dos pilares centrais da auditoria operacional é a identificação de achados estruturados de forma lógica e sequencial. O processo parte da comparação entre um critério previamente definido e a situação encontrada no campo, seguido pela análise das causas que explicam o desvio e pela avaliação dos efeitos decorrentes dessa situação. Trata-se de uma construção analítica que permite ao auditor visualizar a cadeia lógica entre o esperado, o realizado, os motivos para o desvio e as suas consequências. Esse encadeamento é especialmente relevante quando o objetivo da auditoria é não apenas apontar problemas, mas orientar soluções.

Para facilitar a compreensão dos elementos que compõem um achado de auditoria, a Tabela 5 apresenta a estrutura tradicionalmente utilizada, com seus principais componentes e respectivas descrições:

Tabela 6 – Estrutura dos Achados de Auditoria Operacional

Elemento do Achado	Descrição
Critério	Padrão ou expectativa de desempenho, podendo ser uma norma, diretriz, meta ou parâmetro estabelecido.
Condição	Situação efetivamente observada durante o trabalho de campo, com base em evidências coletadas.
Causa	Fatores ou motivos que explicam o desvio entre a condição observada e o critério definido.
Efeito	Consequências, impactos ou riscos decorrentes da situação encontrada.

Fonte: Elaborada pela autora, adaptado de BRASIL (2020).

A diversidade de técnicas de coleta de dados utilizadas na auditoria operacional é outro aspecto que a diferencia de outras formas de fiscalização. Entre os métodos mais aplicados estão a revisão documental, entrevistas com atores-chave, aplicação de questionários, observação direta e grupos focais. Cada uma dessas técnicas é escolhida de

acordo com o escopo da auditoria, as questões de auditoria formuladas e a disponibilidade de dados. Por exemplo, a revisão documental permite analisar registros oficiais e relatórios anteriores, enquanto as entrevistas podem revelar percepções, dificuldades operacionais e pontos de vista dos gestores públicos.

No campo da análise de dados, a auditoria operacional recorre a um leque de ferramentas quantitativas e qualitativas. Técnicas como estatística descritiva e regressão são frequentemente empregadas para identificar padrões de desempenho ou correlações entre variáveis. Já métodos como análise de conteúdo e triangulação de fontes permitem ao auditor captar nuances qualitativas que não seriam perceptíveis apenas com números. A triangulação, por sua vez, é fundamental para fortalecer a consistência dos resultados, combinando diferentes métodos e perspectivas sobre a mesma questão auditada.

"O auditor, ao executar uma auditoria operacional, deverá emitir um relatório apresentando seus comentários sobre se a administração adquiriu seus insumos com qualidade e ao menor custo, se eles foram bem utilizados e no tempo certo, se os resultados propostos foram alcançados, assim como comentários sobre o impacto ocasionado pelo uso desses insumos" (ARAÚJO, 2008, p. 31).

Ou seja, o processo de análise na auditoria operacional não se limita à descrição dos fatos. Exige uma interpretação crítica dos dados coletados, visando estabelecer conexões causais, identificar padrões e, principalmente, formular recomendações que sejam viáveis e orientadas para a solução dos problemas identificados. Ao integrar diferentes métodos, organizar os achados de forma estruturada e embasar as conclusões em evidências robustas, a auditoria operacional contribui para a melhoria contínua da gestão.

Dessa forma, a análise de dados em auditoria operacional vai além da simples verificação de conformidade ou do relato descritivo das situações observadas. Trata-se de um processo dinâmico e analítico, que demanda do auditor não apenas domínio técnico das ferramentas quantitativas e qualitativas, mas também capacidade crítica para interpretar os resultados obtidos à luz dos objetivos de auditoria. O resultado esperado é a produção de recomendações que não apenas apontem as falhas, mas também ofereçam soluções factíveis, baseadas em evidências concretas, visando a melhoria da eficiência, eficácia e efetividade das ações públicas.

2.3 Lições extraídas

Para o adequado funcionamento do Estado de Direito, torna-se imprescindível a existência de mecanismos de controle externo capazes de garantir que a administração pública atue em conformidade com os limites legais e constitucionais. Sem esses instrumentos de fiscalização, o risco de desvios, ineficiências e afrontas aos direitos fundamentais dos cidadãos aumenta consideravelmente, comprometendo a efetividade das políticas públicas.

Nesse cenário, os princípios da legalidade, da economicidade e da legitimidade assumem papel central na orientação das ações tanto da administração pública quanto dos órgãos de controle. Esses fundamentos não apenas norteiam a gestão dos recursos públicos, mas também balizam a atuação do TCU ao exercer o controle externo, incluindo a análise de temas relacionados à proteção de dados pessoais.

Assim, sempre que o TCU realiza uma auditoria, independentemente de sua natureza ou escopo, a atuação deve observar tais princípios, de modo que a fiscalização da implementação da LGPD pelos órgãos públicos também ocorra sob essa perspectiva. O respeito a esses valores assegura que o controle seja efetivo, legítimo e contribua para a boa governança pública.

Durante o desenvolvimento deste capítulo, foram apresentadas as três principais modalidades de auditoria realizadas pelo TCU: auditoria de conformidade, auditoria financeira e auditoria operacional. Embora cada uma possua objetivos e metodologias distintas, observa-se que, no contexto da análise da implementação da LGPD no setor público, a auditoria operacional oferece um enfoque que possibilita uma avaliação mais detalhada. Isso ocorre porque seu foco está na eficiência, eficácia e efetividade de programas e políticas públicas, permitindo um exame mais aprofundado das ações concretas adotadas pelos órgãos públicos para garantir a proteção dos dados pessoais.

Por fim, um aspecto relevante identificado refere-se ao avanço da inteligência artificial nas atividades internas do TCU. Essa abordagem tecnológica é especialmente importante para que as auditorias contemplem a verificação de hipóteses que envolvam a proteção de dados pessoais no uso da IA, bem como a existência de capacitação específica nos órgãos públicos para lidar com esse tema sensível.

3. IMPLEMENTAÇÃO DA LGPD SEGUNDO O TRIBUNAL DE CONTAS DA UNIÃO - TCU

Conforme discutido anteriormente, ao abordar a sociedade informacional e os riscos decorrentes de vazamento de dados pessoais, bem como superar as temáticas introdutórias relacionadas à LGPD e o TCU, buscou-se fornecer uma base conceitual e normativa sólida para que fosse possível avançar com consistência para a análise da auditoria objeto deste estudo, a qual será detalhada no presente capítulo.

A referida auditoria tem origem na problemática central que motivou esta pesquisa. Sua análise aprofundada, portanto, se revela essencial para alcançar a resposta à pergunta da pesquisa formulada. Nesse contexto, o capítulo inicia-se com os aspectos iniciais do processo que culminou no Acórdão 1384/2022 – TCU/Plenário, apresentando um panorama geral sobre a trajetória procedimental e os principais elementos do conteúdo deliberado.

Na sequência, o estudo avança para o desenvolvimento de uma análise crítica da auditoria realizada, estruturada em três eixos principais: (i) avaliação crítica da metodologia empregada pela auditoria; (ii) análise do questionário aplicado às organizações públicas auditadas; e (iii) discussão sobre aspectos relevantes da proteção de dados pessoais que não foram contemplados pela auditoria, com o objetivo de evidenciar lacunas existentes e sugerir caminhos para o aprimoramento de futuras fiscalizações realizadas pelo Tribunal de Contas da União.

Ao final deste capítulo, espera-se oferecer uma análise crítica das contribuições e limitações da Auditoria nº 1384/2022 do TCU, à luz dos critérios adotados e dos resultados alcançados, no contexto da implementação da LGPD nos órgãos públicos federais. Considerando que a auditoria foi realizada em momento próximo à entrada em vigor da Lei, examinar-se-á se a metodologia utilizada foi adequada para captar os principais desafios da adaptação institucional à nova normativa. A partir dessa análise, busca-se compreender se o controle externo realizado pelo TCU contribuiu efetivamente para o fortalecimento da política pública de proteção de dados e para o aperfeiçoamento das estratégias de fiscalização adotadas no setor público.

3.1 Auditoria para avaliar o grau de cumprimento da Lei – Acórdão 1384/2022

O presente estudo tem como base a análise da primeira auditoria realizada pelo TCU em matéria de proteção de dados pessoais, cujo resultado culminou no Acórdão nº 1384/2022 – TCU – Plenário, sob relatoria do Ministro Augusto Nardes. A auditoria teve como objetivo avaliar as ações governamentais relacionadas à implementação da LGPD e os riscos associados à proteção dos dados pessoais. O processo foi registrado sob o número TC 039.606/2020-1 e conduzido pela Secretaria de Fiscalização de Tecnologia da Informação (Sefti), unidade técnica responsável pela análise.

A investigação envolveu 382 organizações, sendo que, nesta primeira auditoria, foram consideradas apenas entidades públicas federais. As instituições auditadas foram convidadas a responder a um questionário eletrônico, elaborado com o objetivo de captar respostas que refletissem, da forma mais precisa possível, a situação do órgão em relação à conformidade com a LGPD. O instrumento metodológico empregado foi a Autoavaliação de Controles (*Control Self-Assessment – CSA*), técnica que estimula a participação ativa dos gestores na identificação, análise e avaliação dos próprios controles internos e práticas de governança.

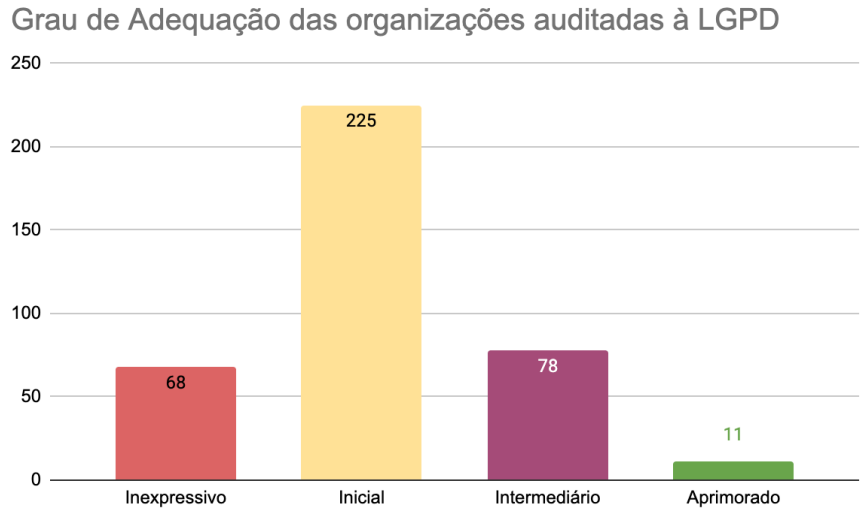
A estrutura da auditoria foi centralizada em três questões-chave: as duas primeiras tinham como objetivo identificar se as organizações implementaram medidas adequadas à LGPD e se os controles de proteção de dados pessoais estavam estruturados conforme a legislação. Essas questões foram desdobradas em perguntas específicas e encaminhadas às organizações públicas federais analisadas. Já a terceira questão buscava avaliar se a ANPD e o CNPD estavam estruturados conforme estabelecido na Lei, e gerou outro grupo de perguntas, que foram respondidas por meio de reuniões realizadas com membros da ANPD.

Contudo, para fins da presente pesquisa, o recorte metodológico adotado restringe-se à análise do primeiro grupo de questões, direcionadas às organizações públicas federais. Este foco se justifica pelo objetivo central deste trabalho, que é examinar a atuação da auditoria enquanto instrumento indutor da implementação da LGPD e do fortalecimento da segurança da informação no âmbito da administração pública. Assim, não serão abordadas neste estudo as análises relacionadas à estrutura da ANPD e do CNPD, concentrando-se exclusivamente nas práticas adotadas pelos jurisdicionados.

