UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE MESTRADO PROFISSIONAL EM GESTÃO PÚBLICA PARA O DESENVOLVIMENTO DO NORDESTE

VIRNA DE SOUZA GODOY OLIVEIRA

PROTEÇÃO DE DADOS PESSOAIS:

Um estudo no âmbito dos processos administrativos eletrônicos da UFRPE (2020-2022)

Recife
2024

VIRNA DE SOUZA GODOY OLIVEIRA

PROTEÇÃO DE DADOS PESSOAIS:

Um estudo no âmbito dos processos administrativos eletrônicos da UFRPE (2020-2022)

Dissertação apresentada ao Mestrado em Gestão Pública para o Desenvolvimento do Nordeste, à Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de mestra em Gestão Pública.

Área de Concentração: Gestão Pública para o Desenvolvimento Regional

Orientador: Prof. Dr. Thiago Vasconcellos Modenesi

Recife

2024

Catalogação na Fonte
Bibliotecária Maria Betânia de Santana da Silva CRB4-1747

O48p Oliveira, Virna de Souza Godoy
Proteção de dados pessoais: um estudo no âmbito dos processos administrativos eletrônicos da UFRPE (2020-2022) / Virna de Souza Godoy Oliveira. - 2024.
93 folhas: il. 30 cm.

Orientador: Prof. Dr. Thiago Vasconcellos Modenesi .
Dissertação (Mestrado Profissional em Gestão Pública para o Desenvolvimento do Nordeste) – Universidade Federal de Pernambuco, CCSA, 2024.
Inclui referências e apêndices.

1. Proteção de dados. 2. Processo administrativo. 3. Tecnologia da informação – Administração. 4. Programas de compliance. I. Modenesi, Thiago Vasconcellos (Orientador). II. Título.

658.4038 CDD (22. ed.) UFPE (CSA 2024 – 045)

VIRNA DE SOUZA GODOY OLIVEIRA

PROTEÇÃO DE DADOS PESSOAIS:

Um estudo no âmbito dos processos administrativos eletrônicos da UFRPE (2020-2022)

Dissertação apresentada ao Mestrado em Gestão Pública para o Desenvolvimento do Nordeste, à Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de mestre em Gestão Pública.

Orientador: Thiago Vasconcellos Modenesi, Dr.

Aprovada em: 21 de março de 2024.

BANCA EXAMINADORA

Prof. Thiago Vasconcellos Modenesi (orientador), Dr.
Universidade Federal de Pernambuco

Profª. Emanuela Sousa Ribeiro (avaliadora), Drª.
Universidade Federal de Pernambuco

Profª. Monica Felts de La Roca Soares (avaliadora), Drª.
Universidade Federal de Pernambuco

Recife
2024

À minha família.

AGRADECIMENTOS

Agradeço a Deus por poder realizar esse sonho e por me manter firme durante essa jornada.

À minha família, por todo apoio, renúncia e compreensão da minha ausência. A vovó Socorro (Dona Coca) por todo amor e orações. Aos meus pais, Lany e S. Godoy, por serem base e pela paciência com os "colóquios", às minhas irmãs Oli e Ivana, por toda torcida, apoio, palavras e por acreditarem em mim. À Fafa por todo apoio e sessões de terapia. À tia Lu por sempre me motivar a alçar novos voos. Aos meus primos, Pedro e Uilson, por serem irmãos e me apoiarem. Às minhas afilhadas, Marina e Beatriz, por esperarem a "dindinha" terminar os estudos. Ao meu filho, Rafael, a razão por todo empenho e dedicação nesse processo, por todo amor, carinho, compreensão, motivação e paciência.

À Paula Nascimento, pelo apoio e compreensão da minha ausência, e à Ieda Cabral (*in memoriam*), por serem inspiração e exemplo de mulher na ciência. À Ligia, amiga obrigada por todas as orientações e por sentar ao meu lado quando precisei. Ao Rogério, por compartilhar comigo seu conhecimento, muito obrigada amigo. À Cris, pela torcida e atenção. À Patrícia, por ser um anjo na minha vida. A todos os meus amigos que torceram por mim.

Ao Prof. Thiago Modenesi, pela disponibilidade e paciência na orientação. Às professoras Emanuela Ribeiro e Monica Soares, pelas contribuições à pesquisa. A todos os professores que fazem parte do MGP/UFPE por compartilharem seus conhecimentos.

Aos professores da UFRPE, Romilson Cabral e Jorge Correia, por todo apoio, incentivo e troca durante essa jornada. A toda equipe da UFRPE e da PROGEPE por oportunizarem esse curso aos servidores, vocês transformaram minha vida. Ao chefe mais parceiro e compreensivo, Luiz Regueira. Aos amigos de jornada diária, por toda paciência, apoio, torcida e compreensão, Celia, Gleide, Joyce, Amanda, Marília, Jane e Dona Conceição.

Aos meus amigos, parceiros da vida e mosqueteiros, Matheus Batista e Rodolpho Belarmino (*chi-coach*), não tenho palavras para expressar toda minha gratidão por cada palavra, gesto, escuta, orientação, troca de conhecimento, contribuições e por não soltarem minha mão, sem vocês eu não teria conseguido chegar até aqui. Ainda, agradeço a vocês e às amigas queridas Elylian Pereira e Maria Lêda por todo apoio e noites de estudo, sem dúvida a equipe "Tico e Teco" era a mais animada da madrugada.

Aos colegas do MGP/UFPE, por serem a turma mais parceira e unida, foi muito divertido trilhar esse caminho com vocês ao meu lado.

Tudo tem o seu tempo determinado, e há tempo para todo o propósito debaixo do céu. (Eclesiastes 3:1)

RESUMO

O objetivo geral desta pesquisa foi analisar como se apresenta a proteção de dados pessoais à luz da governança de dados, a partir das normas que regulamentam o tratamento de dados pessoais no âmbito da Universidade Federal Rural de Pernambuco (UFRPE), no escopo dos processos administrativos eletrônicos. A governança de dados consiste no conjunto de políticas, a fim de garantir uma gestão adequada dos dados de uma instituição, a conformidade com as normas regulatórias e o gerenciamento dos riscos associados. No âmbito da administração pública, essa conformidade, ou *compliance*, se apresenta como um mecanismo de integridade pública. A pesquisa pretendeu identificar o cenário de adequação dos processos administrativos eletrônicos das Universidades Federais da região nordeste, a fim de fazer um comparativo com a UFRPE, bem como identificar ações e investimentos na promoção da proteção de dados pessoais e diagnosticar a conformidade dos níveis de acessos dos documentos que compõem os processos eletrônicos. Trata-se de uma pesquisa com abordagem qualitativa e de natureza aplicada. Quanto aos objetivos, tipifica-se como descritiva. Como método de investigação, é uma pesquisa diagnóstico e documental. A coleta de dados foi subdividida em três etapas. Na primeira etapa, foi elaborado um questionário, submetido às 20 Universidades Federais da região Nordeste, por meio da ferramenta Fala.BR. A segunda consistiu na pesquisa documental referente às diretrizes e às legislações federais e institucionais sobre governança de dados, proteção de dados pessoais e processo administrativo eletrônico, adotadas pela UFRPE. A última etapa verificou a conformidade e o nível de acesso (público ou restrito) dos documentos que compõem os processos de pensão civil, instruídos no período de abril de 2020 a dezembro de 2022, arquivados na Seção de Arquivo e Registro Funcional (SARF). Após a coleta, os dados foram organizados e tabulados em uma planilha do *Microsoft Excel*, e as frequências de cada pergunta foram calculadas. A partir da análise dos resultados, foi possível concluir que assegurar a conformidade do nível de acesso à informação em relação à proteção de dados pessoais no escopo dos processos administrativos eletrônicos é um desafio para a universidade, considerando que essa atribuição ainda é muito centrada nos operadores de tratamento de dados. Nesse sentido, é fundamental que a UFRPE implemente programas de *compliance*, proceda com o mapeamento de riscos de maneira holística, ofereça capacitação continuada, e atualize os sistemas de gestão de informação, a fim de disseminar o conhecimento, promover a cultura de proteção de dados no âmbito institucional e garantir a integridade e legalidade na prestação dos serviços.

Palavras-chave: conformidade; processo administrativo eletrônico; proteção de dados pessoais.

ABSTRACT

The general objective of this research was to analyze data protection based on data governance standards, UFRPE's (The Federal Rural University of Pernambuco) regulatory standards of personal data treatment, and the scope of electronic administrative procedures. Data governance reefers to the policies of securing adequate data managing by an institution, compliance to regulatory standards, and associated risk management. Within the scope of public administration, such compliance is considered a mechanism of public integrity. The present research intended to identify the adequacy of electronic administrative procedures within the Federal Universities from the Northeast region in order to compare them with UFRPE, as well as identify actions and initiatives to promote personal data protection and diagnose conformity to the levels of access to electronic procedures' documents. This research makes a qualitative approach to an applied character. Regarding its objectives, it is characterized as descriptive. As for its investigation methods, it is characterized as diagnostic and documental research. Data gathering was done in three phases. First, a questionnaire was prepared and submitted to all twenty Federal Universities from the Northeast region through the Fala.BR tool. The second phase involves documental research on federal guidelines and laws about data governance, personal data protection, and electronic administrative procedures adopted by UFRPE. The final phase verified compliance and access levels (public or classified) of civil pension documents that were instructed between April 2020 and December 2022, and filed in the Functional Record File. Once the data was gathered, it was entered into Microsoft Excel, and the frequency of each question was calculated. Upon analyzing the data, it has been found that maintaining compliance with regards to access to information and personal data protection within the electronic administrative procedures of the university is a challenging task, as it involves people who handle data on a regular basis. Therefore, it is of utmost importance that UFRPE implements compliance programs, provides continuous training to personnel, updates its information management systems, and promotes a data protection culture within the institution to ensure the integrity and legality of its service delivery.

Keywords: compliance; electronic administrative process; data protection.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

AGU	Advocacia-Geral da União
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
CGPPD	Comitê Gestor de Privacidade e Proteção de Dados
CGU	Controladoria-Geral da União
CNH	Carteira Nacional de Habilitação
CNPD	Conselho Nacional de Proteção de Dados Pessoais e da Privacidade
CONSU	Conselho Universitário
CPF	Cadastro Pessoa Física
EC	Emenda Constitucional
EGD	Estratégia de Governança Digital
ERP	*Enterpise Resource Flanning*
GDPR	*General Data Protection Regulation*
IFES	Instituição Federal de Ensino Superior
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LRF	Lei de Responsabilidade Fiscal
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
PDI	Plano de Desenvolvimento Institucional
PROAD	Pró-Reitoria de Administração
PROGEPE	Pró-reitora de Gestão de Pessoas
RG	Registro Geral
RGPD	Regulamento Geral sobre a Proteção de Dados
SARF	Seção de Arquivo e Registro Funcional
SEGES/ME	Secretaria de Gestão do Ministério da Economia
SEI	Sistema Eletrônico de Informações
SI	Segurança da Informação
SIAPE	Sistema Integrado de Administração de Recursos Humanos

SIG	Sistema Integrado de Gestão
SIGAA	Sistema Integrado de Gestão de Atividades Acadêmica
SIGRH	Sistema Integrado de Gestão de Recursos Humanos
SIPAC	Sistema Integrado de Patrimônio, Administração e Contratos
STD	Secretaria de Tecnologias Digitais
STPC/CGU	Secretaria de Transparência e Combate à Corrupção da Controladoria Geral da União
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
TRF-4	Tribunal Regional Federal da 4ª Região
UE	União Europeia
UFRN	Universidade Federal do Rio Grande do Norte
UFRPE	Universidade Federal Rural de Pernambuco

SUMÁRIO

1. INTRODUÇÃO

A globalização e o avanço tecnológico têm contribuído para que a administração pública busque modernizar seus procedimentos, a fim de tornar o Estado mais eficiente, promover inovação e celeridade no acesso à informação, bem como fornecer ferramentas para subsidiar tomadas de decisão, resguardar os direitos e os deveres dos órgãos, entidades e de seus agentes e sociedade em geral. Essa discussão remonta à década de 1990, quando se intensificaram os debates sobre a necessidade de uma reforma do Estado brasileiro, para aumentar a governança (Brasil, 1995).

Contemporaneamente, esse debate tem se ampliado, tendo em vista que a transformação digital tem permeado a realidade das entidades. Para Castells (2000), a transformação digital é essencial para a modernização da administração pública, pois permite a melhor utilização da informação e da tecnologia na gestão dos serviços. Essa reforma deve ser entendida como parte de uma mudança global que está transformando a forma como a sociedade e a economia funcionam, e que tem impacto direto na administração pública (Castells, 2000).