Os resultados da auditoria revelaram um cenário preocupante quanto ao grau de adequação das organizações públicas federais à proteção dos dados pessoais. Das 382

entidades avaliadas, apenas 11 (2,9%) demonstraram um nível aprimorado de conformidade, outras 78 organizações (20,4%) apresentaram estágio intermediário, indicando avanços pontuais, porém ainda com lacunas significativas. A maioria das entidades, contudo, situou-se nos níveis mais baixos de adequação: 225 (58,9%) no estágio inicial e 68 organizações (17,8%) sequer alcançaram esse nível, sendo classificadas como de conformidade inexpressiva, o que revela um total desconhecimento ou ausência de iniciativas relacionadas à LGPD, vejamos o gráfico a seguir:

Gráfico 1 - Grau de adequação das organizações auditadas à LGPD



Fonte: TCU (2022)

As lições extraídas no primeiro capítulo desta pesquisa permitem compreender que os dados pessoais, especialmente os dados sensíveis, transcendem sua função instrumental de servir exclusivamente à finalidade para a qual foram originalmente coletados. Na sociedade informacional, esses dados passaram a representar um ativo valioso, utilizado não apenas por entes públicos e privados em processos legítimos de gestão, mas também, de maneira indevida, em contextos de perseguição, discriminação e manipulação.

O cenário se agrava diante do aumento de ataques cibernéticos e vazamentos de dados, que evidenciam o despreparo dos sistemas públicos e privados para enfrentar os desafios atuais. Nesse contexto, os resultados apresentados pela auditoria revelam um grau preocupante de vulnerabilidade institucional por parte de diversas organizações da administração pública federal. Conclui-se, portanto, que se o nível federal que dispõe de

maior estrutura técnica, orçamentária e organizacional, já enfrenta tantas dificuldades, o panorama nos entes subnacionais é ainda mais delicado.

A realidade dos municípios de pequeno porte impõe uma camada adicional de preocupação. Essas localidades frequentemente operam com orçamento restrito, carência de pessoal qualificado e defasagem tecnológica, fatores que, juntos, tornam a implementação efetiva da LGPD um desafio quase intransponível. A sobrecarga de servidores, a ausência de capacitação continuada e a inexistência de estruturas mínimas de governança de dados apenas reforçam o abismo entre o que exige a legislação e o que é possível realizar na prática.

O voto do Ministro Aroldo Cedraz abordou algumas das complexidades da aplicação da LGPD no setor público, com ênfase especial nas dificuldades relacionadas à interoperabilidade de sistemas. Cedraz destacou sua experiência anterior na defesa da integração de bases de dados como instrumento para o aperfeiçoamento da prestação de serviços públicos e para o fortalecimento de políticas públicas. No entanto, ao acompanhar o voto do relator, reconheceu a necessidade de reforçar as salvaguardas previstas na LGPD no que se refere ao tratamento de dados pessoais e ao compartilhamento com entidades externas. Segundo ele, a ausência de medidas adequadas de proteção poderia ter como efeito colateral indesejado o retrocesso nas iniciativas de integração tecnológica entre órgãos públicos.

Diante disso, o Ministro sugeriu que fosse considerada a possibilidade de dispensar exigências mais rigorosas quando o compartilhamento de dados ocorrer entre órgãos e entidades que integrem a administração direta federal, entendidos como partes de um mesmo corpo institucional. A proposta buscava equilibrar o imperativo da proteção de dados pessoais com a manutenção das melhorias já alcançadas por meio da interoperabilidade de sistemas públicos.

A manifestação do Ministro Aroldo Cedraz revela um dilema clássico na implementação da LGPD no setor público: o equilíbrio entre a proteção de dados pessoais e o interesse público, nesse caso concreto a continuidade de políticas públicas de integração tecnológica entre os órgãos. De um lado, há a necessária observância aos direitos fundamentais dos titulares de dados e, de outro, o interesse público na eficiência administrativa.

A proteção de dados pessoais não deve ser interpretada como um obstáculo à eficiência administrativa. Para tanto, é necessário que os entes públicos adotem medidas que assegurem o tratamento adequado dos dados, sem comprometer a integridade, a segurança e a

finalidade legítima dessas informações, evitando, assim, qualquer forma de vulnerabilidade que resulte em incidentes de segurança.

O Ministro reconheceu que o TCU enfrenta determinadas limitações quanto à sua atuação no tema, especialmente diante da disposição legal que atribui à ANPD a competência para o estabelecimento de normas complementares. Contudo, destacou que essa circunstância não poderia justificar a omissão do TCU diante da relevância da matéria, manifestando-se da seguinte forma:

> Por outro lado, ressalto igualmente que não pode o Tribunal de Contas da União se omitir diante de assunto de tamanha relevância, diante dos prejuízos causados à eficiência da Administração Pública pela falta de compartilhamento e integração de dados entre órgãos e entidades do Estado, conforme sobejamento demonstrado em múltiplos Acórdãos desta Corte. (BRASIL, 2022, p. 7)

Essa manifestação reforça diretamente o que se apresentou no Capítulo 1, ao tratar da teoria da dimensão objetiva dos direitos fundamentais. Conforme exposto, essa teoria impõe ao Estado não apenas o dever de abster-se de violar direitos fundamentais, mas, sobretudo, o dever de promovê-los ativamente por meio de políticas públicas e decisões administrativas que concretizem sua efetividade.

Nessa perspectiva, a aplicação da teoria da dimensão objetiva dos direitos fundamentais oferece o alicerce normativo necessário para afirmar que o Poder Público, em todas as suas esferas e instituições, encontra-se vinculado à promoção efetiva dos direitos fundamentais, isso significa que o TCU dotado de instrumentos institucionais adequados, deve exercer sua função não apenas como uma prerrogativa, mas também como uma responsabilidade constitucional.

O voto do relator Ministro João Augusto Ribeiro Nardes, buscou contextualizar a aplicação da LGPD, relacionando-a à atuação dos órgãos jurisdicionados, bem como apresentou os resultados da auditoria de maneira global, por percentual de conformidade, e de forma temática, permitindo aferir o grau de maturidade das organizações auditadas em relação à proteção de dados pessoais. Essa abordagem tem o mérito de oferecer uma visão geral do cenário institucional, mas apresenta limitações importantes.

Ocorre que ao agrupar todos os órgãos públicos em um único conjunto, desconsideram-se as particularidades de cada instituição, especialmente aquelas que tratam dados pessoais sensíveis e, portanto, exigem maior atenção. Assim, corre-se o risco de que

entidades mais expostas a riscos estejam entre aquelas classificadas com grau de adequação "inexpressivo", sem que isso seja devidamente evidenciado.

Com o objetivo de facilitar a compreensão acerca da diversidade de instituições públicas e dos diferentes tipos de dados pessoais tratados, elaborou-se a tabela 1, apresentada ainda na introdução deste trabalho, que classifica os órgãos públicos federais segundo critérios como o âmbito de atuação, o tipo de administração, o poder ao qual pertencem, além de exemplos concretos de instituições e os tipos de dados pessoais por elas tratados.

O voto apresentou também a estrutura organizacional da ANPD, discutindo os desafios enfrentados pelo órgão e as consequências decorrentes de sua limitação institucional, técnica e orçamentária. O ministro relator também acolheu recomendações formuladas por outros membros do Tribunal, entre eles o Ministro Aroldo Cedraz , voltadas ao fortalecimento da governança de dados pessoais na administração pública. Ao final, concluiu pela continuidade dos trabalhos de auditoria, reforçando o papel do TCU.

Esse indicativo de que os trabalhos terão prosseguimento, somado à manifestação do Ministro Aroldo Cedraz de que o Tribunal não pode permanecer inerte, reforça a compreensão da proteção de dados pessoais como expressão da dimensão objetiva dos direitos fundamentais.

Por fim, as propostas de encaminhamento resultantes da auditoria tiveram como base a recomendação aos órgãos para que editem normas, guias e orientações voltadas ao aprimoramento da proteção de dados pessoais. Essas recomendações consideraram o papel de controle exercido pelos órgãos de fiscalização sobre a atuação administrativa das organizações sob sua jurisdição, com o objetivo de orientar e uniformizar práticas que garantam maior conformidade à LGPD no âmbito da Administração Pública.

3.1.1 Avaliação crítica da metodologia empregada pela auditoria

No capítulo 2, foram abordadas as atribuições do TCU, com destaque para os diferentes tipos de auditoria por ele realizados: auditoria operacional, financeira e de conformidade. Nesse contexto, identificou-se que a metodologia adotada para aferir o grau de aderência à LGPD foi a auditoria de conformidade. O objetivo principal da auditoria, portanto, foi avaliar as ações governamentais relacionadas à proteção de dados pessoais, bem como os riscos a que esses dados estão expostos no âmbito da administração pública federal.

O principal ponto de crítica à metodologia utilizada reside no fato de que a autoavaliação depende da percepção e do grau de maturidade dos próprios avaliados, o que pode gerar vieses de confirmação ou até omissões involuntárias. Além disso, o simples cumprimento de determinado requisito não garante que o órgão esteja, de fato, devidamente adequado, uma vez que esse método não permite medir a eficácia da implementação. Essa situação pode resultar em relatórios que mascaram fragilidades que permaneceriam ocultos até a ocorrência de um incidente ou de uma fiscalização mais rigorosa.

Ou seja, a auditoria baseou-se apenas em respostas fornecidas pelos próprios órgãos auditados, sem o cruzamento dessas informações com outras fontes objetivas, como: análise documental, entrevistas com os responsáveis pelo tratamento de dados, entre outros elementos. Tal abordagem fragiliza a robustez dos achados, desde que partindo da premissa de que o objetivo de uma auditoria em LGPD deve ser a minimização da vulnerabilidade no tratamento dos dados pessoais.

A crítica à metodologia adotada pelo TCU na Auditoria nº 1384/2022, especialmente no que diz respeito à confiabilidade das respostas autorreferidas, é reforçada pelo estudo **"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"**. O artigo identificou incongruências nas informações prestadas pela entidade auditada, como o fato de haver um encarregado de proteção de dados nomeado, mas que não constava no site institucional, contrariando a exigência de publicidade prevista na LGPD.

Além disso, a FUNAI respondeu positivamente sobre a existência de uma Política de Segurança da Informação, embora não houvesse normativas complementares para assegurar a efetiva proteção dos dados. Em outros pontos, como a revisão de contratos com operadores e a existência de controladores conjuntos, as respostas indicaram "não se aplica", o que levanta dúvidas sobre o grau de compreensão da norma por parte dos respondentes. Segundo o autor, esses achados sugerem que, em alguns casos, as respostas podem refletir mais o nível de conhecimento ou maturidade institucional do que a realidade prática da implementação. Assim, o estudo corrobora a crítica de que uma metodologia baseada exclusivamente na autoavaliação pode não captar com precisão o estágio real de conformidade dos órgãos públicos com a LGPD, especialmente em contextos de baixa capacitação técnica.

Por outro lado, é imprescindível reconhecer que toda análise de eficácia pressupõe a existência de práticas implementadas, ainda que de forma inicial ou incipiente. Nesse sentido,

a utilização da Autoavaliação de Controles como instrumento metodológico revela-se adequada para aferir o grau de conformidade formal e estrutural dos órgãos auditados, estabelecendo um ponto de partida necessário para avaliações futuras mais robustas.

No entanto, após o estudo realizado sobre os tipos de auditoria e considerando que a proteção efetiva dos dados pessoais envolve não apenas a conformidade formal, mas também a eficácia das medidas implementadas, parece razoável refletir sobre a possibilidade de que a auditoria operacional pudesse contribuir com uma análise mais aprofundada dos resultados obtidos pelos órgãos públicos. Essa abordagem, voltada para os efeitos e impactos das ações adotadas, talvez oferecesse subsídios adicionais à compreensão do estágio de maturidade na implementação da LGPD.

Não obstante, surge uma preocupação relevante quanto ao perfil dos órgãos auditados, uma vez que a amostra inicial contemplou entidades da administração pública federal, cujas estruturas técnicas, em tese, seriam mais preparadas para o enfrentamento dos desafios impostos pela LGPD. Apesar disso, os resultados da primeira rodada evidenciaram um quadro preocupante: identificou-se um número expressivo de órgãos com grau de maturidade inexpressivo, o que expõe não apenas o risco associado à proteção de dados pessoais no âmbito federal, mas também a dificuldade concreta de implementação efetiva, mesmo em ambientes institucionalmente estruturados.

Atualmente, encontra-se em andamento uma nova auditoria, que, além dos órgãos federais, passou a englobar também entes estaduais e municipais. Importante destacar que diversos Tribunais de Contas estaduais aderiram à iniciativa, ampliando o alcance e a representatividade da avaliação. Com isso, será possível verificar se a realização periódica dessas auditorias contribui, de fato, para o aprimoramento da conformidade e, ainda, se existem diferenças relevantes nas dificuldades de implementação da LGPD em função do nível federativo.

Diante do baixo grau de maturidade identificado, o que pode refletir uma limitação no domínio técnico sobre o tema por parte dos respondentes, cabe refletir se o questionário aplicado está, de fato, estruturado de forma a contribuir para a construção de um caminho viável de implementação. Ou, ao contrário, se sua formulação acaba dificultando a definição de uma metodologia clara e aplicável.

O questionário foi elaborado não apenas com o intuito de mensurar o grau de conformidade das organizações públicas, mas também de auxiliar na própria implementação

da LGPD. Isso porque todas as perguntas vieram acompanhadas de referências normativas detalhadas, indicando os artigos pertinentes da LGPD, da LAI, do Código de Defesa do Consumidor - CDC... Além de normas técnicas como a ABNT NBR ISO/IEC, com remissão aos itens específicos de cada norma, o que contribui significativamente para orientar os responsáveis pela implementação e facilita a compreensão dos requisitos exigidos.

Apesar de o questionário aplicado contar com 60 perguntas e cobrir diversos aspectos relevantes da LGPD, é possível que alguns controles adicionais importantes para a completa conformidade à norma não tenham sido plenamente explorados. Essa característica pode influenciar o nível de abrangência do diagnóstico gerado e, eventualmente, sinalizar oportunidades de aprimoramento no instrumento utilizado, com vistas a apoiar de forma ainda mais eficaz as ações de implementação da legislação.

Uma reflexão que pode ser considerada diz respeito aos critérios adotados para a elaboração das perguntas do questionário: será que todas contribuem de forma efetiva para os objetivos pretendidos? E, ainda, será que alguns pontos relevantes para uma avaliação mais completa da conformidade à LGPD não poderiam ter sido incluídos? A depender da abordagem adotada, existe a possibilidade de que o instrumento deixe de captar certos aspectos importantes, o que pode reduzir seu potencial de fornecer um diagnóstico mais amplo e útil à gestão. Essa limitação, ainda que sutil, pode influenciar os resultados da auditoria e, em alguma medida, a identificação de melhorias necessárias à segurança da organização.

Ainda que se reconheça o esforço em padronizar o questionário como ferramenta inicial de diagnóstico, é necessário ponderar se a estrutura atual é suficiente para captar com precisão a realidade de todos os órgãos auditados. Considerando que há instituições com temáticas diversas e em diferentes estágios de maturidade em relação à implementação da LGPD, uma abordagem única pode gerar diagnósticos imprecisos e comprometer a utilidade prática da auditoria.

Nesse cenário, uma proposta mais eficaz seria a segmentação dos órgãos públicos em grupos distintos, considerando tanto o grau de adequação à LGPD quanto a natureza das atividades institucionais. Por exemplo, poderia-se estruturar a análise a partir de três grandes blocos: grupo com grau de inexpressividade, grupo intermediário e grupo avançado. Essa divisão permitiria que as recomendações fossem calibradas de forma mais realista e efetiva, adaptadas ao estágio atual de maturidade de cada instituição.

3.1.2 Análise do questionário aplicado às organizações auditadas

Encerrada a análise do método, passa-se agora ao exame do questionário aplicado, com atenção especial às temáticas nele abordadas. Desde já, importa esclarecer que não se pretende aqui reproduzir ou comentar de forma exaustiva todas as questões formuladas na auditoria. O foco recai sobre alguns pontos que, à luz de uma leitura crítica, podem indicar oportunidades de aperfeiçoamento, seja por eventuais lacunas ou abordagens que poderiam ser desenvolvidas de forma mais ampla. Além disso, serão mencionados aspectos que, embora já contemplados, poderiam se beneficiar de um maior aprofundamento ou de questões complementares, com vistas a uma avaliação mais precisa e abrangente.

O questionário elaborado pelo TCU foi estruturado em nove dimensões, com a seguinte distribuição: Preparação (3 questões), Contexto organizacional (11 questões), Liderança (13 questões), Capacitação (4 questões), Conformidade do tratamento (8 questões), Direitos do titular (5 questões), Compartilhamento de dados pessoais (5 questões), Violação de dados pessoais (6 questões) e Medidas de proteção (5 questões), totalizando 60 questões.

Uma primeira observação crítica recai sobre o foco na escolha dos critérios de distribuição temática do questionário. Embora não se exija que todas as dimensões recebam o mesmo número de perguntas, seria esperado que a quantidade de itens atribuída a cada tema refletisse a relevância de cada um no contexto da LGPD.

Observa-se uma priorização de aspectos de governança, liderança e contexto organizacional, em detrimento de áreas que guardam relação direta com a proteção efetiva dos dados pessoais, como por exemplo medidas de segurança da informação.

A metodologia adotada para a análise crítica do questionário de auditoria seguiu um processo estruturado e alinhado aos objetivos desta pesquisa. Inicialmente, procedeu-se à identificação e estudo dos critérios utilizados para a elaboração da auditoria, conforme consta nos documentos oficiais do TCU, as perguntas tiveram como referência a LGPD e as normas técnicas ABNT NBR ISO/IEC 27701/2019, entre outras referências citadas nos documentos.

Neste subcapítulo, a proposta é analisar exclusivamente os aspectos contemplados no questionário, aprofundando o exame das questões abordadas e sugerindo aprimoramentos pontuais a partir do conteúdo já existente. A análise busca contribuir com o aperfeiçoamento do instrumento, oferecendo sugestões que possam torná-lo mais aderente às necessidades de

avaliação. As eventuais lacunas identificadas, isto é, elementos previstos na normativa que não foram abordados no questionário, serão apresentadas de forma sistematizada no subcapítulo seguinte.

A fase de preparação na adequação à LGPD desempenha um papel importante na definição das bases que orientarão as ações futuras de conformidade. No entanto, ao contar com apenas duas perguntas para avaliar esse estágio inicial, o questionário pode não captar toda a complexidade envolvida e acaba por deixar de fora aspectos relevantes para assegurar que a organização esteja devidamente preparada para iniciar a implementação. Mais do que elaborar um plano de ação, essa etapa envolve a criação de um ambiente institucional que reconheça a importância da proteção de dados e esteja disposto a promover uma mudança cultural interna.

A primeira questão relevante é a necessidade de conscientização e capacitação mínima dos colaboradores. Antes de iniciar qualquer processo de adequação, a organização precisa garantir que todos os envolvidos, desde a alta gestão até os colaboradores operacionais, compreendam as exigências da LGPD e sua importância para o funcionamento da instituição. A falta de treinamento e conscientização pode resultar em falhas graves na implementação da lei. Como formar um comitê de proteção de dados, por exemplo, se os membros do comitê não compreendem claramente os aspectos legais, técnicos e estratégicos envolvidos? O comitê precisa ser composto por pessoas que, além de ter suas funções bem definidas, também devem entender como suas decisões impactam a proteção de dados e a conformidade com a lei.

No relatório, foram apresentados os dados globais sobre as respostas a cada pergunta. Quando o ponto analisado é a capacitação, os dados revelam fragilidades significativas no processo de implementação da LGPD nas organizações públicas auditadas. A baixa porcentagem, cerca de 10%, de instituições que treinaram todos os colaboradores envolvidos com o tratamento de dados evidencia um descuido generalizado com a capacitação, que é um dos pilares essenciais para a efetividade da proteção de dados pessoais.

Esse cenário aponta para uma limitação estrutural que pode influenciar a qualidade das respostas fornecidas durante o processo de autoavaliação. A identificação desse nível reduzido de preparo reforça a necessidade de se considerar com cautela a metodologia utilizada, uma vez que eventuais lacunas no conhecimento técnico podem levar a respostas menos precisas ou superficiais, afetando a consistência dos resultados obtidos.

Além disso, o fato de apenas 29% possuírem um plano de capacitação estruturado voltado à proteção de dados pessoais indica que, na maioria das organizações, a capacitação ainda é tratada de forma pontual ou improvisada, sem um planejamento contínuo e alinhado à estratégia institucional de governança de dados. Soma-se a isso o dado de que 46% sequer consideraram a necessidade de realizar treinamentos diferenciados de acordo com as funções exercidas, o que demonstra um desconhecimento sobre a complexidade e especificidade dos papéis dentro do ciclo de tratamento de dados.

A legislação é complexa e exige um grau de conhecimento interdisciplinar, especialmente no âmbito da administração pública, onde é comum a necessidade de ponderação de direitos e a invocação de outras normas para sua correta interpretação e aplicação. Nesse sentido, a ausência de capacitação adequada acarreta o risco de tratamento equivocado dos dados, em razão de interpretações incorretas, falhas na implementação das medidas de segurança e, principalmente, a exposição indevida de informações sensíveis.

Nesse sentido, como forma de contribuir com possíveis melhorias na abordagem sobre capacitação, a auditoria poderia ter questionado, por exemplo, se foram realizados testes pós-treinamento para avaliar a efetividade do aprendizado, se houve a elaboração de um plano de capacitação após a etapa de conscientização e plano de ação onde seria possível a identificação estruturada das necessidades de capacitação e, especialmente, se esse plano é periodicamente revisto à luz das novas demandas que surgem ao longo da implementação, conforme o ciclo de melhoria contínua PDCA (Planejar, Fazer, Verificar e Agir).

Na auditoria realizada, o tema da capacitação foi tratado dentro da quinta dimensão, o que pode ser repensado. Dada sua relevância estratégica, seria mais adequado posicionar esse aspecto como um dos pilares da fase de preparação, já que a capacitação é o alicerce para todas as demais etapas de conformidade. Uma reorganização das dimensões nesse sentido contribuiria para reforçar a compreensão de que, sem servidores minimamente preparados, as demais ações institucionais previstas na LGPD tendem a ser implementadas de forma falha ou meramente formal.

Ainda no contexto da capacitação, e considerando que estamos tratando da primeira dimensão, correspondente à fase de preparação, observa-se que a constituição do Comitê de Proteção de Dados, é composta por profissionais de áreas distintas dentro da organização, o que permite uma abordagem multidisciplinar e complementar sobre o tratamento de dados pessoais. Cada integrante contribui com sua perspectiva específica: jurídica, tecnológica,

administrativa, recursos humanos, entre outras, favorecendo uma análise mais completa dos fluxos de dados e dos riscos envolvidos. Nesse sentido, também merece atenção mais robusta e criteriosa.

A formação desse comitê não pode ser tratada como uma formalidade apressada, tampouco limitada à nomeação genérica de membros. Pelo contrário, deve ser resultado de uma escolha criteriosa, baseada nas competências técnicas, estratégicas e operacionais dos participantes, bem como nas necessidades específicas da organização frente aos riscos e à maturidade institucional em proteção de dados.

Dessa forma, seria importante que a auditoria incluísse perguntas como: A organização identificou e nomeou formalmente os membros do Comitê de Proteção de Dados? Houve capacitação específica dos membros do comitê sobre a LGPD, segurança da informação e governança de dados? O comitê possui ato normativo, plano de atuação e cronograma de reuniões regulares?