Cavalieri (2020a, p. 4) enfatiza que, nesse cenário de "Transformação Digital e da Sociedade da Informação, a Governança de Dados e o *Compliance* Digital assumem protagonismo como instrumento de Integridade Governamental", os quais merecem a atenção e a efetiva aplicação por parte do poder público. Ao referir-se à governança de dados, Barbieri (2019) a define como um conjunto de práticas, políticas e procedimentos que visam garantir a gestão adequada e segura dos dados numa organização, em conformidade às regulamentações e políticas internas (Barbieri (2019). Imbricado a este conceito, encontra-se o *compliance*, que se apresenta como um mecanismo de integridade pública, visando não apenas a conformidade legal, mas também a promoção de uma cultura institucional que priorize o comprometimento dos agentes públicos com o interesse coletivo (Magacho; Trento, 2021).

No âmbito normativo, constata-se que, nos últimos anos, têm sido publicados diversos dispositivos correlacionados com este tema. Em 2015, o Poder Executivo Federal sancionou o Decreto nº 8.539, de 08 de outubro de 2015, que dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Essa normativa determinou o prazo de dois anos, contados da sua publicação, para os órgãos e as entidades implementarem o uso do meio eletrônico para realização de processos administrativos (Brasil, 2015).

Considerando a possível vulnerabilidade de informações disponíveis na rede, discussões sobre a proteção de dados pessoais surgiram em todo mundo, principalmente no âmbito privado.

Conforme Frazão, Oliva e Abilio (2019, p. 679), tal preocupação ganhou ainda mais relevância diante do crescente interesse comercial nos dados pessoais, que se tornaram um ativo essencial para o desempenho e melhoria de diversas atividades, ressaltando que "tal arquitetura protetiva precisa ser endereçada igualmente ao Estado, para o qual os dados são também importantes para inúmeras finalidades públicas".

Na administração pública brasileira, apesar da existência da Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso à informação e contém dispositivos sobre proteção de informações pessoais, é com a denominada Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, com vigência parcial em 2020, que houve uma maior rigidez no tratamento e proteção desses dados, aumentando o nível de segurança e privacidade para os indivíduos (Brasil, 2018).

Ressalta-se que a proteção dos dados pessoais não era tão rigorosa quanto é hoje, embora já houvesse algumas leis para proteger a privacidade das pessoas. Esse fato decorre da evolução tecnológica e da capacidade de armazenamento e compartilhamento de informações em grande escala, elevando a importância da proteção de dados pessoais (Bioni, 2019).

A crescente preocupação com a segurança da informação e a privacidade dos indivíduos ganhou força mediante o avanço tecnológico e a velocidade, quase que imediata, da propagação de informações em meios digitais, tornando-se um tema socialmente relevante. A partir do ano de 2022, a proteção de dados pessoais adquiriu mais notoriedade, com *status* de uma garantia e direito fundamental expresso na Constituição brasileira, a partir da Emenda Constitucional (EC-115/2022), no qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais." (Brasil, 2022a). Nessa conjuntura, a proteção de dados pessoais amplia os direitos protetivos, garantindo a dignidade da pessoa humana, uma vez que, esses dados são de direito e propriedade apenas do indivíduo, não interessando a terceiros.

Outro grande marco na administração federal refere-se à Política de Governança Digital, instituída através do Decreto nº 8.638, de 15 de janeiro de 2016, posteriormente revogado pelo Decreto nº 10.332, de 2020, (alterado pelo Decreto nº 10.996, de 14 de março de 2022 e Decreto 11.260, de 22 de novembro de 2022), com o propósito de promover integração e direcionar os entes da gestão pública nas ações relacionadas à governança de dados. Por meio dessa política, foi criada a "Estratégia de Governança Digital (EGD) para o período de 2020 a 2023, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional." (Brasil, 2020a).

No setor público brasileiro, a EGD é uma ferramenta administrativa de planejamento e gestão, alinhada às orientações globais, que "apresenta diretrizes e orientações que devem ser seguidas pelos demais setores do governo federal do país, bem como pelos demais níveis da República" (Santos, 2021, p. 8).

Um dos objetivos definidos e previstos na EGD para o período de 2020 a 2023 foi a implementação da LGPD no âmbito do Governo Federal, tendo como uma das iniciativas o estabelecimento de método de adequação e conformidade dos órgãos com os requisitos da referida lei até 2020 (Brasil, 2020a), arraigado na organização e condução da gestão dos dados.

Sob a égide das normas de proteção de dados pessoais e da governança de dados, a Universidade Federal Rural de Pernambuco (UFRPE) regulamentou a divulgação e o acesso de documentos com dados pessoais de pessoa natural[1] no escopo dos processos administrativos eletrônicos da instituição, por meio da Resolução 031/2020, de 11 de agosto de 2020 (UFRPE, 2020a).

Cabe destacar que a implementação do meio eletrônico para a gestão dos processos administrativos na UFRPE ocorreu em abril de 2020, com a adoção do Sistema Integrado de Patrimônio, Administração e Contratos (SIPAC), um dos aplicativos disponíveis no Sistema Integrado de Gestão (SIG) da Universidade Federal do Rio Grande do Norte (UFRN). Desse modo, visualiza-se que a instituição não cumpriu o prazo estabelecido pelo Decreto nº 8.539, de 08 de outubro de 2015.

Diante do exposto, esta pesquisa teve como norte a seguinte questão-problema: *Como se apresenta a proteção de dados pessoais de pessoa natural, à luz da governança de dados, no âmbito dos processos administrativos eletrônicos SIPAC/UFRPE, instruídos e arquivados no período de abril de 2020 a dezembro de 2022?*

Esta dissertação encontra-se estruturada em cinco capítulos. O primeiro é composto pela Introdução, no qual foram realizadas a delimitação temática e uma breve contextualização sobre governança de dados, com destaque para as normas de implantação do processo administrativo eletrônico e as normas de proteção de dados pessoais no âmbito da gestão pública e UFRPE.

O segundo capítulo é composto pelo Referencial Teórico, no qual foi apresentada a revisão de literatura, com exposição das teorias referente ao problema de pesquisa, direcionado para a governança de dados e proteção de dados pessoais na administração pública federal.

[1] Conforme Código Civil, art. 2º e art. 6º, a personalidade civil da pessoa começa do nascimento com vida, e a existência da pessoa natural termina com a morte (Brasil, 2002).

No terceiro capítulo, foram apresentados os métodos adotados para conseguir atingir os objetivos definidos, incluindo os procedimentos realizados para a coleta, análise e interpretação dos dados.

No quarto capítulo, foram expostos os resultados e as discussões da pesquisa. Por seu turno, no último, foram expostas as considerações finais, incluindo-se as limitações do estudo e as propostas para futuras pesquisas.

1.1 OBJETIVOS

O objetivo geral desta pesquisa é analisar como se apresenta a proteção de dados pessoais de pessoa natural, a luz da governança de dados, no âmbito dos processos administrativos eletrônicos SIPAC/UFRPE, instruídos e arquivados no período de abril de 2020 a dezembro de 2022.

Os objetivos específicos são:

I. Analisar o cenário de adequação à proteção de dados pessoais das Universidades Públicas Federais do Nordeste, a fim de fazer um comparativo com a UFRPE, considerando as normas que regulamentam o tratamento de dados pessoais no âmbito dos processos administrativos eletrônicos;

II. Identificar as ações e investimentos na promoção da Proteção de Dados Pessoais no âmbito da Instituição;

III. Analisar a conformidade dos processos eletrônicos em relação às normas que regulamentam o tratamento de dados pessoais na UFRPE, instruídos e arquivados no período de abril de 2020 a dezembro de 2022;

IV. Propor ações complementares para subsidiar o tratamento das informações pessoais, no âmbito dos processos eletrônicos da UFRPE, com vistas a aprimorar a governança de dados e assegurar os direitos à privacidade e à proteção de dados pessoais e sensíveis.

1.2 JUSTIFICATIVA

Com a necessidade da adaptação para transformação digital dos órgãos e das entidades da administração pública federal, visando eficiência na oferta de políticas públicas e qualidade dos serviços prestados, foram editados e publicados os decretos nº 8.638/2016 e nº 10.332/2020, a fim de estabelecer as diretrizes da EGD (Brasil, 2020a).

No contexto da EGD, as instituições precisam adequar suas rotinas e sistemas, a fim de garantir as conformidades previstas na LGPD e promover gestão de privacidade e uso dos dados pessoais do cidadão, voltadas à promoção de uma boa governança de dados (Brasil, 2020a).

Entretanto, no tocante às universidades federais, Tenório Filho *et al*., (2021) destacam que há um grande desafio para efetivar essa adequação, que não é discricionária, uma vez que, caso não ocorra, poderão ser aplicadas sanções administrativas. Nesse cenário, a fim de atender as normas de proteção de dados pessoais no âmbito dos processos eletrônicos, a UFRPE publicou a Resolução nº 031/2020, que regulamenta a restrição à divulgação de documentos que contenham dados pessoais e sensíveis de pessoa natural no âmbito da instituição, em especial na utilização do SIPAC (UFRPE, 2020a).

Essa regulamentação interna vai ao encontro de Barbosa *et al.* (2021, p. 2120), que enfatizam a importância e dever das instituições públicas de ensino em adequarem os seus "processos e sistemas, tal como a mudança de cultura institucional de tratamento de dados pessoais", conforme previsão na LGPD.

Por sua vez, Leão *et al.* (2022) constataram, por meio de pesquisa bibliométrica, a baixa produção acadêmica nesta área, sugerindo estudos de governança de dados na administração pública associados a temas envolvendo a segurança da informação e proteção de dados pessoais, com vistas a subsidiar a gestão pública na promoção da conformidade das normas vigentes.

Nesse sentido, esta pesquisa tem relevância acadêmica e social, uma vez que pretende contribuir para o conhecimento na área da governança de dados na administração pública, no escopo da proteção de dados pessoais em processos administrativos eletrônicos, dentro de uma Instituição Federal de Ensino Superior (IFES).

Especificamente, esse estudo pretende analisar como se apresenta a proteção de dados pessoais, à luz da governança de dados, a partir das normas que regulamentam o tratamento de dados pessoais no âmbito da UFRPE, por meio da observação dos processos administrativos eletrônicos da instituição, instruídos e arquivados no período de 2020 a 2022, de posse da Seção de Arquivo e Registro Funcional da UFRPE (SARF).

Cabe ressaltar que o critério de acessibilidade foi adotado, uma vez que a pesquisadora é servidora da instituição, lotada na SARF, o que facilitou o acesso à informação. Salienta-se que compete à SARF o arquivamento dos processos relativos à vida funcional do servidor ativo, aposentado e instituidor de pensão e, em boa parte dos fluxogramas processuais, é o último setor que recebe esses processos.

Acredita-se que a análise dessas práticas poderá subsidiar não apenas a conformidade com as leis de proteção de dados, mas também fortalecer a segurança da informação e promover a transparência e a confiança nas operações administrativas. Além disso, ao destacar áreas de melhoria na gestão de dados pessoais, este estudo poderá auxiliar a implementação de medidas preventivas e corretivas, contribuindo para uma governança mais eficaz e responsável no uso de informações pessoais.

Consoante Gonçalves (2019, p. 142), a administração precisa primar pela transparência, tendo em vista que é o "principal mecanismo de controle dos dados pelos cidadãos" e, ao mesmo tempo, garantir a proteção de dados pessoais e sensíveis. Em seu estudo, a autora sugere que sejam realizadas investigações, a partir de 2020, quanto à efetividade na aplicação das normas orientadas à proteção de dados no setor público.

Portanto, observar as ações voltadas à proteção de dados nos processos eletrônicos e a forma como as práticas de governança digital estão sendo adotadas pela administração pública é importante como forma de garantir uma democracia participativa e o controle social.

2 REFERENCIAL TEÓRICO

Neste capítulo, serão apresentados o referencial teórico, com exposição de algumas teorias referente à governança pública, governança de dados e proteção de dados pessoais na administração pública, além do debate sobre processo eletrônico. Após essa contextualização, serão abordadas as normas de proteção de dados que regem o âmbito público.

2.1 GOVERNANÇA PÚBLICA

Numa dimensão ampliada, a "governança" consiste num conceito multifacetado, isto é, possui múltiplas interpretações e abrange diversos campos do conhecimento. A origem desta palavra remonta ao termo grego "governar" (κυβερνά/κυβερνώ), que tem o sentido de "dar direção para um destino" (Brasil, 2020b, p. 26). Desse modo, governança significa "dirigir a economia e a sociedade visando objetivos coletivos" (Peters, 2013, p. 29). A partir dessa raiz etimológica, o conceito fundamental encontra-se relacionado à direção ou liderança de aspectos da economia e da sociedade em direção a objetivos coletivos.