Na fase de levantamento do contexto organizacional, correspondente à segunda dimensão da auditoria, foram aplicados 11 questionários, os temas abordados incluíram: normativos internos relacionados ao tratamento de dados pessoais, identificação das categorias de titulares cujos dados são tratados, operadores e controladores conjuntos envolvidos, processos institucionais que realizam tratamento de dados pessoais, tipos de dados tratados, e os riscos associados a esses processos.

A identificação, por parte da organização, das categorias de titulares de dados e dos operadores envolvidos no tratamento é fundamental para a conformidade com a LGPD, pois permite à organização mapear com precisão quem são os indivíduos impactados e quais terceiros tratam dados em seu nome. Essa etapa viabiliza a adoção de medidas proporcionais aos riscos envolvidos, garante maior transparência, facilita o atendimento aos direitos dos titulares, além de assegurar o devido controle sobre os operadores.

Quanto ao operador, 51% das organizações públicas auditadas não realizaram a identificação formal desses agentes. Esse dado revela que mais da metade das instituições estão incorrendo em uma falha grave no processo de adequação à LGPD, considerando que o operador exerce papel essencial no ciclo de tratamento de dados, sendo o responsável por executar atividades sob as ordens do controlador, nos termos do art. 5º, inciso VII, da Lei nº 13.709/2018.

A omissão na identificação dos operadores compromete diretamente a governança de dados e representa um risco relevante à proteção das informações pessoais. Sem esse mapeamento, torna-se inviável formalizar contratos com cláusulas específicas de segurança, responsabilidade, dentre outros. Isso expõe as organizações públicas a fragilidades jurídicas e operacionais, incluindo dificuldades para atribuição de responsabilidades em casos de incidentes de segurança, como vazamentos ou uso indevido de dados.

O fato é que no próprio acórdão ficou relatado da seguinte forma: *O cenário é preocupante, pois a identificação dos operadores é um ponto chave para efetividade da proteção de dados pessoais, uma vez que realizam tratamento de dados em nome de organizações. Além disso, cumpre frisar que o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir obrigações da legislação ou quando não seguirem instruções licitas do controlador. (LGPD, art. 42, 1, inciso I).*

Quanto aos dois pontos em questão, identificação de categoria e operadores, a abordagem adotada poderia ir além da simples verificação da existência dessa identificação, buscando compreender também a metodologia utilizada no processo. Isso porque o fato de a organização afirmar que realizou o levantamento não garante, por si só, que ele tenha sido conduzido de maneira completa ou adequada.

A profundidade e o rigor aplicados nessa etapa são importantes para o desenvolvimento da política de proteção de dados. A partir da identificação clara dos titulares e operadores, torna-se possível categorizar os dados pessoais corretamente e adotar medidas proporcionais aos riscos envolvidos, conforme destacado no acórdão analisado.

Dessa forma, para que o processo de adequação vá além de uma simples formalidade, seria interessante que a auditoria ou diagnóstico inicial buscasse elementos que indiquem como a identificação foi conduzida, quais critérios foram adotados e se houve a participação dos setores estratégicos da organização. Isso pode contribuir para uma avaliação mais equilibrada sobre a adequação da estrutura estabelecida para a proteção dos dados e sua adequação às demandas do órgão.

Caso a instituição tivesse informado que procedeu com a avaliação de todos os operadores, era exibida uma subquestão destinada a verificar se os contratos firmados com esses operadores foram adequadamente ajustados, com a devida delimitação de responsabilidades e papéis no que se refere à proteção de dados pessoais.

No tocante aos contratos públicos, observa-se, na prática, o uso recorrente de modelos padronizados de editais e minutas contratuais, o que, por um lado, confere celeridade aos processos licitatórios. Por outro lado, no que diz respeito à delimitação de responsabilidades em proteção de dados, essa padronização pode apresentar algumas limitações.

A definição clara dos papéis, obrigações e limites do controlador e do operador é importante para garantir que o tratamento de dados seja feito conforme a lei e respeitando os princípios de segurança, prevenção e responsabilidade. Muitas vezes, quando os contratos não trazem cláusulas específicas ou usam termos mais gerais, isso acontece não por má-fé, mas por falta de conhecimento adequado. Sem uma fiscalização cuidadosa, esses contratos podem acabar cumprindo apenas uma formalidade, sem realmente trazer os resultados esperados.

As respostas indicam que cerca de 15% das organizações realizaram a adequação completa dos contratos firmados. Nesse contexto, é importante que os órgãos de controle adotem uma postura mais cuidadosa e técnica, especialmente no acompanhamento da inclusão e aplicação dessas cláusulas, assim como na verificação do seu cumprimento ao longo da execução dos contratos. A proteção de dados pessoais, especialmente nas contratações públicas, deve ser considerada não apenas como uma exigência burocrática, mas como um aspecto relevante da gestão de riscos e da responsabilidade em relação aos direitos fundamentais.

Na auditoria analisada neste estudo, percebe-se que as perguntas se concentram apenas nos contratos já firmados, sem uma avaliação dos processos licitatórios em andamento ou futuros, principalmente no que se refere à inserção de cláusulas relacionadas à conformidade com a Lei. Essa abordagem merece atenção, especialmente considerando que decisões recentes de Tribunais de Contas têm tratado especificamente desse tema.

A ausência de dispositivos sobre a LGPD nos editais de licitação tem se revelado uma considerável brecha jurídica. Em um ambiente competitivo, é comum que empresas se valham dessa lacuna para apresentar impugnações e denúncias, muitas vezes com o objetivo de tumultuar o processo licitatório e retardar a contratação pública.

Em um dos casos analisados pelo TCE-MG, Acórdão nº 1149236, tratou de uma denúncia alegando que o edital não trazia expressamente a obrigação de aplicação da LGPD. O relator entendeu ser desnecessária tal previsão, diante do caráter cogente da norma (TRIBUNAL DE CONTAS DO ESTADO DE MINAS GERAIS, 2024). No entanto, se há a obrigação de adequar os contratos administrativos à LGPD, por que não assegurar que essa

adequação já conste desde a origem, no próprio edital, em alinhamento com o princípio do *privacy by design*?

No âmbito federal, a prática tem caminhado em sentido diverso: alguns ministérios solicitaram manifestação da Câmara Nacional de Convênios e Instrumentos Congêneres (CNCIC) quanto à aplicabilidade da LGPD e requisitaram modelos padronizados com cláusulas específicas de proteção de dados para convênios e instrumentos congêneres. Em resposta, a CNCIC concluiu pela necessidade de referência expressa ao tratamento de dados pessoais nesses instrumentos, conforme disposto no *Parecer n. 00001/2024/CNCIC/CGU/AGU* (BRASIL, 2024).

A reflexão se amplia: além de prever cláusulas contratuais sobre a LGPD, as contratações públicas têm exigido comprovações práticas? Ou seja, as empresas contratadas estão, de fato, adequadas à legislação? Há exigência de documentos que atestem a implementação de medidas técnicas, administrativas e de segurança da informação?

Nesse ponto, não se verifica questionamento, na auditoria, sobre a conformidade das empresas contratadas quanto à proteção de dados pessoais. De que adianta o órgão público adequar seus procedimentos e contratos à LGPD, se os seus parceiros na execução contratual não estiverem igualmente em conformidade?

A terceira dimensão abordada no questionário refere-se à liderança, composta por 13 questões que destacam temas como a nomeação do Encarregado pelo Tratamento de Dados Pessoais (DPO) e a existência de políticas, tais como: política de segurança da informação, política de classificação da informação e política de proteção de dados pessoais.

A política de segurança de uma empresa é um conjunto de regras, normas e procedimentos que determina qual deve ser o comportamento das pessoas que se relacionam com a organização no que se refere ao tratamento da informação. Não é um documento independente com regras de conduta desconectadas, mas um documento em continuidade de regras, normas e leis já existentes (NEVES et al., 2021, p. 194).

Os dados da auditoria revelam que 24% das organizações públicas federais analisadas não possuem política de segurança da informação, o que representa um risco significativo para a proteção de dados pessoais. A ausência dessa política compromete a padronização de condutas e a clareza sobre responsabilidades, deixando os colaboradores sem diretrizes claras sobre como agir em situações que envolvem a segurança da informação.

A relevância do tema ganha ainda mais proporção quando se observa que esse foi o único quesito da auditoria em que o TCU propôs dar ciência às organizações que não possuíam a política de segurança da informação, reconhecendo que a ausência do referido documento afronta diretamente o disposto nas normativas de referência.

Seria interessante que o questionário da auditoria abordasse com um pouco mais de profundidade o conteúdo mínimo das políticas de segurança da informação adotadas pelas organizações públicas, indo além da simples existência do documento. Um aspecto importante seria verificar se essas políticas incluem requisitos básicos, como segurança das pessoas, dos sistemas, da web e do suporte técnico.

Além disso, a metodologia utilizada não contempla uma análise mais detalhada sobre a implementação prática dessas políticas no dia a dia dos órgãos auditados. Essa lacuna pode resultar em um diagnóstico que não reflita completamente a realidade, criando uma percepção de conformidade que pode não corresponder ao efetivo cumprimento previsto no art. 50, § 2º, II da LGPD.

No entanto, ao analisar o portal do TCU, verifica-se que existe uma auditoria operacional específica voltada à segurança da informação, o que demonstra que o Tribunal mantém uma atuação constante e atenta ao tema. Diante disso, compreende-se que a auditoria sobre a LGPD tenha tratado a Política de Segurança da Informação de forma mais superficial.

A inclusão das políticas de segurança da informação, classificação da informação e proteção de dados pessoais, sob o eixo temático da liderança suscita outra reflexão: não seria mais adequado abordar essas políticas na fase de documentação, quando se trata da formalização das bases legais e dos instrumentos de controle e governança? Dessa forma, haveria maior coerência na distribuição temática e cronológica das etapas de implementação, evitando-se sobreposição de tópicos e reforçando a lógica evolutiva do processo.

Portanto, reorganizar a disposição dessas questões de acordo com o fluxo real de um projeto de adequação, desde a preparação até a consolidação dos documentos, não apenas tornaria a avaliação mais clara, como contribuiria para a efetividade do diagnóstico e da auditoria, e consequentemente em uma implementação em um órgão.

É oportuno retomar brevemente a figura do Encarregado pelo Tratamento de Dados Pessoais, embora já tenha sido abordado com detalhes no Capítulo 1.2. Trata-se da pessoa responsável por orientar e supervisionar a aplicação da LGPD na instituição, atuando como elo de comunicação entre o órgão, os titulares dos dados e a ANPD.

A auditoria apontou que 69% das organizações públicas federais nomearam um DPO. No entanto, apenas 75% dessas instituições providenciaram a devida publicação dessa informação. Isso significa que, na prática, menos da metade das entidades analisadas tornaram pública a identidade e os canais de contato com o encarregado, o que representa uma grave falha de transparência e de cumprimento das legislações.

A ausência do encarregado ou a falta de publicidade sobre sua identidade e formas de contato compromete a efetividade da proteção de dados, uma vez que prejudica o canal direto de comunicação com os titulares, impede a atuação eficaz da ANPD, debilita a governança institucional de privacidade e proteção de dados e configura descumprimento de dever legal.

O voto propôs recomendar à ANPD que oriente as organizações quanto às responsabilidades atribuídas ao Encarregado pelo Tratamento de Dados Pessoais, bem como sobre o perfil e os requisitos profissionais desejáveis para o exercício da função, além de indicar locais apropriados para sua vinculação institucional. No entanto, é importante destacar que tais diretrizes já haviam sido objeto da Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020, que estabelece orientações para a atuação do Encarregado no âmbito da administração pública federal.

Um ponto relevante de reflexão diz respeito à complexidade das diretrizes sobre o perfil e as atribuições do DPO, os documentos orientadores, traçam um perfil técnico, ético e institucional robusto para esse profissional, exigindo conhecimentos multidisciplinares e autonomia. Diante disso, surge o questionamento: será que tais exigências são plenamente aplicáveis a todos os níveis da administração pública, especialmente nos municípios de pequeno porte ou em autarquias com estrutura reduzida?

Além disso, ao observar a sequência proposta para a implementação da LGPD, percebe-se uma certa inconsistência na forma como esse aspecto foi apresentado. A nomeação do DPO poderia estar contemplada já na etapa inicial de preparação, já que ela é fundamental para a estruturação da governança em proteção de dados. Sem uma definição clara das lideranças responsáveis e das diretrizes básicas, há o risco de que etapas operacionais avancem sem o devido alinhamento sobre responsabilidades e parâmetros normativos necessários para a conformidade com a LGPD.

A quarta dimensão da auditoria abordou o tema da capacitação, este ponto já foi analisado neste trabalho em conjunto com a primeira dimensão, correspondente à fase de preparação, conforme os argumentos e fundamentos já apresentados ao longo desta pesquisa.

Isso se deve ao fato de que a capacitação não deve ser tratada como um elemento isolado ou meramente operacional, mas sim como um componente estruturante da fase preparatória, essencial para a consolidação de uma cultura organizacional voltada à proteção de dados.

Nesse sentido, passa-se à análise da quinta dimensão, que trata sobre a conformidade de tratamento, composta por 08 (oito) questões que versam sobre elementos centrais da operacionalização da LGPD nas instituições auditadas. Os temas abordados nesta etapa incluem:finalidade das atividades de tratamento de dados pessoais, bases legais, registro das operações de tratamento de dados pessoais, relatório de impacto à proteção de dados pessoais.

O Relatório de Impacto à Proteção de Dados Pessoais é um documento que visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018). De uma análise da auditoria em debate, constata-se que apenas 2% dos auditados elaboraram o documento.

Observa-se que o questionário aplicado na auditoria não abordou diretamente a elaboração da Avaliação de Impacto. Contudo, ao examinar o Acórdão, percebe-se que o tema foi tratado no tópico relacionado ao RIPD, o que pode levar a interpretações de que se tratam do mesmo instrumento jurídico. Essa diferença entre o questionário e o relatório final pode dificultar a clareza e a transparência dos resultados da auditoria, indicando que poderia haver um alinhamento mais claro entre os documentos utilizados no processo.

A LGPD contempla dois instrumentos distintos relacionados à análise de impactos: a avaliação de impacto à privacidade e o relatório de impacto à proteção de dados pessoais (RIPD). Conforme Grasso (2022, p. 167-168), “a avaliação de impacto à privacidade [...] é medida de boas práticas, enquanto o RIPD é obrigatório assim que preenchidas certas condições, de modo que não elaborar um RIPD, quando necessário, pode ensejar em sanções”. Essa diferenciação é importante para compreender as exigências legais e as obrigações a serem cumpridas pelas organizações.

A análise dos riscos associados às atividades de tratamento de dados não pode se limitar apenas à prevenção de falhas de segurança, tendo em vista que iniciativas que envolvem a aplicação de tecnologias emergentes, por exemplo, podem gerar impactos significativamente mais graves quando conduzidas de forma irresponsável, como no caso de decisões discriminatórias ilegais, decorrentes do uso de informações tendenciosas no treinamento de sistemas baseados em inteligência artificial.

A sexta dimensão da auditoria trata sobre a efetivação dos direitos dos titulares dos dados pessoais, compreendendo um total de 05 (cinco) questões. Os temas avaliados concentram-se, principalmente, na existência e divulgação da política de privacidade da organização, bem como nos mecanismos implementados para assegurar o atendimento aos direitos dos titulares. Após análise detalhada, não foram identificadas lacunas significativas nesta dimensão, razão pela qual não se faz necessária a apresentação de críticas ou propostas de melhoria neste ponto específico da auditoria.

A sétima dimensão da auditoria refere-se ao compartilhamento de dados pessoais, sendo composta por 05 (cinco) questões que visam avaliar como as organizações públicas auditadas tratam os fluxos de compartilhamento de dados com outros órgãos e entidades, sejam eles públicos ou privados. Cabe destacar que, neste trabalho, dedicamos um capítulo específico à análise aprofundada desta temática, no qual abordamos detalhadamente as diversas nuances envolvidas nas operações de compartilhamento de dados.

Caso a organização auditada afirmasse que identificou os dados pessoais que são compartilhados, era então exibida uma subquestão relativa à conformidade dessas transferências e compartilhamentos com a LGPD. No entanto, apenas 34% das instituições responderam afirmativamente.

Embora tais perguntas sejam relevantes para mapear as práticas existentes, elas parecem estar voltadas predominantemente para a identificação formal dessas operações. É importante lembrar que, conforme os princípios da proteção de dados, o mero ato de informar que há compartilhamento não é suficiente para validar a conformidade com a legislação. É necessário observar os critérios mencionados no capítulo 1 da presente dissertação, além da cronologia das medidas adotadas, ou seja, se foram implementadas previamente ações de segurança e controles adequados.

Outro ponto que merece ser incorporado ao instrumento de auditoria diz respeito à proporcionalidade e à finalidade do compartilhamento, de modo a coibir práticas abusivas ou desnecessárias. O episódio envolvendo o IBGE, exemplo que foi abordado no início da presente dissertação, demonstrou que o compartilhamento massivo de dados, ainda que sob uma base legal aparentemente válida, pode ferir os princípios da LGPD se desproporcional e sem salvaguardas adequadas.

A oitava e penúltima dimensão da auditoria trata da violação de dados pessoais, sendo composta por 06 (seis) questões voltadas à avaliação da estrutura e dos procedimentos

adotados pelas organizações públicas com temas planos de respostas a incidentes, sistemas de gestão a incidentes, monitoramento de eventos, comunicação de incidente de segurança que possa acarretar risco ou dano ao titular.

No que se refere aos questionários, não foram identificadas considerações adicionais que indicassem um aprofundamento nas questões formuladas. Por outro lado, chama atenção a ausência de um ponto relevante: não há qualquer menção à existência de um plano de emergência e continuidade do negócio. Esse tipo de planejamento é fundamental para que a organização esteja preparada para responder a incidentes de segurança, assegurando a mitigação de impactos e a continuidade das atividades essenciais.

Isso porque, dentre os vários exemplos concretos de gravidade de incidentes de segurança para a Administração Pública, podemos mencionar o que ocorreu em outubro de 2023, quando o sistema de gestão da Prefeitura de Araguari, no Estado de Minas Gerais, foi alvo de um ataque hacker. Conforme informado pelo Município, a invasão resultou na exclusão de informações do sistema, sem, contudo, a cópia ou retenção dos dados, a perda de registros comprometeu o funcionamento do sistema e gerou paralisação temporária de serviços essenciais, evidenciando o impacto direto que incidentes de segurança podem ter sobre a continuidade da prestação de serviços (GLOBO, 2023).

A nona e última dimensão da auditoria trata das medidas de proteção, sendo composta por 05 (cinco) perguntas que avaliam se as organizações públicas auditadas adotaram salvaguardas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados, dentre os temas, são medidas de segurança, controle de acesso em sistemas, registro de eventos (logs), utilização de criptografia, privacy by design e privacy by default.

No que diz respeito a essa dimensão, observa-se que a auditoria tratou o tema da criptografia de maneira bastante pontual, restringindo-se a uma única pergunta sobre a utilização dessa técnica de segurança pela Administração Pública. Essa abordagem, embora válida, revela-se limitada diante da complexidade do tema, especialmente quando se consideram os dados apresentados na introdução deste trabalho.

Os dados apresentados pelo CITR Gov demonstram que, nos últimos 05 (cinco) anos, a criptografia tem sido o principal fator envolvido nos incidentes de segurança registrados no setor público, totalizando um número expressivo de 12.912 ocorrências. (BRASIL, 2025). Ou

seja, a temática é um ponto delicado quando se trata de proteção de dados, nesse sentido, uma abordagem tão pontual pode não refletir a complexidade inerente à temática.

Do ponto de vista da efetividade da segurança da informação, a auditoria poderia ser aprofundada com perguntas como: Que tipo de criptografia foi adotada: em repouso, em trânsito ou ambos? Houve teste de eficácia dos controles de criptografia implementados? Existe monitoramento de tentativas de quebra de criptografia? Foram identificadas falhas, incidentes ou violações anteriores relacionadas à criptografia? Se sim, quais medidas foram adotadas?

É importante destacar que, no Capítulo 1 deste trabalho, abordamos a ocorrência de golpes baseados em técnicas de *sniffing*, justamente em contextos onde os dados trafegam sem o devido uso de criptografia. Esse exemplo real de vulnerabilidade evidencia o quanto a proteção da informação em trânsito é essencial para a segurança dos dados pessoais e para a prevenção de fraudes.

Diante desse cenário, observa-se que a abordagem adotada na auditoria, ao se limitar a uma única pergunta sobre o uso de criptografia, deixa de explorar aspectos relevantes do tema. Considerando a gravidade e a recorrência dos incidentes de segurança relacionados à criptografia, seria recomendável um aprofundamento maior na análise. Essa limitação metodológica pode dificultar a identificação de aspectos relevantes relacionados à segurança da informação e limitar a elaboração de recomendações mais detalhadas voltadas à proteção de dados pessoais no setor público.

Após a contextualização da auditoria realizada pelo TCU, bem como a análise crítica tanto da metodologia adotada quanto dos temas abordados nos questionários aplicados, cabe agora destacar possíveis temáticas relevantes que não foram abarcadas pelo instrumento de auditoria, mas que se mostram de fundamental importância. Tal abordagem se justifica, sobretudo, diante do papel estratégico desempenhado pelos Tribunais de Contas na indução de políticas públicas e na fiscalização dos seus jurisdicionados.

3.1.3 Lacunas identificadas na auditoria

A fim de conferir maior rigor metodológico à análise do questionário de auditoria utilizado pelo TCU, foi realizada uma análise de lacunas, fundamentada no cruzamento direto entre os dispositivos da LGPD e as questões contempladas pelo instrumento de avaliação. O objetivo desse procedimento foi verificar a cobertura normativa do questionário, identificando

os pontos plenamente abordados, já detalhados no subcapítulo anterior, e as lacunas relevantes que podem comprometer a eficácia da auditoria na aferição da conformidade das organizações públicas com a LGPD.

Para dar suporte a essa análise, elaborou-se uma tabela comparativa que sintetiza os principais resultados do cruzamento entre os dispositivos da LGPD e as questões constantes do questionário. A tabela está organizada em quatro colunas principais: o artigo da LGPD, a exigência legal associada, a indicação sobre a presença ou ausência desse item no questionário, e uma coluna de observações, destinada a registrar eventuais lacunas ou limitações identificadas. Esse formato permitiu uma análise sistemática, facilitando a visualização das omissões existentes e evidenciando quais aspectos da legislação não foram devidamente contemplados na auditoria

Tabela 7 – Cruzamento entre dispositivos da LGPD e questões do questionário de auditoria

Artigo da LGPD	Exigência Legal	O Questionário aborda?	Observação Crítica
Art. 12 e 13	Anonimização e pseudoanonimização	Parcial	Há menção genérica a medidas de segurança, mas não há uma pergunta clara sobre técnicas de anonimização para minimização de riscos.
Art. 15	Término do tratamento / Política de retenção e descarte	Não	Não há perguntas sobre ciclo de vida dos dados, prazos de retenção ou descarte seguro.
Art. 20	Decisão automatizada	Não	Não há nenhuma pergunta sobre decisões automatizadas, nem sobre direito de revisão pelo titular.
Art. 6º, X	Não discriminação	Não	Lacuna

fonte: elaborado pela autora

Outro aspecto importante identificado na análise de lacunas foi a ausência de perguntas no questionário relacionadas à revisão periódica das políticas de privacidade das organizações. A atualização contínua dessas políticas é uma exigência implícita da própria dinâmica da proteção de dados, dada a necessidade de adaptação às mudanças normativas, tecnológicas e organizacionais. Além disso, o instrumento de avaliação também não abordou a existência de indicadores de governança em privacidade, que são fundamentais para

monitorar a efetividade das ações implementadas, permitir o acompanhamento de resultados e apoiar a tomada de decisão em níveis estratégicos da administração pública.