De acordo com Zorzal (2015, p. 70), o conceito de governança "é fraco no significado e forte na extensão", ou seja, a governança é caracterizada por sua falta de precisão intrínseca em relação ao significado, mas sua abrangência é notável. Segundo a autora, no sentido amplo, "refere-se à capacidade governativa ou, dizendo de outra forma, decorre da capacidade financeira e administrativa de o governo realizar políticas" (Zorzal, 2015, p. 75). Por sua vez, Matias-Pereira (2010) advoga que a governança pode ser entendida como a forma pela qual o poder é adquirido e distribuído entre os diferentes atores sociais.

No âmbito público, a governança é vista como uma importante ferramenta para melhorar a eficiência, a transparência e a responsabilidade na gestão dos recursos públicos, bem como para promover a participação da sociedade na tomada de decisões (Cavalieri, 2020a). Ao convergir com este posicionamento, o Tribunal de Contas da União (TCU) complementa que a governança pública teve origem na governança corporativa, abrangendo princípios, normas, diretrizes, procedimentos e ações para regulamentar a gestão desses recursos, visando também assegurar a eficácia e a integridade (Brasil, 2020b).

No Brasil, a importância da governança surgiu em resposta às demandas da sociedade por uma gestão mais eficiente, transparente e responsável dos recursos públicos. No final do século XX, ocorreram importantes mudanças na gestão pública brasileira, incluindo a reforma do Estado e a modernização da administração pública (Bresser-Pereira, 2010). Essas mudanças levaram à implementação de novas políticas e a práticas de governança que, ao longo dos anos,

foram evoluindo e se consolidando com a implementação de leis, regulamentos e mecanismos de controle.

Umas das normativas foi a Lei de Responsabilidade Fiscal (LRF), aprovada no ano de 2000, que estabeleceu normas de transparência e de controle na gestão pública, incluindo a obrigatoriedade de prestação de contas dos órgãos públicos e a definição de metas e indicadores para avaliação da gestão (Brasil, 2000).

Em 2013, com o objetivo de promover boas práticas de governança na gestão pública, o governo federal e o TCU reuniram esforços e desenvolveram um referencial básico sobre o tema, destinado a organizações públicas e outros entes jurisdicionados ao órgão de controle que, no ano de 2020, teve a publicação de sua terceira edição (Brasil, 2020b).

Outro divisor de águas foi o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional (Brasil, 2017). Segundo este decreto, governança pública consiste no "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade" (Brasil, 2017).

Esse conceito demonstra a complexidade e a abrangência das atividades envolvidas na governança pública, que não se limita apenas à gestão no sentido de função realizadora, mas engloba também aspectos estratégicos e o cumprimento das metas condicionais para a condução de políticas públicas.

Aqui, cabe enfatizar que "governança não é o mesmo que gestão" (Brasil, 2020b, p. 16). Em seu referencial, o TCU diferencia e apresenta a relação entre governança e gestão, conforme ilustrado na Figura 1. Nesse sentido, a governança está voltada para as atividades de avaliação, direcionamento e monitoramento, com foco na "qualidade do processo decisório e sua efetividade", ao passo que a gestão está relacionada ao planejamento, execução e controle das ações e processos para alcançar os resultados desejados, ou seja, "recebe o direcionamento superior e se preocupa com a qualidade da implementação desta direção, com eficácia e eficiência" (Brasil, 2020b, p. 17).

Figura 1 - Relação entre Governança e Gestão na visão do TCU

Fonte: Brasil (2020b, p.17).

Dessa forma, apesar de serem distintas, a governança e a gestão estão intimamente relacionadas, sendo interdependentes, complementares e essenciais para o desempenho eficaz de uma organização pública. A governança se concentra na direção estratégica e no acompanhamento do desempenho de uma organização; a gestão, por sua vez, é responsável por colocar em prática as estratégias definidas pela governança, e é responsável pelo uso eficiente dos recursos.

O principal objetivo da governança pública é aumentar as chances de fornecer resultados positivos para os cidadãos, tanto em termos de serviços públicos quanto de políticas públicas (Honorio, 2022). Assim, para garantir que as organizações atendam a essas demandas sociais de forma ética e eficaz, o Decreto 9.203/2017 estabelece seis princípios da governança pública (Brasil, 2017; Brasil, 2020b):

- **capacidade de resposta**: refere-se à agilidade e eficácia do setor público em atender às necessidades e demandas da sociedade;
- **integridade**: administração pública deve agir de forma ética e transparente evitando práticas com conflito de interesse, garantindo a confiança da sociedade;
- **confiabilidade**: relaciona-se com a consistência e a previsibilidade das ações da administração pública, garantindo a conformidade com as normas, leis e regulamentos;
- **melhoria regulatória**: visa simplificar e aprimorar as legislações e regulamentos governamentais, reduzindo burocracia e normas desnecessárias;
- **prestação de contas e responsabilidade**: refere-se ao dever da administração pública em prestar contas de suas ações e decisões, responsabilizando seus agentes por seus atos;

- **transparência**: disponibilizar informações de interesse público a todos, de forma compreensível e acessível. Promovendo a participação cidadã na tomada de decisões e fiscalização pública.

Magacho e Trento (2021) enfatizam a importância da governança na construção e na manutenção da confiança da sociedade nas instituições públicas. As autoras argumentam que a inobservância das práticas de governança pode conduzir à perda de confiança, o que, por sua vez, gera regras mais rígidas e custosas, alimentando um ciclo de disfunções burocráticas, desconformidade e desconfiança (Magacho; Trento, 2021).

Considerando a diversidade da aplicação da governança pública na prestação de serviços para sociedade e diante da importância crescente dos dados na era digital, emerge a necessidade de explorar o modelo de governança de dados, que consiste na preocupação com a melhor organização e integração dos dados e metadados das instituições (Barbieri, 2019). Na próxima seção, será abordada a discussão sobre esse tema, analisando suas implicações e desafios para as organizações.

2.1.1 Governança de dados na administração pública brasileira

Para tratar de governança de dados, inicialmente, faz-se necessário contextualizar os conceitos de dados, informação e conhecimento.

Quando se refere ao conceito de dados, Barbieri (2019) o define como um conjunto de informações brutas que representa fatos numéricos, alfabéticos ou alfanuméricos que podem ser registrados e armazenados em um sistema, e utilizados como base para a construção de informações.

Para o autor, a informação é constituída “dando ao dado certo entorno ou contexto”, nesse sentido, um dado seria uma estrutura elementar da cadeia informacional, e a informação seria a semântica e contextualização dos dados para geração de fatos (Barbieri, 2019, p. 15).

Desse modo, a informação é o resultado do processamento e interpretação dos dados, tornando-os significativos e úteis para o tomador de decisão. Bioni (2019, p. 11) destaca que a “informação em si não é o que alavanca eficiência na atividade empresarial, mas o seu processamento-organização a ser transformado em conhecimento aplicado.”

Barbieri define conhecimento como:

> o ato de entender as coisas (a informação, por exemplo) por meio da razão ou do experimento ou experiência. Ele exige as sinapses cerebrais para ajuntar outros ingredientes. O conhecimento nos diria que "uma temperatura corporal de 38°C significa febre" e que antitérmico deve ser ministrado. Ou seja, expandimos a informação em direção a (ou pela agregação de) conhecimento (2019, p. 15).

Em outras palavras, a informação é a transformação dos dados em algo significativo e útil. Ou seja, enquanto dados são simples representações numéricas ou alfanuméricas, a informação tem contexto e significado, oferecendo percepções e conhecimento ao usuário.

De acordo com Bioni (2019), a informação deve ser convertida em conhecimento, a fim de torná-la produtiva e estratégica para a atividade empresarial. Já Tapscott e Williams (2006) argumentam que a informação é uma das principais fontes de valor na economia atual e que a capacidade de criar, compartilhar e utilizar informação é a chave para o sucesso na sociedade digital.

Barbieri (2019) ressalta que, atingido o nível do conhecimento, há um quarto patamar, que é a sabedoria. O autor define a sabedoria como "uma espécie de experiência acumulada no tempo, revista e com certos contornos de vivência e empirismo, associados com percepções e pontos de vista populares" (Barbieri, 2019, p. 15). Ou seja, no exemplo supracitado, da temperatura corporal de 38ºC, apresentado pelo autor, a sabedoria poderia indicar que, caso o antitérmico não funcione, um banho frio poderia ser aplicado para ajudar no controle da febre (Barbieri, 2019).

Assim, é possível perceber o dado como um "elemento atômico" que "precisa de contexto (metadados) para começar a agir e produzir informação", que pode ser convertida em conhecimento e, com maturidade e experiência, atinge o ápice da sabedoria (Barbieri, 2019, p. 15). O autor ainda destaca que, os termos dado e informação são "normalmente usados de forma intercambiada no tratamento desse ativo" (Barbieri, 2019, p. 15), o que será considerado neste estudo.

Nesse contexto, a governança pública atual tem como componente diferenciador a informação (Faleiros Júnior, 2021). Com isso, a governança de dados se torna cada vez mais relevante no âmbito das organizações.

Conforme apresentado por Barbieri, a governança de dados é:

> um termo produzido na esteira dos jargões que brotaram a partir do termo raiz "governança". Extraída do contexto maior da governança corporativa e tangenciando pontos da Governança de TI, a de dados foca em princípios de organização e controle sobre esses insumos essenciais para a produção de informação e conhecimento das empresas (2019, p. 35).

Logo, a governança de dados pode ser entendida como um processo organizacional para garantir a proteção de dados de uma instituição. Cavalieri (2020a) aponta que, em relação à proteção de dados pessoais, a governança de dados, estabelece regras com base na natureza e finalidade do tratamento de dados, bem como na análise dos riscos e benefícios associados.

Na administração pública federal do Brasil, o Decreto nº 8.638, de 15 de janeiro de 2016, instituiu a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional (Brasil, 2016). Esse decreto foi posteriormente revogado pelo Decreto nº 10.332, de 28 de abril de 2020, (alterado pelo Decreto nº 10.996, de 14 de março de 2022, e Decreto 11.260, de 22 de novembro de 2022) que instituiu a Estratégia de Governo Digital (EGD) para o período de 2020 a 2023, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências (Brasil, 2020a).

Cabe salientar que o Governo Federal, visando estimular a cultura do Governo Digital, prorrogou o período de vigência da EGD de 2020 a 2022 para 2020 a 2023, por meio do Decreto 11.260, de 22 de novembro de 2022 (Brasil, 2022c). Essa prorrogação indica um compromisso em fortalecer o Governo Digital como uma política de Estado e assegurar sua continuidade, possivelmente para garantir a eficácia das iniciativas digitais governamentais e promover uma transformação mais ampla na administração pública. Destaca-se que a EGD, para o período de 2024 a 2027, ainda está em construção, com previsão de publicação e vigência a partir de março de 2024 (Brasil, 2024a).

Na visão de Rodrigues e Cammarosano (2022), a introdução da governança digital na administração pública não se limita à adoção de novas tecnologias, mas também implica na incorporação de um novo conceito de gestão pública, adaptado para atender às demandas emergentes da sociedade contemporânea.

A EGD para o quadriênio 2020-2023, apresentada pelo mencionado Decreto nº 10.332, está fundamentada em princípios, objetivos e iniciativas que têm como finalidade guiar a transformação da Gestão Pública por meio das tecnologias digitais. Essa transformação visa promover a evolução das políticas e serviços públicos, com o intuito de oferecer serviços de alta qualidade e atender às expectativas da sociedade e, consoante Brasil (2020a), contribuir para um governo mais:

- **Centrado no Cidadão**: direciona seus esforços para oferecer uma experiência mais positiva e satisfatória aos cidadãos ao interagirem com os serviços públicos;

- **Integrado**: busca proporcionar uma experiência de atendimento mais eficaz e conveniente para o cidadão, ao mesmo tempo em que otimiza recursos e processos administrativos por meio da integração de dados e serviços entre os diversos entes federativos;
- **Inteligente**: utiliza dados e evidências para tomar decisões informadas, antecipar e atender às necessidades da sociedade de forma eficaz, e promover um ambiente propício para o crescimento econômico e o investimento;
- **Confiável**: busca equilibrar a inovação e a eficiência proporcionadas pelas tecnologias digitais com a proteção dos direitos e da privacidade dos cidadãos, assegurando uma abordagem responsável e ética no uso dessas tecnologias no âmbito do Estado;
- **Transparente e aberto**: reconhece a importância da transparência como um princípio fundamental da governança democrática, e se esforça para promover a participação cidadã e o controle social por meio da disponibilização eficiente dos dados e informações públicas;
- **Eficiente**: busca maximizar o uso de seus recursos e adotar tecnologias e práticas que permitam oferecer serviços públicos de qualidade de forma econômica e sustentável.