Identificou-se também a ausência de um aspecto fundamental: questões relacionadas à transparência, com fundamento na Lei de Acesso à Informação. Esse tema é relevante, sobretudo em se tratando de uma auditoria conduzida pelo próprio Tribunal de Contas, instituição cuja missão inclui a promoção da transparência e do controle social.

No tópico 1.1.3. da presente dissertação, discute-se conceitos introdutórios e o conflito aparente entre as normas da LGPD e da LAI, evidenciando, a partir de dados e exemplos reais, que a LGPD tem sido, em determinados contextos, invocada como fundamento para restringir indevidamente o acesso a informações públicas garantido pela LAI.

Este ponto é importante, pois ressalta uma das distinções mais significativas entre a aplicação da LGPD no setor público e no setor privado, este último não está submetido ao dever de transparência imposto à Administração Pública. Assim, a busca pelo equilíbrio entre a proteção de dados pessoais e a transparência pública constitui um desafio central para o setor público, que não deve ser negligenciado em processos de auditoria e fiscalização.

No entanto, embora a auditoria objeto do presente estudo não tenha contemplado especificamente essa temática, durante o desenvolvimento da pesquisa foi identificada uma auditoria operacional realizada pelo TCU, registrada sob o TC 002.249/2023-5, que aborda de forma aprofundada os desafios relacionados à implementação da LGPD no contexto de sua compatibilização com as exigências da LAI. Essa auditoria foi estruturada em torno de quatro questões-chave.

Diante da complexidade e relevância do tema, compreende-se que a realização de uma auditoria autônoma produz efeitos mais aprofundados e específicos. No entanto, mesmo diante dessa autonomia temática, seria pertinente que a presente auditoria da LGPD contemplasse, ainda que de forma simplificada, ao menos uma questão relacionada ao tema, assim como fez com outros assuntos que, embora também contem com auditorias específicas, foram abordados resumidamente no instrumento atual.

3.2 Lições extraídas

A partir da análise dos resultados da auditoria realizada pelo TCU sobre a implementação da LGPD na Administração Pública, algumas lições importantes podem ser extraídas. Em primeiro lugar, os dados levantados deixam claro um baixo grau de aderência à

Lei por parte dos órgãos públicos federais. Essa constatação nos leva a uma conclusão preocupante: nossos dados pessoais, enquanto cidadãos, seguem expostos e, consequentemente, estamos todos vulneráveis a incidentes de segurança e uso indevido de informações.

Outro ponto que merece destaque é a relação direta entre a fala do Ministro relator e a teoria da dimensão objetiva dos direitos fundamentais, já abordada no primeiro capítulo deste trabalho. Mesmo reconhecendo os limites da sua atuação, em razão da competência da ANPD, o Ministro sinalizou que o TCU não poderia se manter inerte diante de um cenário de fragilidade institucional em matéria de proteção de dados. Esse posicionamento reforça a ideia de que os direitos fundamentais possuem uma dimensão que transcende a esfera individual, impondo ao Estado um dever de proteção ativa e eficaz.

A partir da análise realizada, é possível reconhecer que a auditoria de conformidade aplicada aos órgãos da Administração Pública federal representou um passo relevante na inserção da proteção de dados pessoais na agenda do controle externo. No entanto, certos aspectos metodológicos adotados podem ter limitado uma apreciação mais aprofundada sobre a complexidade do tema. A padronização dos questionários, a abordagem mais superficial de pontos sensíveis, como o uso de criptografia, e a ausência de tópicos importantes, como a existência de planos de continuidade de negócios, sinalizam oportunidades de aprimoramento.

Diante do aumento de incidentes de segurança e da crescente responsabilidade dos órgãos públicos na proteção das informações dos cidadãos, uma abordagem mais contextualizada e sensível às especificidades de cada órgão pode contribuir para um controle mais efetivo e alinhado aos desafios atuais da governança de dados.

Além disso, o próprio questionário utilizado na auditoria evidenciou algumas limitações. Apesar de ter cumprido o papel de oferecer um panorama inicial, faltou aprofundamento técnico nas perguntas. A ausência de questionamentos mais direcionados, capazes de verificar a formalização e a aplicação prática das medidas adotadas, reduziu o potencial diagnóstico da auditoria. Em um tema como a proteção de dados pessoais, são justamente os detalhes que distinguem uma estrutura formal de uma estrutura efetivamente comprometida com a segurança da informação.

Por fim, chama atenção a ausência de um olhar mais atento para um tema caro ao próprio TCU: a LAI. A auditoria deixou de explorar, mesmo que de forma superficial, a interrelação entre a LGPD e a LAI, um ponto fundamental para o equilíbrio entre

transparência e proteção de dados no setor público.Essas lições evidenciam a necessidade de aperfeiçoamento das futuras auditorias sobre o tema, com abordagens metodológicas mais alinhadas à complexidade da proteção de dados e à efetividade dos direitos fundamentais.

CONCLUSÃO

A presente dissertação teve como objetivo analisar a atuação do TCU na fiscalização da proteção de dados pessoais no setor público, tomando como base a auditoria que resultou no Acórdão nº 1384/2022. A pesquisa procurou compreender de que forma o controle externo tem incorporado a temática da proteção de dados, destacando os avanços e as limitações observadas, com especial atenção à metodologia empregada e ao seu potencial de induzir melhorias nas práticas adotadas pelos órgãos auditados.

O problema que norteou esta pesquisa partiu da constatação de que, embora o TCU exerça papel fundamental na fiscalização da implementação da LGPD nos órgãos públicos federais, há uma carência de estudos críticos que avaliem detalhadamente a metodologia e os critérios adotados na Auditoria nº 1384/2022. Essa lacuna dificulta a compreensão do alcance real da atuação do TCU, assim como a identificação de eventuais limitações e oportunidades de aprimoramento na fiscalização da proteção de dados pessoais no setor público. Diante desse cenário, este trabalho buscou responder: se existem limitações e oportunidades de melhoria na auditoria do TCU, conforme o Acórdão nº 1384/2022, para a fiscalização da implementação da LGPD nos órgãos públicos federais?

O objetivo principal desta investigação foi analisar os elementos que compõem a atuação do TCU na auditoria sobre a implementação da LGPD, a partir do estudo do Acórdão nº 1384/2022, com o intuito de identificar suas contribuições e limitações. A partir das análises realizadas ao longo desta pesquisa, percebe-se que a atuação do TCU na fiscalização da implementação da LGPD na administração pública federal ainda está em fase inicial. A auditoria examinada, foco deste estudo, revelou uma abordagem que poderia ser mais aprofundada, apresentando questionamentos relativamente superficiais sobre aspectos essenciais da proteção de dados pessoais. Entretanto, é importante reconhecer que essa auditoria constituiu um passo relevante para inserir a temática no âmbito do controle externo. Esse primeiro movimento institucional, mesmo que ainda não atenda integralmente às demandas da LGPD, aponta para a necessidade de desenvolver gradualmente mecanismos de fiscalização mais consistentes e eficazes.

A conclusão alcançada a partir da análise da Auditoria nº 1384/2022 confirma a hipótese inicialmente proposta nesta dissertação: diante do contexto recente de vigência da LGPD à época da fiscalização, o TCU adotou uma metodologia orientada mais à sensibilização e ao diagnóstico preliminar de conformidade do que à exigência de medidas estruturais e aprofundadas. Essa escolha metodológica, embora compreensível em um estágio inicial de implementação normativa, revelou limitações quanto à abrangência dos critérios adotados e à efetividade das recomendações formuladas, evidenciando desafios importantes para a consolidação de uma política pública robusta de proteção de dados no setor público federal.

Para atingir o objetivo principal e, consequentemente, responder a pergunta proposta nesta pesquisa, os objetivos específicos foram cuidadosamente explorados ao longo dos capítulos, servindo como alicerces para a análise crítica desenvolvida. Cada um deles contribuiu para a construção de uma compreensão mais aprofundada sobre os desafios enfrentados na implementação da LGPD no setor público e sobre o papel fiscalizatório do TCU nesse processo.

O desenvolvimento do primeiro capítulo permitiu o cumprimento do primeiro objetivo específico desta dissertação, ao proporcionar uma base teórica e normativa sólida sobre a proteção de dados pessoais. Foram abordados os principais conceitos ligados ao direito fundamental à proteção de dados, seus fundamentos constitucionais, os riscos associados ao tratamento inadequado de informações pessoais e as ameaças cibernéticas mais frequentes, além das especificidades do tratamento de dados pelo poder público, incluindo as tensões entre a LGPD e a LAI.

Essas informações serviram de parâmetro técnico e jurídico essencial para a análise da auditoria realizada pelo TCU, explorada no terceiro capítulo. Ao realizar o cruzamento entre os referenciais apresentados neste primeiro capítulo e os pontos efetivamente fiscalizados na auditoria, foi possível constatar lacunas significativas. Entre elas, destaca-se a ausência de verificação quanto ao descarte seguro de documentos, dados pessoais no portal da transparência, entre outros.

Além disso, ao analisar os fundamentos constitucionais e a teoria da dimensão objetiva dos direitos fundamentais, consolidou-se a compreensão de que, uma vez dotado de instrumentos técnicos e normativos, o TCU não apenas pode, mas, havendo os mecanismos necessários, tem o dever de atuar na fiscalização da proteção de dados. Esses mecanismos

foram aprofundados no segundo capítulo, o que contribuiu para o alcance do próximo objetivo específico desta pesquisa.

No decorrer da pesquisa, foram apresentadas as três modalidades de auditoria previstas no âmbito do controle externo: auditoria de conformidade, auditoria financeira e auditoria operacional. Contudo, para fins de análise e discussão nesta dissertação, o foco foi direcionado às duas modalidades mais pertinentes ao tema: a auditoria de conformidade e a auditoria operacional. Observou-se que o TCU, ao realizar a fiscalização sobre a implementação da LGPD na administração pública federal, escolheu adotar o modelo de auditoria de conformidade, centrando-se na verificação do cumprimento formal das exigências legais.

A estruturação de achados de auditoria operacional demonstrada no segundo capítulo poderia ter contribuído significativamente para a fiscalização da LGPD no setor público. A construção de um achado envolve a comparação entre a situação encontrada e o critério estabelecido, exigindo a identificação de quatro elementos: critério (o que deveria ser), condição (o que é), causa (por que a situação está fora do esperado) e efeito (consequência da não conformidade). Essa estrutura oferece um roteiro lógico que permite aos auditores diagnosticar, de forma fundamentada, os problemas relacionados à governança de dados pessoais, como ausência de políticas internas, fragilidade nos controles ou descumprimento das obrigações legais previstas na LGPD.

O critério de auditoria, nessa aplicação, pode ser baseado em dispositivos legais da própria LGPD, guias de boas práticas da ANPD ou normas internas de governança de dados. Já a identificação da condição envolve a verificação, por meio de coleta de evidências, da situação real encontrada no órgão público auditado. A partir da análise da causa, é possível compreender fatores como ausência de capacitação, insuficiência de recursos tecnológicos ou falta de prioridade institucional para o tema. Por fim, a identificação dos efeitos pode evidenciar riscos de exposição indevida de dados pessoais, impactos na privacidade dos cidadãos e eventuais sanções administrativas.

Outro aspecto essencial da auditoria operacional é a obtenção e validação de evidências apropriadas e suficientes para sustentar os achados. Essas evidências podem ser físicas, documentais, testemunhais ou analíticas. No caso da LGPD, isso pode incluir, por exemplo, registros de incidentes de segurança, políticas internas de privacidade, entrevistas com os encarregados de dados (DPOs), entre outros elementos. A triangulação dessas

diferentes fontes fortalece a credibilidade dos resultados, oferecendo um diagnóstico mais consistente para fundamentar as recomendações do órgão de controle.

A análise desenvolvida no terceiro capítulo, voltada para o atendimento dos objetivos específicos remanescentes, apontou a existência de limitações metodológicas que impactaram diretamente o conteúdo e a estrutura do questionário aplicado pelo TCU. Embora o instrumento tenha cumprido seu papel ao oferecer um panorama geral sobre a situação, observou-se uma carência de aprofundamento técnico e de perguntas que permitissem avaliar, com maior precisão, o grau de maturidade institucional dos órgãos públicos em relação à proteção de dados pessoais.

Percebeu-se uma oportunidade de aprimoramento no sentido de incluir questionamentos voltados à formalização e aos mecanismos de avaliação da efetividade das medidas adotadas em conformidade com a legislação. Também se identificou a possibilidade de um olhar mais atento à interrelação entre a LGPD e a LAI, aspecto essencial para o adequado equilíbrio entre transparência e proteção de dados no setor público.

É importante reconhecer algumas limitações desta pesquisa, o estudo concentrou-se na análise de uma única auditoria realizada pelo TCU, o que restringe a possibilidade de generalização para outras ações de controle externo ou para o conjunto dos Tribunais de Contas brasileiros. Além disso, a abordagem metodológica adotada foi predominantemente documental e bibliográfica, sem a realização de pesquisa de campo ou entrevistas com os auditores responsáveis ou representantes dos órgãos fiscalizados. Ressalta-se, ainda, que o recorte temporal da pesquisa reflete a realidade vigente à época da auditoria analisada, o que pode não representar o estágio atual de maturidade institucional do TCU em relação à fiscalização da proteção de dados pessoais. Essas limitações, contudo, não comprometem a relevância das reflexões apresentadas, mas indicam oportunidades para aprofundamentos futuros.

Diante das reflexões apresentadas, esta pesquisa oferece uma contribuição relevante tanto para o campo acadêmico quanto para a prática institucional. Do ponto de vista teórico, o trabalho reforça a importância de incorporar a proteção de dados pessoais como elemento integrante do controle externo, ampliando o debate sobre a accountability no poder público. Em termos práticos, os achados desta dissertação podem servir de subsídio para o aperfeiçoamento das futuras auditorias do TCU e de outros Tribunais de Contas, contribuindo para o fortalecimento da governança em privacidade e proteção de dados.

Por fim, recomenda-se que pesquisas futuras aprofundem a análise sobre os impactos concretos das auditorias em relação à efetividade das ações de proteção de dados adotadas pelos órgãos públicos. Sugere-se, ainda, a realização de estudos comparativos com outras cortes de contas, incluindo os Tribunais de Contas Estaduais, bem como investigações empíricas que envolvam entrevistas com auditores e gestores públicos responsáveis pela implementação da LGPD. Tais iniciativas certamente enriquecerão o campo de estudos sobre proteção de dados e controle externo, promovendo a construção de políticas públicas mais eficientes e alinhadas aos direitos fundamentais dos cidadãos.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo para o poder público sobre a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 10 mar. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Dispõe sobre a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) para agentes de tratamento de pequeno porte. **Diário Oficial da União: seção 1**, Brasília, DF, 27 fev. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 13 mar. 2025.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Anatel passa por auditoria do TCU sobre a implementação da LGPD. **Agência Nacional de Telecomunicações**, 2024. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-passa-por-auditoria-do-tcu-sobre-a-implementacao-da-lgpd. Acesso em: 7 fev. 2025.

AGU – ADVOCACIA-GERAL DA UNIÃO. **Parecer nº 00001/2024/CNCIC/CGU/AGU. Aplicabilidade da Lei Geral de Proteção de Dados aos convênios e instrumentos congêneres**. Brasília, 26 jan. 2024. Disponível em: https://www.gov.br/transferegov/pt-br/comunicados/arquivos-e-imagens/parecer-n-00001-2024.pdf. Acesso em: 8 jun. 2025.

ALMEIDA, Jéssica de. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como instrumento de accountability na Administração Pública. **Cadernos Jurídicos da FADI**, v. 4, n. 1, p. 135–160, 2021. Disponível em: https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/95/80. Acesso em: 10 jun. 2025.

AMARAL JÚNIOR, José Levi Mello do. Sobre a organização dos poderes em Montesquieu: comentários ao capítulo VI do livro XI de O espírito das leis. **Revista dos Tribunais**, ano 97, v. 898, fev. 2008.

ARAÚJO, Inaldo da Paixão Santos. **Introdução à auditoria operacional**. 4. ed. Rio de Janeiro: **Editora FGV**, 2008.

BITENCOURT, Caroline Müller; MARTINS, Luisa Helena Nicknig. A inteligência artificial nos órgãos constitucionais de controle de contas da administração pública brasileira. **Revista de Investigações Constitucionais**, Curitiba, v. 10, n. 1, p. 275–298, jan./abr. 2024. Disponível em: https://www.scielo.br/j/rinc/a/WJgdHhvqpvyr7XnHhMN39Wz/?lang=pt. Acesso em: 17 jun. 2025.

BRAGA, M. P. N. O Tribunal de Contas da União e a efetividade do direito à proteção de dados pessoais na Administração Pública Federal. **Revista de Direito da ADVOCEF**, [S. l.], v. 21, n. 38, p. 267–288, 2025. Disponível em: https://revista.advocef.org.br/index.php/ra/article/view/459. Acesso em: 11 jun. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Relatório do Ciclo de Monitoramento 2023**. Brasília: **ANPD**, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf. Acesso em: 15 nov. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público**. Brasília, DF: **ANPD**, 2023. Disponível

em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 17 jun. 2025.

BRASIL. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov. CTIR Gov em números. **CTIR Gov**, [S. l.], [s.d.]. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 15 jun. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 jun. 2018.

BRASIL. Decreto nº 12.069, de 7 de março de 2024. Dispõe sobre a Estratégia Nacional de Governo Digital. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/D12069.htm. Acesso em: 6 mar. 2025.

BRASIL. Decreto nº 12.069, de 9 de janeiro de 2024. Regulamenta a Lei nº 14.129, de 2021, sobre a transformação digital no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2024/Decreto/D12069.htm. Acesso em: 13 mar. 2025.

BRASIL. Estruturas organizacionais do governo federal. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/estruturas-organizacionais. Acesso em: 9 fev. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União: seção 1**, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 jun. 2024.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre a transformação digital no Brasil e estabelece a Lei de Governo Digital. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 6 mar. 2025.

BRASIL. Medida Provisória nº 954, de 29 de abril de 2020. Dispõe sobre a disponibilização de informações essenciais para a execução do Censo Demográfico pelo Instituto Brasileiro de Geografia e Estatística – IBGE, durante o estado de calamidade pública de que trata o Decreto Legislativo nº 6, de 20 de março de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 30 set. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Estruturas organizacionais. **Ministério da Gestão e da Inovação em Serviços Públicos**, 2024. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/estruturas-organizacionais. Acesso em: 9 fev. 2025.

BRASIL. Polícia Federal deflagra operação contra organização criminosa especializada em obtenção e venda de dados sigilosos do INSS. **Polícia Federal**, 2024. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2024/09/pf-deflagra-operacao-contra-organizacao-criminosa-especializada-em-obtencao-e-venda-de-dados-sigilosos-do-inss. Acesso em: 29 set. 2024.

BRASIL. Secretaria de Governo Digital. **Guia de resposta a incidentes cibernéticos**. Brasília: **Ministério da Gestão e da Inovação em Serviços Públicos**, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf. Acesso em: 5 jun. 2025.

BRASIL. Superior Tribunal de Justiça. Segunda Turma. Agravo Interno no Agravo em Recurso Especial n. 2.008.980/AL, Rel. Min. Mauro Campbell Marques, j. 28 fev. 2023. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788&registro_numero=202201522622. Acesso em: 30 maio 2025.

BRASIL. Tribunal de Contas da União. **ISSAI 100 – Princípios Fundamentais da Auditoria do Setor Público**. Brasília: **TCU**, 2024. Disponível em: https://portal.tcu.gov.br/data/files/80/04/47/3A/C1DEF610F5680BF6F18818A8/ISSAI_100_principios_fundamentais_auditoria_setor_publico.pdf. Acesso em: 29 fev. 2025.

BRASIL. Tribunal de Contas da União. **Manual de auditoria operacional**. 4. ed. Brasília: **TCU**, Secretaria-Geral de Controle Externo (Segecex), 2020.

CABRAL, Flávio Garcia. Como o Tribunal de Contas da União tem se comportado ao longo da Constituição de 1988?. **A&C - Revista de Direito Administrativo & Constitucional**, Belo Horizonte, v. 21, n. 85, p. 161–183, 2021. DOI: 10.21056/aec.v21i85.1579. Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1579. Acesso em: 16 jun. 2025.

CALDERA, Loana Costa Irmão. Duas formas de pensar: insights da economia comportamental e inteligência artificial nos processos decisórios de controle externo do Tribunal de Contas da União (TCU). 2023. 104 f. Dissertação (Mestrado em Governança, Tecnologia e Inovação) – Universidade Católica de Brasília, Brasília, 2023.

CALISSI, Jamile; FRANCO NEME, Eliana; ALBERTO MAIA, Bruno. A proteção de dados e o princípio da dignidade humana: uma compreensão acerca da autodeterminação informativa. **Revista do Direito Público**, [S. l.], v. 19, n. 1, p. 201–219, 2024. DOI: 10.5433/1980-511X.2024.v19.n1.46952. Disponível em: https://ojs.uel.br/revistas/uel/index.php/direitopub/article/view/46952. Acesso em: 9 jun. 2025.

CONSULTORIA NACIONAL DE CONVÊNIOS E INSTRUMENTOS CONGÊNERES – CNCIC. **Parecer nº 01/2024/CNCIC/CGU/AGU: aplicabilidade da LGPD a convênios e instrumentos congêneres**. [S.l.], 2024. Disponível em: https://ronnycharles.com.br/wp-content/uploads/2024/12/PArecer-01-2024-CNCIC-Aplicabilidade-da-Lei-Geral-de-Protecao-de-Dados-aos-convenios-e-instrumentos-congeneres-1.pdf. Acesso em: 6 jun. 2025.

COSTA, Gledson Pompeu Corrêa da; DUTRA, Tiago Alves de Gouveia Lins. Auditoria financeira na era do Big Data: novas possibilidades para avaliação e resposta a riscos em demonstrações financeiras do Governo Federal. **Revista do TCU**, Brasília, n. 131, p. 54–61, 2014. Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/62. Acesso em: 19 jun. 2025.

COSTA, Luiz Bernardo Dias. **O Tribunal de Contas no Estado Contemporâneo**. 2005. 139 f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Paraná, Centro de Ciências Jurídicas e Sociais, Curitiba, 2005.

COSTA, Maria Cristina Castilho. Sociedade informacional. **Comunicação & Educação**, São Paulo, Brasil, n. 15, p. 15–20, 1999. DOI: 10.11606/issn.2316-9125.v0i15p15-20. Disponível em: https://revistas.usp.br/comueduc/article/view/36858. Acesso em: 9 jun. 2025.

COSTA, Yara Cristine dos Santos. **A proteção de dados pessoais sensíveis e a transparência no setor público federal: desafios e práticas**. 2023. 151 f. Dissertação (Mestrado Profissional em Gestão Pública) – Universidade de Brasília, Brasília, 2023.