Nesse sentido, ao analisar a governança de dados, verifica-se uma correlação com a expectativa de ser um governo confiável, conforme norteado pela EGD 2020-2023. A confiabilidade de um governo envolve não apenas a prestação de serviços eficientes e transparentes, mas também o respeito à privacidade e à segurança dos dados dos cidadãos (Brasil, 2020a).

A normativa da EGD 2020-2023, apresenta 18 (dezoito) objetivos a serem alcançados, conforme Quadro 1:

Quadro 1 - Objetivos que norteiam a EGD 2020-2023

OBJETIVO	DESCRIÇÃO
Objetivo 1	Oferta de serviços públicos digitais
Objetivo 2	Avaliação de satisfação nos serviços digitais
Objetivo 3	Canais e serviços digitais simples e intuitivos
Objetivo 4	Acesso digital único aos serviços públicos
Objetivo 5	Plataformas e ferramentas compartilhadas
Objetivo 6	Serviços públicos integrados

OBJETIVO	DESCRIÇÃO
Objetivo 7	Políticas públicas baseadas em dados e evidências
Objetivo 8	Serviços públicos do futuro e tecnologias emergentes
Objetivo 9	Serviços preditivos e personalizados ao cidadão
Objetivo 10	Implementação da LGPD no âmbito do Governo Federal
Objetivo 11	Garantia da segurança das plataformas de governo digital e de missão crítica
Objetivo 12	Identidade digital ao cidadão
Objetivo 13	Reformulação dos canais de transparência e dados abertos
Objetivo 14	Participação do cidadão na elaboração de políticas públicas
Objetivo 15	Governo como plataforma para novos negócios
Objetivo 16	Otimização das infraestruturas de tecnologia da informação
Objetivo 17	O digital como fonte de recursos para políticas públicas essenciais
Objetivo 18	Equipes de governo com competências digitais

Fonte: adaptado do Decreto nº 10.332/2020 (Brasil, 2020a).

A EGD 2020-2023 visa modernizar a administração pública, tornando-a mais eficiente, transparente e acessível para os cidadãos, por meio da adoção de tecnologias e processos digitais. Essa estratégia inclui a disponibilização de serviços *online*, a centralização e integração de diferentes áreas da gestão pública, e a abertura de canais de participação cidadã (Brasil, 2020a). Rodrigues e Cammarosano (2022) enfatizam que essa modernização dos serviços públicos impulsiona uma mudança profunda, buscando desenvolver novos modelos de serviço que aproveitem ao máximo as capacidades da tecnologia.

Nesse contexto, no que tange à proteção de dados pessoais, o Objetivo 10 da EGD 2020-2023 tem como direcionamento a implementação da LGPD no âmbito do Governo Federal, conforme iniciativas apresentadas no Quadro 2:

Quadro 2 - Iniciativas do Objetivo 10 da EGD 2020-2023

INICIATIVA	DESCRIÇÃO
Iniciativa 10.1.	Estabelecer método de adequação e conformidade dos órgãos com os requisitos da Lei Geral de Proteção de Dados, até 2020.
Iniciativa 10.2.	Estabelecer plataforma de gestão da privacidade e uso dos dados pessoais do cidadão, até 2020.

Fonte: adaptado do Decreto nº 10.332/2020 (Brasil, 2020a).

Dessa forma, é essencial que a administração pública atue em conformidade com as leis e normas aplicáveis para uma boa governança de dados, com implementação de um "Programa de Governança em Privacidade" ou "Programa de *Compliance* Digital" previsto na LGPD (Brasil, 2018).

A adoção de boas práticas de *compliance*, como a implementação de controles internos e a adoção de medidas de prevenção à corrupção, contribui para a garantia da integridade e da legalidade nos serviços públicos (Cavalieri, 2020a).

Frazão (2007, p. 42) define *compliance* como "conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou," nos casos em que já tiverem ocorrido, "propiciar o imediato retorno ao contexto de normalidade e legalidade".

O termo *compliance* pode entendido como conformidade, adequação, obediência e deve ser visto não só como um compromisso social dos envolvidos, mas também como ferramenta pedagógica, influenciando a adoção de valores de ética e de integridade, visando à moralidade administrativa e à excelência no serviço público (Cavalieri, 2020b).

Nesse sentido, o *compliance* não consiste apenas em assegurar a conformidade legal e observância às normas, mas abrange também valores éticos e a busca pela prevenção de ato ilícito no âmbito da organização (Miranda, 2017), além de promover a cultura para o ambiente e aumentar o compromisso dos agentes econômicos (Magacho e Trento, 2021).

Nesse contexto, Frazão, Oliva e Abilio (2019) advogam que a implementação de mecanismos de *compliance* é fundamental para promover comportamentos que estejam de acordo com a legislação, agindo como uma ferramenta importante tanto para as atividades operacionais quanto de forma preventiva.

Para Magacho e Trento (2021), uma das vantagens dos programas de *compliance* é a promoção da gestão adequada dos riscos e a prevenção de práticas ilegais, que permitem a identificação rápida de descumprimentos e a correção de possíveis danos, incentivando uma cultura de conformidade com as normas legais e internas da organização. Ressalta-se que a gestão de riscos é um dos elementos fundamentais para implementação de um programa de *compliance*, e a sua não execução pode refletir na inefetividade do programa de conformidade (Frazão; Oliva; Abilio, 2019).

Em relação aos elementos para um programa de *compliance* eficaz, Frazão, Oliva e Abilio (2019) destacam dez pontos essenciais que compõem a estruturação efetiva desses programas. Primeiramente, ressaltam a importância da avaliação contínua de riscos e a necessidade de atualização constante do programa para garantir sua eficácia. Em seguida, enfatizam a elaboração de códigos de ética e conduta, a fim de publicizar as condutas aceitáveis e vedadas na entidade. Além disso, sinalizam a relevância de uma organização compatível com os riscos da atividade, o comprometimento da alta administração e a autonomia do setor de

compliance. As autoras também realçam a necessidade de treinamentos periódicos para os funcionários e a criação de uma cultura corporativa que promova o respeito à ética e às leis.

Outros pontos cruciais incluem o monitoramento constante dos controles e processos, a existência de canais seguros de comunicação de infrações e a detecção, apuração e punição adequadas de condutas contrárias ao programa. Esses elementos, quando implementados de forma integrada, contribuem para fortalecer a conformidade e a ética dentro da organização.

No escopo da proteção de dados pessoais, Frazão, Oliva e Abilio (2019) apontam três fatores que fortalecem o papel dos mecanismos de *compliance* na proteção de dados pessoais, especialmente no contexto da LGPD, a seguir:

1. **Amplo escopo de aplicação da LGPD**: abrange não apenas atividades diretamente relacionadas à coleta e tratamento de dados, mas também as atividades mais simples da organização;
2. **Caráter transversal**: essa natureza transversal do *compliance* demanda a revisão dos padrões de conduta estabelecidos para o cumprimento de outras normas, uma vez que o *compliance* de dados exige adaptações em todas as unidades de uma organização;
3. **Tornar efetivas as disposições da lei**: o terceiro fator destacado é a necessidade de conferir concretude a certos preceitos da LGPD, dada a significativa margem interpretativa de muitos comandos legais. Visa à adoção de comportamentos alinhados com a lei, a fim de evitar interpretações que possam comprometer a proteção dos dados pessoais.

Nesse sentido, depreende-se que o cumprimento eficaz da LGPD requer uma interpretação precisa da lei e uma abordagem abrangente, envolvendo adaptações em todas as áreas da organização, não apenas aquelas diretamente relacionadas à coleta e ao tratamento de dados.

Logo, a importância de uma governança sólida no tratamento de dados pessoais é destacada diante da ampla aplicação da LGPD, da transversalidade do *compliance* de dados e da necessidade de interpretação precisa da lei. Uma estrutura organizacional robusta, adaptável e abrangente é essencial para garantir a conformidade efetiva com a legislação e melhoria na prestação dos serviços.

2.2 PROTEÇÃO DE DADOS NA GESTÃO PÚBLICA

Com o advento da era digital, as organizações passaram a enxergar a informação como um bem valioso. No caso das privadas, o valor encontra-se atrelado ao âmbito econômico, ao passo que, nas instituições públicas, a informação aprimora a elaboração de políticas, visando à prestação de serviços com maior qualidade à sociedade. Em ambas, exige-se uma postura estratégica que garanta não apenas a privacidade, mas também a segurança dos dados, em uma sociedade cada vez mais conectada e interdependente.

Castells e Cardoso (2005) defendem uma reforma no setor público para promover o desenvolvimento da sociedade em rede, incluindo a implementação de sistemas de *e*-governança e a adaptação à era digital. Por seu turno, Bioni (2019) enfatiza que os indivíduos vivem numa sociedade na qual as interações e transações dependem de dados identificadores dos cidadãos, e que essas atividades têm uma grande influência na vida das pessoas.

Doneda (2016) destaca a influência direta da tecnologia e das mudanças sociais no contexto atual em que a informação pessoal e a privacidade operam. O autor enfatiza que a tecnologia intensificou os fluxos de informação, alterando os equilíbrios de poder na sociedade, o que refletiu numa nova estrutura de poder, ligada à arquitetura informacional contemporânea (Doneda, 2016).

Essa mudança para a nova economia, voltada a dados, trouxe consigo a necessidade de se repensar a proteção dessas informações, que passaram a ser vistas como prioritárias, o que tem suscitado reflexões sobre a importância de proteger esses dados e assegurar que sejam tratados com respeito aos direitos e interesses das pessoas envolvidas (Bioni, 2019).

Dessa forma, muitos países se viram obrigados a criar legislações que regulamentassem o tratamento, a disponibilidade, a acessibilidade e o uso dos dados pessoais e das informações (Almeida; Soares, 2022).

A União Europeia (UE), por exemplo, tem uma longa história de proteção de dados pessoais. O direito à privacidade foi assegurado pela Convenção Europeia dos Direitos do Homem de 1950, que preconiza que toda pessoa tem direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência (União Europeia, 1950).

A partir desta premissa, a UE tem trabalhado para garantir a proteção desse direito por meio de leis específicas, tendo aprovado, em 1995, a Diretiva de Proteção de Dados, que estabeleceu uma estrutura básica de proteção de dados pessoais em toda a UE (Barbieri, 2019).

Em 2016, a UE criou a *General Data Protection Regulation*[2] (GDPR), que estabeleceu um novo marco regulatório para a proteção de dados pessoais em toda a UE. O GDPR estabelece, entre outros, uma série de requisitos para as organizações que processam dados pessoais, incluindo a necessidade de obter o consentimento do titular dos dados, o direito dos titulares dos dados de consentir, corrigir e excluir seus dados, a obrigação das organizações de notificar as autoridades em caso de violação de dados pessoais e a possibilidade de aplicar sanções para as organizações que não cumprem as normas (EU-GDPR, 2016).

Nesse aspecto, a GDPR evidencia a responsabilidade como cerne da proteção e da privacidade dos dados, enfatizando a governança de dados como aspecto primordial. Ainda, conforme salientado por Silva (2021), a GDPR exige que os encarregados do gerenciamento e tratamento de dados demonstrem, tanto aos órgãos fiscais quanto aos proprietários das informações, a aderência aos princípios protetivos.

No Brasil, a legislação de proteção de dados pessoais evoluiu em um ritmo mais lento e começou a progredir na década de 1990, com o surgimento da Internet e a ampliação da coleta de dados pessoais por parte de empresas e governos. Em 1996, foi criada a Lei n° 9.296, que tratava sobre o sigilo e interceptação das comunicações, mas não especificamente sobre dados pessoais (Brasil, 1996).

Em 2010, iniciaram as primeiras discussões, com consulta pública do Ministério da Justiça, sobre proteção de dados pessoais. Em 2011, foi aprovada a Lei de Acesso à Informação (LAI), com o propósito de regulamentar o acesso a informações públicas aplicáveis aos três Poderes da União, Estados, Distrito Federal e Municípios (Brasil, 2011).

A LAI foi uma das primeiras leis a tratar de forma específica sobre a proteção de informação pessoal, especialmente no que diz respeito ao acesso à informação pública e à privacidade dos dados pessoais. A referida lei considera informação pessoal como "aquela relacionada à pessoa natural identificada ou identificável" (Brasil, 2011). Ressalta-se que a LAI estabelece a transparência como regra para a administração pública, e tornou-se fundamental para promover a prestação de contas, a participação cidadã e a integridade institucional, sendo o sigilo a exceção, reservado para casos estritamente necessários, como questões de segurança nacional ou privacidade pessoal (Brasil, 2011).

Em 2014, a Lei nº 12.965, conhecida como Marco Civil da Internet, estabeleceu regras sobre o uso da Internet e proteção de dados pessoais no Brasil, abordando, dentre outros temas, a privacidade e a retenção de dados (Brasil, 2014).