DONEDA, Daniel. **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 pessoais: fundamentos e desafios**. Rio de Janeiro: Renovar, 2006.
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.
DUTRA, Tiago Alves de Gouveia Lins; CHAMPOMIER, Jean-Michel. A função de auditoria financeira em Tribunais de Contas: as perspectivas do TCU e a experiência da Corte de Contas da França. **Revista do TCU**, Brasília, n. 130, p. 70–81, 2014. Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/43. Acesso em: 18 jun. 2025.
FERNANDES, Jorge Ulisses Jacoby. **Tribunais de Contas do Brasil: jurisdição e competência**. 2. ed. Belo Horizonte: Fórum, 2008.
FRAZÃO, Ana. Os dados pessoais como o "petróleo do século XXI" e a necessidade de regulação adequada. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 3. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2023. p. 218.
FREIRE, Elias Sampaio. **Direito Administrativo: teoria, jurisprudência e 1000 questões**. 7. ed. Rio de Janeiro: Elsevier, 2007.
FREITAS JUNIOR, Nilton; FERREIRA, Alyson Silva. Política de segurança da informação: uma proposta aplicada ao contexto da LGPD. **Pensar Acadêmico**, [S. l.], v. 23, n. 1, 2025. Disponível em: https://doi.org/10.21576/pensaracadmico.2025v23i1.4286. Acesso em: 10 jun. 2025.
G1. Ataque hacker exclui dados do sistema de gestão da Prefeitura de Araguari. **G1**, 25 out. 2023. Disponível em: https://g1.globo.com/mg/triangulo-mineiro/noticia/2023/10/25/ataque-hacker-exclui-dados-do-sistema-de-gestao-da-prefeitura-de-araguari.ghtml. Acesso em: 5 jun. 2025.
G1. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **G1**, 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 10 jun. 2025.
GONÇALVES, Benedito (Coord.). *Os 35 anos do Superior Tribunal de Justiça: Volume I – Direito Público*. Londrina: Editora Thoth, 2024. 433 p. ISBN 978-65-5959-903-5.
GRASSO, I. M. Relatório de impacto à proteção de dados pessoais na Lei Geral de Proteção de Dados: uma banalização? **Cadernos Jurídicos da Faculdade de Direito de Sorocaba**, [S. l.], v. 3, n. 1, p. 142–174, 2022. Disponível em: https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/95. Acesso em: 12 jun. 2025.
HACHEM, D. W. A discricionariedade administrativa entre as dimensões objetiva e subjetiva dos direitos fundamentais sociais. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 10, n. 35, p. 313–343, 2016. DOI: 10.30899/dfj.v10i35.104. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/104. Acesso em: 10 jun. 2025.
HACKER invade sistema da Prefeitura de Poços de Caldas e pede R$ 15 milhões de resgate. **G1 Sul de Minas**, 25 out. 2023. Disponível em: https://g1.globo.com/mg/sul-de-minas/noticia/2023/10/25/hacker-invade-sistema-da-prefeitura-de-pocos-de-caldas-e-pede-r-15-milhoes-de-resgate.ghtml. Acesso em: 9 jun. 2025.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE. **Cidades e estados: estatísticas e informações**. Disponível em: https://www.ibge.gov.br/cidades-e-estados. Acesso em: 13 fev. 2025.

LUCAS, Jessica Victoria. **A espionagem norte-americana durante a Guerra Fria e o século XXI: um paralelo entre o governo Truman e o segundo mandato Obama**. 2014. 91 f. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) – Universidade do Sagrado Coração, Bauru, SP, 2014. Orientadora: Profa. Ma. Beatriz Sabia Ferreira Alves.

MANNA BELLASALMA E SILVA, Tatiana; DIAS DA MOTTA, Ivan; MENEZES GONÇALVES, Aline. O direito à privacidade na sociedade informacional: construindo uma educação orientada pela proteção de dados. **Revista de Pesquisa e Educação Jurídica**, Florianópolis, Brasil, v. 9, n. 2, 2024. DOI: https://doi.org/10.26668/IndexLawJournals/2525-9636/2023.v9i2.10088. Disponível em: https://indexlaw.org/index.php/rpej/article/view/10088. Acesso em: 9 jun. 2025.

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

MELLO JUNIOR, João Câncio de. **A função de controle dos atos da administração pública pelo Ministério Público**. Belo Horizonte: Líder Cultura Jurídica, 2001.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.). **Tratado de proteção de dados pessoais**. Coord. executivo: Bruno Bioni. 2. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2023.

MENDES, Laura Schertel et al. (org.). **Direitos fundamentais na era digital** [recurso eletrônico]: anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD). Porto Alegre: Editora Fundação Fênix, 2023. 284 p. (Série Direito; 87). Disponível em: https://www.fundarfenix.com.br. ISBN 978-65-5460-079-8. DOI: https://doi.org/10.36592/9786554600798.

MENDES, Gilmar F. Direitos fundamentais e controle de constitucionalidade - Estudos de Direito Constitucional, 4ª edição. Rio de Janeiro: Saraiva, 2012. E-book. p.121. ISBN 9788502134249. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502134249/. Acesso em: 12 jul. 2025.

MENEZES, Ana Paula Veras Carvalho. **Inteligência artificial para identificação de indícios de fraude e corrupção em compras públicas no TCU**. 2023. 109 f. Dissertação (Mestrado em Administração Pública) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2023.

MITIDIERO, Daniel F.; MARINONI, Luiz Guilherme B.; SARLET, Ingo W. Curso de direito constitucional. 12. ed. Rio de Janeiro: Saraiva Jur, 2023. E-book. p.629. ISBN 9786553624771. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786553624771/. Acesso em: 12 jul. 2025.

MOREIRA NETO, Diogo de Figueiredo. **Curso de Direito Administrativo**. 12. ed. Rio de Janeiro: Forense, 2002. p. 74.

NARDELLI, Cleber. Segurança da Informação e LGPD Aplicado no Desenvolvimento de Software. In: **ESCOLA REGIONAL DE ENGENHARIA DE SOFTWARE (ERES)**, 5., 2021, Evento Online. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 169-178. DOI: https://doi.org/10.5753/eres.2021.18462.

NEVES, D. L. F.; LOPES, T. S. de A.; PAVANI, G. C.; SALES, R. M. A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber**, [s. l.], v.

13, p. 186-198, 9 jun. 2021. DOI 10.5281/zenodo.15073440. Disponível em: https://www.fatecpg.edu.br/revista/index.php/ps/article/view/171. Acesso em: 12 jun. 2025.
ORWELL, George. *1984*. São Paulo: Companhia das Letras, 2009.
PINHEIRO, Francischetto. A pesquisa jurídica: para além da revisão bibliográfica. **Revista Jurídica Cesumar – Mestrado**, Maringá, v. 19, n. 2, p. 429-457, 2019. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/6927/3531. Acesso em: 6 mar. 2025.
POZZO, Gabriela Tomaselli Bresser Pereira Dal. **As funções do Tribunal de Contas e o Estado de Direito**. Belo Horizonte: Editora Fórum, 2010.
POLÍCIA FEDERAL. PF deflagra operação contra organização criminosa especializada em obtenção e venda de dados sigilosos do INSS. 2024. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2024/09/pf-deflagra-operacao-contra-organizacao-criminosa-especializada-em-obtencao-e-venda-de-dados-sigilosos-do-inss. Acesso em: 29 set. 2024.
PRESTES, Felipe Pinheiro; PRÉVE, Daniel Ribeiro; BONA, Marcio Teza de. **Controles de proteção de dados pessoais dos povos indígenas implementados na FUNAI**. *Federal University of Rio Grande*, v. 34, n. 1, p. 60, 2024. DOI: https://doi.org/10.14295/juris.v34i1.17613.Acesso em: 23 abril. 2025.
REDE INTEGRAR. Plano Anual de Trabalho – PAT 2024 da Rede Integrar. Brasília: Instituto Rui Barbosa, 2024. Disponível em: https://redeintegrar.irbcontas.org.br/wp-content/uploads/2024/01/PLANO_ANUAL_DE_TRABALHO_2024.pdf. Acesso em: 17 jun. 2025.
RIBAS DO NASCIMENTO, V.; SCHORN RODRIGUES, M. A sociedade informacional em xeque: o princípio da publicidade versus o direito à intimidade e a Lei n. 12.527/11. **Revista Direitos Fundamentais & Democracia**, [S. l.], v. 14, n. 14.1, p. 181–195, 2013. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/380. Acesso em: 9 jun. 2025.
RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.
SERAFINI, Lucas. Os impactos da Lei Geral de Proteção de Dados Pessoais sobre os portais de transparência e as boas práticas determinadas pela Lei de Acesso à Informação. 2023. 149 f. Dissertação (Mestrado em Direito) – ATITUS Educação, Passo Fundo, 2023.
SILVA , Walyf Lopes da; SILVA, Camila Medeiros da; MATEUS, Carollayne Reges; ROCHA, Greicy Kelle Sousa; CRUVINEL, Larice Inez Alves; SILVA, Maria Fernanda Rodrigues da. Aspectos jurídicos da exposição de dados pessoais na internet e a sua relação com o direito fundamental à privacidade. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 8, n. 9, p. 666–684, 2022. DOI: 10.51891/rease.v8i9.6822. Disponível em: https://periodicorease.pro.br/rease/article/view/6822. Acesso em: 9 jun. 2025.
SOUZA, Nicolle Bêtta de; ACHA, Fernanda Rosa. A proteção de dados como direito fundamental: uma análise a partir da Emenda Constitucional 115/2022. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 8, n. 9, p. 666–684, 2022. DOI: 10.51891/rease.v8i9.6822. Disponível em: https://periodicorease.pro.br/rease/article/view/6822. Acesso em: 9 jun. 2025.
SUPREMO TRIBUNAL FEDERAL. **ADI nº 6.387**. [S. d.]. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 30 set. 2023.
SUPREMO TRIBUNAL FEDERAL. **Guia LGPD: guia de boas práticas e orientações sobre a Lei Geral de Proteção de Dados Pessoais no Supremo Tribunal Federal**. Brasília:

STF, 2021. Disponível em: https://bibliotecadigital.stf.jus.br/xmlui/bitstream/handle/123456789/7488/GUIA%20LGPD_13%202%20%281%29.pdf?sequence=1&isAllowed=y. Acesso em: 6 jun. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **AREsp 2.130.619**. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788&registro_numero=202201522622&publicacao_data=20230310&formato=PDF. Acesso em: 6 jun. 2025.

THE ECONOMIST. The world's most valuable resource is no longer oil but data. **The Economist**, 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 12 nov. 2024.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Orientações de auditoria de conformidade. Brasília: **TCU, Secretaria de Métodos e Suporte ao Controle Externo**, 2024. Disponível em: https://apoioauditoria.tcu.gov.br//wp-content/uploads/sites/17/2024/12/Orientacoes-de-auditoria-de-conformidade.pdf. Acesso em: 22 jun. 2025.

TRIBUNAL DE CONTAS DA UNIÃO (TCU), Secom. TCU adota modelo personalizado de assistente de redação baseado em inteligência artificial. Brasília: **Secom/TCU**, 20 jun. 2023. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-adota-modelo-personalizado-de-assistente-de-redacao-baseado-em-inteligencia-artificial. Acesso em: 17 jun. 2025.

TRIBUNAL DE CONTAS DO ESTADO DE MINAS GERAIS (TCE-MG). Acórdão nº 1.149.236. Belo Horizonte: **TCE-MG**, 2024. Disponível em: https://tcjuris.tce.mg.gov.br/Home/Detalhes/1149236. Acesso em: 5 jun. 2025.

VALADARES, Heloisa de Carvalho Feitosa. Sociedade informacional e execução da política pública de proteção de dados no Brasil: estudo comparado das estratégias adotadas no Brasil e na Austrália e o enforcement como diferencial de efetividade. 2024. 245 f. Tese (Doutorado em Direito) – Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2024.

WARREN, Samuel; BRANDEIS, Louis. *The right to privacy*. Harvard Law Review, [s.l.], v. 4, p. 2303-2312, 15 dez. 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 5 jan. 2025.