[2] Em tradução literal, quer dizer Regulamento Geral sobre a Proteção de Dados (RGPD).

Em 2018, foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD) n° 13.709, de 14 de agosto de 2018, que regulamentou o uso de dados pessoais pelo setor público e organizações privadas e instituiu o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) (Brasil, 2018). Vale destacar que essa lei teve sua vigência parcial em 2020, com previsão de aplicação de sanções apenas em 2021.

Nesse sentido, a LGPD tem o diferencial de ser a primeira legislação específica voltada para proteção de dados pessoais. Bioni (2019, p. 108) destaca que, no país, antes da publicação da LGPD, só havia leis setoriais de proteção de dados, numa espécie de ““colcha de retalhos” que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regulamento”.

A LGPD tem por objetivo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018) e dispõe sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, por pessoa natural (física) ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais (Brasil, 2020c). Crespo (2021) enfatiza que essa norma visa à conscientização das instituições na formulação de programas de boa governança de dados, a fim de protegê-los.

Por sua vez, Bioni (2019, p. 108) destaca que “historicamente, normas de proteção de dados pessoais sempre tiveram a dupla função de não só garantir a privacidade e outros direitos fundamentais, mas também fomentar o desenvolvimento econômico”.

A LGPD é composta por dez capítulos, no qual se destaca o capítulo IV, voltado para o tratamento de dados pessoais pelo poder público, considerado um grande avanço na administração pública brasileira, com desafio de estabelecer um equilíbrio entre a proteção de dados dos cidadãos e o tratamento desses dados para a elaboração e execução de políticas públicas (Crespo, 2021).

Para Magacho e Trento (2021), essa inclusão pode ser considerada como um marco histórico, uma vez que resultará em ações efetivas para mitigar o uso indevido dos dados coletados nos serviços públicos, anteriormente nunca apurada por uma lei tão detalhada e de alto nível.

A referida lei tem como objetivo fornecer orientações para que as organizações assumam a responsabilidade pela segurança dos dados pessoais, proibindo o uso desses dados para fins diferentes sem o consentimento do usuário (Lima; Presser, 2022).

Bioni (2019) argumenta que os dados, quando ligados à esfera de uma pessoa, podem ser considerados parte dos direitos da personalidade. Para que isso ocorra, os dados devem ser

qualificados como pessoais, ou seja, devem refletir “uma projeção, extensão ou dimensão do seu titular” (Bioni, 2019, p. 65).

O art. 5º da LGPD estabeleceu dados pessoais em duas categorias: **dado pessoal**, como a “informação relacionada a pessoa natural identificada ou identificável”, mantendo a definição apresentada pela LAI; e **dado pessoal sensível**, como o “dado pessoal sobre origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou à organização de caráter religioso, filosófico ou político; dado referente à saúde ou à vida sexual; e dado genérico ou biométrico, quando vinculado a uma pessoa natural” (Brasil, 2018).

Bione (2019, p. 68), destaca que essa estrutura normativa reflete a dualidade intrínseca ao conceituar dados pessoais, uma vez que “há uma bipartição do seu léxico que ora retrai (reducionista), ora expande (expansionista)”. Em outras palavras, uma informação é considerada um dado pessoal se houver a possibilidade de identificação direta ou indireta de uma pessoa natural.

O termo "identificada" refere-se a uma pessoa natural que pode ser claramente identificada por meio dos dados em questão, seja de forma direta (reducionista) ou em conjunto com outras informações disponíveis, como por exemplo o nome completo, cadastro de pessoa física (CPF) ou registro geral (RG) (Bione, 2019). Por outro lado, o termo "identificável" diz respeito a uma pessoa natural que pode ser identificada, ainda que de forma indireta (expansionista), a partir da combinação com outras informações, como por exemplo o endereço e placa de carro (Bione, 2019).

Barbosa *et al*. (2021, p. 2119), apontam que, ao contrário da LAI, a LGPD estende a proteção para todos os dados pessoais, não apenas aos dados sensíveis ou relacionados aos direitos de personalidade, mas também a todas “as legislações existentes, inclusive os regimes efetivos de transparência e acesso à informação”. Essa ampliação do escopo de proteção proporcionada pela LGPD reflete uma mudança significativa na abordagem legal em relação à privacidade e à proteção de dados pessoais.

Na seara da publicidade de informações pessoais de agentes públicos, a Advocacia-Geral da União (AGU) recomenda o uso do número de matrícula incluído no Sistema Integrado de Administração de Recursos Humanos (SIAPE) como substituto do número do CPF em documentos e contratos relacionados a atividades da administração pública federal, uma vez que é suficiente para identificar o servidor público responsável pelo ato, reduzindo a possibilidade de confusão com homônimos e prevenindo o uso indevido do CPF por terceiros (Brasil, 2021b).

A AGU argumenta que, embora o número SIAPE seja considerado um dado pessoal, ele não possui implicações além da esfera pública do servidor, o que significa que não há razões para restringir seu acesso:

> O número SIAPE diz respeito à matrícula que identifica o servidor público no órgão em que desempenha suas atividades, e, embora se enquadre na definição de dado pessoal, à luz da LGPD, não possui repercussões para além da vida pública do servidor, não havendo razões para que esse dado tenha restrição de acesso (Brasil, 2021b).

No que tange ao efetivo tratamento de dados pessoais, a LGPD determina que, além da boa-fé, deverão ser observados outros princípios norteadores (Brasil, 2018), apresentados no Quadro 3, disposto a seguir.

Quadro 3 - Princípios norteadores da LGPD para tratamento de dados pessoais

PRINCÍPIO	DESCRIÇÃO
I. Finalidade	realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
II. Adequação	compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
III. Necessidade	limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
IV. Livre acesso	garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
V. Qualidade dos dados	garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
VI. Transparência	garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
VII. Segurança	utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
VIII. Prevenção	adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
IX - Não discriminação	impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
X - Responsabilização e prestação de contas	demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Fonte: adaptado da LGPD (Brasil, 2018).

Esses princípios formam a base da LGPD e orientam o tratamento responsável e ético dos dados pessoais no Brasil. Nascimento e Silva (2023, p. 13) destacam que todos eles são essenciais para nortear boas práticas para a devida proteção e o tratamento dos dados pessoais. Nesse sentido, é fundamental que as organizações estejam cientes desses princípios e implementem medidas adequadas para garantir sua conformidade, promovendo, assim, a tutela efetiva dos direitos dos titulares de dados.

Conforme definido pela LGPD, o tratamento de dados pessoais compreende todas as atividades realizadas com dados pessoais que envolvem a "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).

É importante acrescentar que a noção de tratamento de dados que a LGPD utiliza é ampla e, com isso, praticamente, todos os agentes econômicos estão envolvidos nas atividades de tratamento de dados e sujeitos aos riscos. Por isso, para Frazão, Oliva e Abilio (2019, p. 688) ressaltam que "o tipo e a intensidade do tratamento de dados, bem como os riscos a ele inerentes, podem variar consideravelmente entre os agentes econômicos, a exigirem uma atenta e individualizada análise".

No escopo da administração pública, a lei estabelece que o tratamento de dados pessoais pelas pessoas jurídicas de direito público, empresa pública e sociedade de economia mista deve ser realizado em conformidade com os princípios e diretrizes estabelecidos pela referida lei (Brasil, 2018).

Nesse contexto, Tenório Filho *et al.* (2021, p. 9) enfatizam que "todas as Universidades Federais devem adequar-se ao estabelecido na LGPD. Essa adequação é de suma importância para garantir a proteção dos direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo". Esses autores ainda acrescentam que "diante dessa realidade, a mudança cultural das instituições de ensino e seus colaboradores é um dos grandes desafios, visto que transições culturais demandam tempo e investimentos em divulgação e treinamento" (Tenório Filho *et al.,* 2021, p. 9). Logo, não basta que a instituição pareça adequada à LGPD, mas é essencial a integração desse dispositivo protetivo a todas as ações e decisões realizadas pelos agentes ativos da instituição (Lugati; Almeida, 2022).

Cabe destacar que a LGPD representa um marco regulatório significativo no Brasil, estabelecendo padrões claros e abrangentes para o tratamento de dados pessoais, a ponto de se estruturar uma agência reguladora própria, a Autoridade Nacional de Proteção de Dados (ANPD) (Frazão; Oliva; Abilio, 2019).

Originalmente, esse órgão integrava a estrutura da Presidência da República. Porém, por meio da Lei 14.460, de 25 de outubro de 2022, foi transformada em uma autarquia de natureza especial, “sendo dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal” (Brasil, 2022b), cuja competência é zelar, elaborar diretrizes, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional (Brasil, 2019).

É importante destacar que em 27 de fevereiro de 2023 foi publicado o regulamento de dosimetria e aplicação de sanções administrativa pela ANPD, através da Resolução nº 4, de 24 de fevereiro de 2023, permitindo uma maior rebusques na fiscalização realizada por essa autarquia (Brasil, 2023a). Essa dosimetria consiste no “método que orienta a escolha da sanção mais apropriada para cada caso concreto em que houver violação à LGPD e permite calcular, quando cabível, o valor da multa aplicável ao infrator” (Brasil, 2023b).

Outros conceitos importantes apresentados na LGPD referem-se aos termos “titular”, “controlador”, “operador”, “encarregado” e “agentes de tratamento”. Para a referida lei, o titular é “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. Por sua vez, o controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (Brasil, 2018). No âmbito das universidades de ensino superior, o controlador é representado pela própria instituição, geralmente por meio de sua administração central ou órgão responsável pela gestão institucional.

Já o operador é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” e o encarregado é a “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD” (Brasil, 2018).

Assim, considerando toda a abrangência das atividades de tratamento de dados e que este compõe-se de atividades rotineiras da administração, entende-se que a gestão pública deve promover mudança cultural e engajamento dos principais agentes para que alcance efetividade na implementação da LGPD, a fim de garantir que o tratamento de dados pessoais pelo poder público seja realizado de forma ética, transparente e respeitando os direitos fundamentais dos cidadãos.

2.2.1 Proteção de Dados Pessoais nos Processos Eletrônicos na Administração Pública Federal

Com o avanço tecnológico e o estabelecimento de espaços públicos virtuais, a atuação da Administração Pública no meio eletrônico tornou-se crucial, introduzindo novas diretrizes para os processos administrativos, antes predominantemente físicos (Rodrigues; Cammarosano, 2022).

Na administração pública federal, o processo administrativo é regulado pela Lei 9.784, de 29 de janeiro de 1999, que "estabelece normas básicas sobre o processo administrativo no âmbito da Administração Federal direta e indireta, visando, em especial, à proteção dos direitos dos administrados e ao melhor cumprimento dos fins da Administração" (Brasil, 1999).

A partir dos avanços tecnológicos e da necessidade de modernização dos procedimentos administrativos, houve uma crescente demanda pela implementação do processo eletrônico. Essa migração para o meio digital foi impulsionada pela busca por maior eficiência, celeridade e economia de recursos, além de proporcionar uma maior acessibilidade e transparência na relação entre administração pública e cidadãos.

No contexto da governança eletrônica, o Decreto nº 8.539, de 08 de outubro de 2015, formalizou e padronizou a utilização do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, estabelecendo diretrizes para sua implantação e funcionamento, visando à promoção da eficiência, transparência e celeridades nos processos administrativos (Brasil, 2015).

Salienta-se que o prazo de implementação do uso do meio eletrônico para a realização de processo administrativo foi de dois anos, contados da data de publicação do decreto, e para os órgãos e entidades que já utilizavam o sistema de processo eletrônico o prazo foi de 03 anos, a fim de promover a adaptação aos termos do referido decreto (Brasil, 2015).

Di Pietro (2016) destaca que "os atos praticados por meio eletrônico devem observar os mesmos requisitos de validade dos atos administrativos em geral, bem como os princípios a que se submete a Administração Pública" (Di Pietro, 2016, p. 772).

Para Pereira (2022) um dos ganhos na implantação dos processos eletrônicos foi a descentralização da abertura de processo – antes atividade exclusiva das unidades de protocolo – para todas as demais unidades administrativas da instituição, possibilitando maior autonomia para os servidores. A autora destaca que "a rotina operacional de manuseio documental", antes do processo eletrônico, era onerosa ao serviço público e com "fácil possibilidade de haver

extravio de documentos", o que já não se vislumbra no processo eletrônico, que permite maior transparência e gestão de documentos (Pereira, 2022, p. 34).

Quanto ao acesso à integra do processo, o referido decreto disciplina que a "vista pessoal do interessado pode ocorrer por intermédio da disponibilização de sistema informatizado de gestão [...] ou por acesso à cópia do documento, preferencialmente, em meio eletrônico", e determina que a "classificação da informação quanto ao grau de sigilo e a possibilidade de limitação do acesso aos servidores autorizados e aos interessados no processo" devem observar os termo da LAI e demais normas vigentes (Brasil, 2015).

Ainda com o objetivo de orientar os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional acerca da transparência de documentos e processos administrativos eletrônicos tramitados nos sistemas de processo eletrônico utilizados em cada instituição, a Secretaria de Gestão do Ministério da Economia (SEGES/ME) e a Secretaria de Transparência e Combate à Corrupção da Controladoria Geral da União (STPC/CGU) publicaram a Orientação Conjunta nº 1/2021/ME/CGU intitulada "Transparência no Processo Administrativo Eletrônico" (Brasil, 2021a).

Essa orientação reforça as diretrizes para a divulgação de informações de interesse público nos sistemas de processo administrativo eletrônico, com foco na transparência ativa, e estabelece critérios para a restrição de acesso a informações, garantindo o sigilo legal e a proteção de dados pessoais (Brasil, 2021a).

A referida orientação conjunta exemplifica as principais aplicações práticas dos níveis de acesso de informação pública e restrita, a serem utilizadas nos sistemas de processo eletrônico das instituições, conforme apresentado no Quadro 4:

Quadro 4 - Níveis de Acesso à Informação em Processo Administrativo Eletrônico

Nível de Acesso	Tipo de Informação	Quem pode acessar	Exemplos de Documentos
Público	De interesse público, geral ou coletivo	• Todas as pessoas	Informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados; Dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades

Nível de Acesso	Tipo de Informação	Quem pode acessar	Exemplos de Documentos
Público	Documento Preparatório utilizado como fundamento de tomada de decisão ou de ato administrativo	• Agentes públicos legalmente autorizados • Interessado, mediante identificação	Notas técnicas, pareceres, notas informativas ou outros documentos que subsidiem decisões dos dirigentes em documentos sobre políticas econômica, fiscal, tributária, monetária, regulatória etc. Documentos que tragam argumentos e conteúdo para os processos que culminarão na edição de ato normativo;
Restrito	Informações pessoais, relacionadas a uma determinada pessoa identificada ou identificável	• Agentes públicos legalmente autorizados • Própria pessoa a quem a informação se referir, mediante identificação	Documentos que contenham dados pessoais e dados pessoais sensíveis, como: • RG, CPF • Estado de saúde do servidor ou familiares • Informações financeiras, patrimoniais; • Alimentandos • Dependentes • Pensões • Endereços, número de telefone, *e-mail* • Origem racial ou étnica • Orientação sexual • Convicções religiosas, filosóficas ou morais • Opiniões políticas • Filiação sindical, partidária, a organizações de caráter religioso, filosófico ou político.
Restrito	Informações protegidas por legislação específica como sigilo fiscal, bancário, comercial, empresarial e contábil.	• Agentes públicos legalmente autorizados • Interessado, mediante identificação	Ofícios, extratos, relatórios, atas, dentre outros, que contenham informações fiscais, bancárias, comerciais, empresariais ou contábeis protegidas por sigilo.

Fonte: adaptado da Orientação Conjunta nº 1/2021/ME/CGU (Brasil, 202a).

Caetano (2023) enfatiza que a disciplina durante a etapa de classificação do nível de acesso aos processos e documentos, no meio eletrônico, é imprescindível para garantir que a informação seja tratada de forma correta, sem prejudicar os cidadãos ou a administração pública no acesso à informação, quando solicitado pelo órgão competente.

Destaca-se que o nível de acesso à informação está diretamente ligado à natureza do assunto do documento, que pode ser ostensivo ou sigiloso (Paes, 2004). Os documentos classificados como ostensivos têm natureza pública e podem ser divulgados, sem prejuízo à administração, ao passo que os documentos sigilosos devem ser de conhecimento restrito (Paes, 2004).

Cabe ressaltar que os sistemas de processo eletrônico disponibilizam um módulo de consulta pública, possibilitando que indivíduos externos ao órgão acessem e monitorem os processos, incluindo o fluxo processual (trâmites) e o teor das informações neles contidas, promovendo a transparência ativa dos atos administrativos. Nesse sentido, o cadastro correto na natureza dos documentos e processos eletrônicos é condição essencial para seja dada publicidade às informações públicas, resguardando, por outro lado, informações restritas, sigilosas ou de caráter pessoal" (Brasil, 2021a).

Lima (2022, p. 72) enfatiza a importância do nível de compreensão da LAI e LGPD por parte dos agentes operadores do sistema de processo eletrônico quanto ao cadastro da natureza dos documentos e processos digitais, uma vez que a falta de conhecimento dessas normas pode gerar "a criação de processos em desacordo com os normativos que garantem a transparência da informação e o direito de proteção e dados pessoais". Ainda, "o bom funcionamento do módulo" está diretamente "ligado à preparação da equipe que opera o sistema" (Brasil, 2021a).

Nesse sentido, é fundamental que a administração pública invista na capacitação e preparação dos seus agentes, com vistas a assegurar o correto cadastramento dos documentos e processos eletrônicos, contribuindo para a transparência e a proteção dos dados.

3 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo, serão apresentados os procedimentos metodológicos norteadores para o desenvolvimento desta pesquisa, incluindo sua classificação, o tipo de abordagem e o objetivo, bem como as técnicas que foram utilizadas para a coleta, análise e interpretação dos dados.

3.1 CLASSIFICAÇÃO DA PESQUISA

Quanto à abordagem, trata-se de uma pesquisa qualitativa, tendo em vista que, conforme Creswell (2007), os estudos qualitativos se concentram em compreender o significado social de fenômenos complexos. Corroborando tal definição, Martins e Theóphilo (2007, p. 137) utilizam a expressão "avaliação qualitativa", destacando que os tipos de informações, dados e evidências obtidos não deveriam ser mensurados de forma quantitativa, o que atesta uma correlação com os objetivos deste trabalho científico.

Como método investigativo, tipifica-se como uma pesquisa diagnóstico e documental. Nesse contexto, foi verificado o estado atual de um fenômeno ou situação, com vistas a fornecer informações baseadas em evidências (Martins; Theóphilo, 2007). Para Martins e Theóphilo (2007), esse tipo de pesquisa é importante no contexto de mudança organizacional, pois permite que esta última seja implementada eficazmente, atendendo às necessidades de uma organização.

Sendo assim, essa estratégia revelou-se apropriada para descrever o contexto atual de como a proteção de dados pessoais, à luz da governança de dados, se apresenta no escopo dos processos administrativos eletrônicos no âmbito da UFRPE, permitindo identificar de maneira sistemática e abrangente possíveis lacunas na conformidade em relação às regulamentações de proteção de dados pessoais, bem como possíveis causas subjacentes dessas deficiências. Some-se a isto que, ao observar os processos administrativos eletrônicos e as políticas de privacidade existentes, este trabalho poderá apontar áreas específicas que requerem uma maior atenção da gestão, para fomentar treinamentos, revisão de procedimentos ou adoção de novas tecnologias.

Outrossim, esta é uma pesquisa documental. Na visão de Gil (2017, p. 35), essa tipologia "vale-se de toda sorte de documentos, elaborados com finalidades diversas", a exemplo dos "documentos institucionais, mantidos em arquivos de empresas, órgãos públicos e outras organizações". Nesse sentido, a pesquisadora debruçou-se sobre as normas legais federais e institucionais correlacionadas à proteção de dados pessoais, para subsidiar a investigação do problema deste estudo.

Quanto aos objetivos, esta pesquisa classifica-se como descritiva, uma vez que analisou a aplicabilidade da proteção de dados nos processos eletrônicos SIPAC/UFRPE, instruídos e arquivados no período de abril de 2020 a dezembro de 2022, a partir do arcabouço normativo que regulamenta o tratamento de dados pessoais. Gil (2017, p. 33) destaca que "as pesquisas descritivas têm como objetivo a descrição das características de determinada população ou fenômeno". Nesse sentido, este trabalho caracterizou a proteção de dados, à luz da governança de dados, no escopo dos processos eletrônicos de uma universidade federal.

Quanto à finalidade, a pesquisa caracteriza-se como aplicada, uma vez que pretendeu obter "conhecimento com vistas à aplicação numa determinada situação" (Gil, 2017, p. 33). Para Barros e Lehfeld (2007), esse conhecimento gerado subsidiará a resolução mais ou menos imediata de problemas que, porventura, possam existir em uma determinação organização.

3.2 COLETA, TRATAMENTO E ANÁLISE DE DADOS

A estrutura da coleta e análise dos dados foi dividida em três etapas, disposta a seguir.

3.2.1 Etapa 1 – Questionário com Universidades Federais

A primeira etapa consistiu no envio de um questionário estruturado às universidades públicas federais da Região Nordeste do Brasil, por meio da ferramenta Fala.BR. Esta plataforma integra a Ouvidoria e o Acesso à Informação do Poder Executivo Federal, possibilitando o envio de denúncias, elogios, reclamações, sugestões e solicitações aos órgãos e entidades. A escolha deste recorte, universidades federais do Nordeste, encontra-se relacionada ao objetivo do programa de pós-graduação, que corresponde à capacitação de gestores no âmbito da Administração Pública da região.

Quanto à escolha desta ferramenta de consulta, o Fala.Br constitui-se como canal oficial e padronizado para solicitação de informações junto aos órgãos públicos, assegurando um tratamento formal e reconhecido legalmente, aumentando a probabilidade do recebimento de uma resposta adequada e dentro dos prazos estabelecidos pela LAI, que são de até 20 dias, nos casos de impossibildiade de envio imeniato, prorrogáveis por mais 10 dias, mediante justificativa expressa (Brasil, 2011), o que permitiu um melhor planejamento da pesquisa.

Além disso, a equipe responsável pelo recebimento das demandas nessa plataforma direciona os questionamentos ao setor competente e responsável pela informação consultada, o que garante uma maior precisão e assertividade na resposta. Outro fator importante é que a ferramenta oferece a possibilidade de recurso, junto à Controladoria-Geral da União (CGU), em caso de ausência ou resposta insatisfatória por parte das instituições.

O questionário foi estruturado com questões 17 objetivas (Apêndice A), categorizadas em cinco sessões, conforme Quadro 5, disposto abaixo.

Quadro 5 - Seções do questionário para consulta junto às universidades via Fala.BR

ITEM	SEÇÃO	CONTEÚDO/OBJETIVO
1	Quanto ao Sistema de Processo Administrativo Eletrônico	Identificação da implementação do sistema de processo eletrônico adotado por cada instituição.
2	Quanto às permissões dos usuários e à natureza do assunto no sistema de processo eletrônico	Identificar se as permissões dos usuários no sistema de processo eletrônico são adequadas para o tratamento de dados pessoais.
3	Quanto à governança	Identificar os aspectos de governança referente à proteção de dados pessoais na instituição.
4	Quanto à proteção de dados pessoais	Identificar os aspectos de normatização interna quanto à proteção de dados pessoais no escopo dos processos administrativos.
5	Quanto à capacitação dos servidores	Identificar a promoção na capacitação dos servidores referente à proteção de dados pessoais no escopo dos processos administrativos.

Fonte: Elaborado pela autora (2024).

Além de permitir a identificação do cenário de adequação à proteção de dados pessoais no âmbito dos processos administrativos eletrônicos, a disponibilização deste instrumento de coleta de dados possibilitou um *benchmark,* ou seja, um comparativo da UFRPE em relação às demais universidades, atendendo ao primeiro objetivo específico estabelecido.

Martins e Theóphilo (2007) pontuam que o questionário é um dos instrumentos mais utilizados em pesquisas sociais. Antes de ser submetido às instituições, foi realizado um teste piloto para validá-lo com três servidores da própria UFRPE, que trabalham diariamente com os processos administrativos eletrônicos e detêm conhecimento sobre as normas de proteção de dados institucionais.

De acordo com Creswell (2007, p. 166), esse pré-teste "é importante para estabelecer a validade de conteúdo de um instrumento e para melhorar questões, formato e escalas". Nesta fase, foram identificados alguns problemas com o questionário, como questões em duplicidade, com respostas inadequadas e algumas que não eram relevantes para o objetivo do estudo.

Após retificação das inconsistências, o instrumento foi enviado às 20 instituições listadas no Quadro 6, que responderam às indagações no período de 21/08/2023 a 29/09/2023,

por meio da plataforma Fala.BR, conforme explicitado, incluindo a própria instituição *lócus* da pesquisa, o que enriqueceu a dimensão interpretativa do estudo.

Quadro 6 - Relação das Universidades Federais Públicas do Nordeste

ITEM	ESTADO	UNIVERSIDADE
1	Alagoas	Universidade Federal de Alagoas
2	Bahia	Universidade Federal da Bahia
3	Bahia	Universidade Federal do Sul da Bahia
4	Bahia	Universidade Federal do Recôncavo da Bahia
5	Bahia	Universidade Federal do Oeste da Bahia
6	Ceará	Universidade da Integração Internacional da Lusofonia Afro-Brasileira
7	Ceará	Universidade Federal do Cariri
8	Ceará	Universidade Federal do Ceará
9	Maranhão	Fundação Universidade Federal do Maranhão
10	Paraíba	Universidade Federal da Paraíba
11	Paraíba	Universidade Federal de Campina Grande
12	Pernambuco	Universidade Federal de Pernambuco
13	Pernambuco	Universidade Federal do Vale do São Francisco
14	Pernambuco	Universidade Federal do Agreste de Pernambuco
15	Pernambuco	Universidade Federal Rural de Pernambuco
16	Piaui	Fundação Universidade Federal do Piauí
17	Piaui	Universidade Federal do Delta do Parnaíba
18	Rio Grande do Norte	Universidade Federal do Rio Grande do Norte
19	Rio Grande do Norte	Universidade Federal Rural do Semi-Árido
20	Sergipe	Universidade Federal de Sergipe

Fonte: Elaborado pela autora (2024).

Após a coleta, os dados foram organizados e tabulados em uma planilha do *Microsoft Excel*, e as frequências de cada pergunta foram calculadas. A fim de facilitar a visualização dos dados e representar as principais tendências e padrões observados, foram elaborados gráficos, que serão apresentados no capítulo sobre os resultados.

3.2.2 Etapa 2 - Pesquisa Documental

A segunda etapa consistiu na pesquisa documental no âmbito da legislação, voltada para a análise da documentação referente às diretrizes e às legislações federais e institucionais sobre governança de dados, proteção de dados pessoais e processo administrativo eletrônico, adotadas pela UFRPE, a fim de atender ao segundo objetivo específico.

O Quadro 7, disposto a seguir, apresenta os documentos consultados na pesquisa.

Quadro 7 - Documentos consultados na pesquisa

DOCUMENTO	ELEMENTO DE ANÁLISE	ANO
Plano de Desenvolvimento Institucional (PDI) da UFRPE Vigência 2013-2020 (revisado em 2018)	Identificar ações para implementação do processo eletrônico atendendo determinação do Decreto 8.539/2015.	2018
Resolução Nº 031/2020-CONSU/UFRPE	Identificar os procedimentos de restrição à divulgação de dados pessoais no âmbito da UFRPE.	2020
Cartilha LGPD da UFRPE	Identificar os procedimentos para a coleta, armazenamento, processamento e compartilhamento de dados pessoais no âmbito da instituição.	2021
Plano de Desenvolvimento Institucional (PDI) da UFRPE Vigência 2021-2030	Analisar as diretrizes, os objetivos e as metas estabelecidos pela UFRPE para assegurar a proteção de dados pessoais no âmbito da instituição.	2021
Resolução Nº 103/2021-CONSU/UFRPE	Identificar os princípios e requisitos para o tratamento de dados pessoais – Política de Privacidade.	2021
Relatório de Gestão da UFRPE - Exercício de 2020	Identificar os resultados da implementação do SIPAC na UFRPE.	2021
Relatório de Gestão da UFRPE - Exercício de 2021	Identificar as ações e investimento de proteção de dados.	2022
Relatório de Gestão da UFRPE - Exercício de 2022	Identificar as ações e investimento de proteção de dados.	2023
Relatório de Gestão da PROGEPE - Exercício de 2023	Identificar as ações e investimento de proteção de dados.	2024

Fonte: Elaborado pela autora (2023).

3.2.3 Etapa 3 - Levantamento dos processos SIPAC

Com o objetivo de analisar a conformidade em relação às normas de proteção de dados pessoais nos processos administrativos eletrônicos, instruídos no período de abril de 2020 a dezembro de 2022, arquivados na SARF e, portanto, atender ao terceiro objetivo específico, foi necessária a escolha de uma tipologia de processo.

Cabe ressaltar, que o critério de acessibilidade foi adotado, uma vez que a pesquisadora é servidora da instituição, lotada na SARF, o que facilitou o acesso à informação. Conforme já mencionado, a SARF é a seção responsável pelo arquivamento dos processos relativos à vida funcional dos servidores.

Desse modo, por conveniência, foram analisados os processos de concessão de pensão civil, tendo em vista a necessidade de inclusão de vários documentos pessoais do beneficiário, público externo da UFRPE, listados no Quadro 8. Todos esses documentos são enviados pelo beneficiário, via *e-mail*, ao Protocolo da instituição, a quem compete a abertura do processo administrativo.

Quadro 8 - Documentos necessários para abertura de processo de pensão civil

ITEM	DOCUMENTAÇÃO NECESSÁRIA
1	Formulário de Requerimento de Pensão
2	Certidão de Óbito
3	CPF do servidor e do solicitante Identidade
4	(RG) do servidor e do solicitante
5	Título de eleitor
6	Certidão de casamento atualizada (para cônjuge)
7	Certidão de nascimento ou de casamento atualizada com averbação do divórcio ou declaração de união estável (para companheiro)
8	Certidão de nascimento (para filhos menores ou maiores com invalidez)
9	Último contracheque
10	Comprovante de endereço
11	Cartão ou contrato do banco de conta corrente e conta salário em nome do solicitante
12	Outros documentos que se façam necessários (comprovação de tutela ou curatela, designação de dependentes, laudo médico no caso de beneficiário inválido ou deficiente, comprovação de dependência econômica e comprovante judicial de percepção de pensão alimentícia).

Fonte: Elaborado pela autora (2024), a partir dos dados disponíveis no site da PROGEPE/UFRPE.

Cabe frisar que este estudo se encontra voltado à observação de documentos constantes em processos administrativos eletrônicos de natureza ostensiva, dada a possibilidade de erro, incluindo-se como "público" algum documento que deveria ser tipificado como "restrito". Além disso, os processos de natureza restrita não foram objeto de análise, tendo em vista que, após a classificação neste nível, os documentos serão cadastrados automaticamente com esta natureza.

No período de abril de 2020 a dezembro de 2022, foram instruídos 79 processos eletrônicos de concessão de pensão civil, os quais foram posteriormente arquivados na SARF. Considerando o quantitativo relativamente pequeno, não houve a necessidade da mensuração do tamanho da amostra a ser analisada, tendo em vista que foi viável a análise de todos os processos encontrados. Neste universo, não foram incluídos os processos protocolados no ano de 2023, uma vez que a análise iniciou no mês de abril do referido ano.

Nesse contexto, a fim de assegurar o cumprimento do terceiro objetivo específico, foram estabelecidos os seguintes parâmetros para análise da conformidade da documentação que compõem os processos, adaptado dos estudos de Lima (2022) e Caetano (2023), Quadro 9:

Quadro 9 - Parâmetros para análise da conformidade das documentações

ITEM	DOCUMENTAÇÃO NECESSÁRIA
1	Quantidade dos processos e documentos observados
2	A conformidade quanto à natureza dos documentos dos processos
3	Documento de interesse público cadastrado com natureza de documento "restrito"
4	Documento com informações pessoais cadastrado com natureza de documento "ostensivo"
5	Titular ("público externo" ou "público interno" – este último abrangendo o operador do processo)
6	Tipo da informação com ocorrência (pública ou pessoal);
7	Forma de apresentação do dado (apenas o dado ou o documento integralmente digitalizado);

Fonte: adaptado dos estudos de Lima (2022) e Caetano (2023)

Os dados coletados por meio da análise dos processos administrativos eletrônicos foram organizados e tabulados em uma planilha do *Microsoft Excel*. A partir desses dados, procedeu-se à elaboração de gráficos e tabelas, a fim de observar a conformidade dos processos com a normas de proteção de dados pessoais. Após análise, foi possível identificar os aspectos em que os processos eletrônicos se encontram em desconformidade com as normativas vigentes, bem como os aspectos que necessitam ser aperfeiçoados, corroborando a dimensão diagnóstica deste trabalho.

3.3 ELABORAÇÃO DAS PROPOSTAS DE AÇÕES COMPLEMENTARES

A partir desse percurso metodológico, estruturado em três etapas, e com base no referencial teórico e resultados da pesquisa, foi possível propor ações complementares para subsidiar o tratamento de informações pessoais, no âmbito dos processos eletrônicos da UFRPE, a fim de aprimorar a governança de dados e assegurar os direitos à privacidade e à proteção de dados pessoais e sensíveis, atendendo ao último objetivo específico deste estudo.

3.4 ASPECTOS ÉTICOS

Os processos administrativos eletrônicos observados nessa pesquisa são públicos e estão disponíveis para consulta, ficando o estudo delimitado ao contexto de observação de dados.

Além disso, os dados observados e coletados foram analisados de forma agregada, sem identificação dos participantes e exposição de dados pessoais dos interessados. Dessa forma, a pesquisa apresentou um rigor técnico e científico, minimizando eventuais riscos e garantindo que os aspectos relativos à privacidade e à segurança de dados fossem devidamente respeitados.

Outro item que cabe pontuar é que foi elaborado um relatório, contendo as não conformidades, cuja regularização iniciou antes da publicação desta pesquisa, corroborando a dimensão prática deste estudo, o que converge com as expectativas de um mestrado de cunho profissional.

No próximo capítulo, serão analisados e discutidos os resultados obtidos no estudo, à luz do referencial teórico constante no segundo capítulo desta dissertação.

4 RESULTADOS E DISCUSSÕES

Neste capítulo, serão apresentados os resultados obtidos, por meio do levantamento junto às Universidades Federais do Nordeste e da análise documental. Por questões didáticas, optou-se por apresentá-los separadamente, a fim de permitir análises com maior refinamento. Em seguida, foi realizado um comparativo entre a IFES investigada e as demais instituições. Posteriormente foram apresentados os resultados referentes à conformidade dos processos administrativos eletrônicos e observações complementares.

4.1 CENÁRIO DOS PROCESSOS ADMINISTRATIVOS ELETRÔNICOS E DA PROTEÇÃO DE DADOS PESSOAIS NA UNIVERSIDADES FEDERAIS DA REGIÃO NORDESTE DO BRASIL

A fim de atender ao primeiro objetivo específico, procedeu-se a um diagnóstico junto às universidades federais da Região Nordeste. Na próxima subseção, será apresentado o contexto da proteção de dados nessas entidades, a partir dos resultados obtidos por meio de questionário.

4.1.1 Processo Administrativo Eletrônico no escopo das Universidades Federais do Nordeste

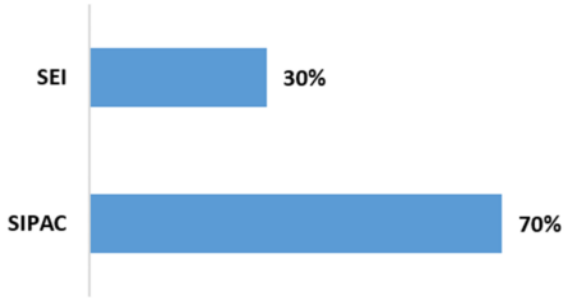
Todas as 20 Universidades Federais do Nordeste consultadas (listadas no Quadro 6) responderam o questionário, que tinha por objetivo permitir uma melhor compreensão do panorama atual dos sistemas eletrônicos adotados para tramitação de processos, a fim de subsidiar uma análise da proteção de dados pessoais no âmbito desses órgãos.

Portanto, visando obter a participação integral dessas instituições na pesquisa, a consulta via Fala.Br foi considerada como o método mais adequado para a coleta de dados junto às universidades, proporcionando um ambiente legalmente amparado, com prazos definidos, possibilidade de recurso e supervisão por parte da CGU, garantindo a transparência e o acesso à informação de caráter público.

Na **Seção 1**, verificou-se a adoção de sistema eletrônico para tramitação dos processos administrativos, a pesquisa revelou que todas as 20 universidades consultadas já utilizam o processo administrativo eletrônico para tramitação dos processos administrativos, conforme previsto no Decreto 8.539/2015, indicando que as universidades estão tomando medidas para modernização e melhoria da eficiência e transparência da gestão pública. Dentre as ferramentas

utilizadas, constatou-se que o SIPAC é o sistema mais utilizado, com adesão de 70% (14) dentre as instituições consultadas. conforme apresentado no Gráfico 1:

Gráfico 1 - Sistema eletrônico adotado pelas Universidade do Nordeste para tramitação dos processos administrativos



Fonte: Dados da pesquisa (2024).

Cabe destacar que o Governo Federal adotou o Sistema Eletrônico de Informações[3] (SEI) como solução oficial para gestão dos processos administrativos eletrônicos e que, atualmente, o Ministério da Gestão e da Inovação em Serviços Públicos (MGI) é o "responsável pelo desenvolvimento colaborativo e pela cessão do direito de uso do SEI, seus módulos e sistemas complementares e suporte, com exclusividade para os órgãos do Poder Executivo Federal", após cooperação com o Tribunal Regional Federal da 4ª Região (TRF-4), promovida pelo Acordo de Cooperação Técnica nº 458/2023 (Brasil, 2024b).

Em se tratando do SIPAC, este é uma ferramenta disponível no Sistema Integrado de Gestão (SIG) criado pela Universidade Federal do Rio Grande do Norte (UFRN). Ao contrário do SEI, requer o pagamento de licença para sua aquisição e uso por parte das instituições. O SIG da UFRN é composto por um conjunto de sistemas para gestão adminstrativa, acadêmica e de recursos humanos, e inclui, além do SIPAC, o Sistema Integrado de Gestão de Atividades Acadêmica (SIGAA), utilizado para registro e controle de atividades relacionadas aos alunos e cursos, bem como o Sistema Integrado de Gestão de Recursos Humanos (SIGRH), voltado para a administração dos recursos humanos da instituição.

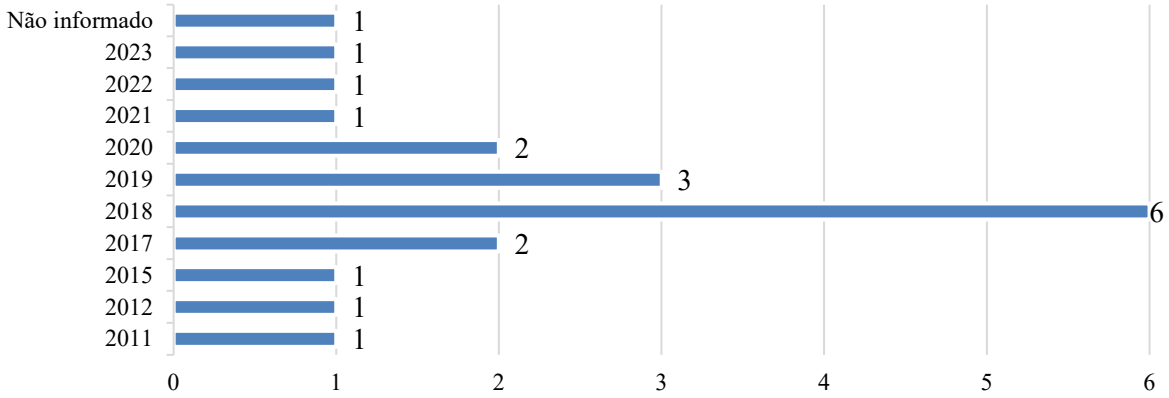
Nesse sentido, pode-se inferir que, embora o SEI seja gratuito e regulado pelo governo federal, a possibilidade de acesso a um conjunto de sistemas integrados, como o SIPAC, SIGRH

[3] Este sistema foi desenvolvido pelo TRF-4, e é disponibilizado gratuitamente para as instituições públicas desde o ano de 2013, com o propósito de aprimorar a eficiência na administração pública (Saraiva, 2018).

e SIGAA, pode ter sido considerada mais eficiente pelas universidades, pois facilita a gestão e o compartilhamento de informações entre diferentes áreas da instituição.

Com base no Gráfico 2, constata-se que 65% (13) das universidades federais do Nordeste[4] implantaram o sistema de processo eletrônico após o ano de 2017. Ressalta-se que, conforme o Decreto 8.539/2015, "o uso do meio eletrônico para a realização de processo administrativo deverá estar implementado no prazo de dois anos, contado da data de publicação deste Decreto", isto é, o prazo expirou em outubro de 2017 (Brasil, 2015). Nesse contexto, resta evidente que boa parte das entidades enfrentaram desafios para assegurar o cumprimento da normativa, já que a adoção de novas ferramentas tecnológicas demanda um planejamento institucional.

Gráfico 2 - Ano de implementação do sistema eletrônico adotado pelas Universidades Federais do Nordeste



Fonte: Dados da pesquisa (2024).

Vale destacar que o Tribunal de Contas da União (TCU), ao analisar o não cumprimento dessa exigência, recomendou a necessidade de "determinar diretamente às instituições que, caso ainda não tenham iniciado a implantação do processo eletrônico (possuam somente processo físico), adotem medidas para garantir tal implementação" (Brasil, 2021c). Para subsidiar esse projeto, o próprio órgão sugeriu que as instituições deveriam elaborar um plano de ação, destacando a prescindibilidade na aplicação de sanções devido ao não cumprimento do prazo (Brasil, 2021c).

4 A Universidade Federal do Agreste de Pernambuco (UFAPE) não foi considerada nessa questão, uma vez que só foi criada no ano de 2018, a partir da Lei Federal nº 13.651, de 11 de abril de 2018, após o desmembramento da UFRPE.

As universidades foram consultadas quanto à customização do sistema para atender necessidades particulares da instituição, tais como regimento interno e rotinas administrativas. Neste caso, 55% (11) declararam que não realizaram adaptações no sistema, provavelmente porque as ferramentas adquiridas já se encontravam alinhadas às legislações em vigor. Vale destacar que, dessas 11 que não realizaram customização, 07 adotaram o sistema SIPAC e 04 o sistema SEI.

Outrossim, essas 04 universidades que adquiriram o SEI não visualizaram necessidade de customização, tendo em vista que, à epoca da implantação pelo Ministério do Planejamento, a Agência Nacional de Telecomunicações (Anatel) elaborou uma série de customizações, criando uma base para o Poder Executivo Federal, já que o sistema foi desenvolvido a partir das características de tramitação de processos do Judiciário (Saraiva, 2018).

Na **Seção 2**, que trata das permissões dos usuários e da natureza do assunto no sistema de processo eletrônico, verificou-se que 60% (12) das universidades descentralizaram a abertura dos processos eletrônicos para todos os servidores ativos da instituição, deixando de centralizar essa atividade para os agentes lotados nas unidades de protocolo. Para Pereira (2022, p. 34), essa descentralização facilita "o fluxo das comunicações entre os setores da universidade". Nesse contexto, visualiza-se como aspectos positivos a autonomia do interessado, celeridade na abertura do processo e atendimento mais célere ao público externo por parte das unidades de protocolo. Em contrapartida, pode-se citar como elementos negativos a possibilidade de abertura de processo em duplicidade e erro na tipologia, classificação e fluxo processual.

No tocante à restrição de acesso a informações pessoais, todas as IFES sinalizaram que há recursos para indicar a natureza do documento[5] e processo, tipificando-os como ostensivo, restrito ou sigiloso. Ademais, 85% (17) delas informaram que, para cadastro de documentos restritos ou sigilosos, é necessário incluir uma justificativa. Salienta-se que a regra é a transparência ativa, conforme a Lei de Acesso à Informação, razão pela qual a restrição deve ser justificada, sob alegação de proteção de dados pessoais.

Quanto à possibilidade de correção em situações de erro na indicação da natureza do documento, ao todo 16 universidades (80%) sinalizaram que têm essa funcionalidade, inclusive aquelas que centralizaram a abertura de processo nas unidades de protocolo. Esse recurso é extremamente importante, pois permite ao usuário a correção de divulgação de dados pessoais de forma indevida. Ressalta-se que 25% (5) das universidades limitaram essa permissão aos usuários com função de chefia no setor de origem do documento. Essa limitação fragiliza o

[5] Neste estudo, as expressões "natureza do documento" e "nível de acesso" serão utilizadas como sinônimas, ao referirem-se à classificação quanto à divulgação da informação (público/ostensivo e restrito).

andamento do processo eletrônico, uma vez que todo servidor tem autonomia instituída por lei em relação aos seus atos e também responsabilidade por eles.

Quando o recurso de corrigir é difundido para todos os usuários, independente do setor ou chefia, possibilita sanar eventual ocorrência de violação à transparência pública e à proteção de dados pessoais, além de fortalecer o senso de responsabilidade dos servidores no geral. Consoante Frazão, Oliva e Abilio (2019, p. 684) "os programas de *compliance* relacionam-se à fixação de controles internos que, em reforço à regulação estatal, auxiliem os agentes econômicos a se manterem em conformidade com a lei (e, de forma mais ampla, também com suas políticas corporativas)".

A **Seção 3** tratou sobre os aspectos da governança, com foco em proteção de dados pessoais. A pesquisa revelou que apenas 55% (11) das instituições apontaram que a adequação dos serviços à LGPD está prevista no Plano de Desenvolvimento Institucional (PDI), o que atesta uma fragilidade no planejamento estratégico no tocante à proteção de dados pessoais em relação à normativa supracitada. Essa ausência conduz à inferência que essa adequação ainda não foi estabelecida como uma política institucional, o que pode comprometer a definição de objetivos estratégicos, indicadores e metas relativas a esse tema.

Ademais, ainda que as instituições tenham se adequado ao cenário de proteção de dados pessoais, é imperativo que haja um acompanhamento contínuo, a fim de fortalecer a cultura da instituição. Nascimento e Silva (2023, p. 19) esclarecem que a "atuação da instituição enquanto controladora e responsável pelo tratamento e segurança dos dados pessoais requer da sua gestão a realização de um trabalho conjunto, integrado e participativo que envolva todos os setores que a compõem e seus respectivos representantes". As autoras discorrem ainda que, neste trabalho, é "possível proceder a realização de uma discussão institucional, que busque o planejamento e o estabelecimento de processos e de fluxos de trabalho, para o efetivo tratamento dos dados pessoais, conforme preconiza a LGPD."

Quanto ao comitê responsável pela implantação da LGPD, 75% das Universidades pontuaram que há uma unidade responsável pela implantação da referida lei, reconhecendo a importância para as boas práticas de governança na instituição. Barbosa *et al.* (2021, p. 2120) reforçam que a designação desse comitê é de grande relevância, uma vez que essa comissão é responsável por "gerir todo o processo de adequação, partindo, a *priori*, do mapeamento dos processos e sistemas que operam e armazenam os dados pessoais e/ou dados pessoais sensíveis", viabilizando a adoção de um melhor direcionamento na adequação.

Quanto à designação de encarregado pelo tratamento de dados pessoais, 90% dos órgãos responderam que há uma portaria de designação, o que é positivo, pois indica que as IFES estão cumprindo as determinações da LGPD.

Na **Seção 4**, foram observados aos aspectos de normatização interna referentes à proteção de dados pessoais no escopo dos processos eletrônicos. A pesquisa revelou que apenas metade das universidades (50%) responderam que existe algum instrumento institucional que regulamenta a proteção desses dados no âmbito do sistema de processo eletrônico da instituição. Lima e Presser (2022, p. 117), reforçam que, para viabilizar uma boa gestão de dados dentro das organizações, é necessário, entre outros, o "desenvolvimento de políticas de gestão de dados interna", a fim de "inibir a sua violação ou uso indevido por agentes internos ou externos à organização não autorizados".

Quanto aos incidentes de exposição e vazamento de dados pessoais provenientes de documentos eletrônicos publicados em processos eletrônicos na instituição, 55% (11) responderam que não há instrumento norteador institucional para registro desses incidentes. A ausência desse tipo de instrumento pode dificultar a identificação e a investigação de incidentes de segurança, aumentando o risco de danos aos titulares de dados pessoais e dificultando o mapeamento dos principais gargalos e, por conseguinte, a definição de ações para otimização do sistema e dos procedimentos.

A maioria das universidades (55%) respondeu que realizou a adequação de documentos internos, como requerimento padrão e formulários internos, para atender de forma mais eficaz aos princípios da LGPD. Para assegurar essa conformidade, especificamente, aos princípios da adequação e necessidade, é imprescindível que as instituições revisem e adequem seus formulários, a fim de garantir que apenas os dados estritamente necessários sejam solicitados, assegurando, assim, a proteção dos dados pessoais e o cumprimento das obrigações legais.

Na **Seção 5**, foram abordados aspectos referentes à promoção de capacitação dos servidores. A pesquisa revelou que 60% (12) das universidades realizaram capacitação dos servidores sobre proteção de dados pessoais e 65% (13) das instituições promoveram palestras e outras ações voltadas à divulgação da proteção de dados pessoais e sensíveis. Lima e Presser (2022, p. 117), ressaltam "que as organizações são compostas por diversos profissionais que trabalham direta ou indiretamente com dados", e reforçam que esses diversos profissionais "devem receber algum tipo de capacitação sobre a importância dos dados e a necessidade de protegê-los de indivíduos não autorizados a manuseá-los". Ainda sob o olhar desses autores, "essa educação dos profissionais significa também uma preocupação em tornar os agentes que

trabalham com dados e informações organizacionais competentes em informação.” (Lima; Presser, 2022, p. 117).

Na próxima seção, será exposto como se apresenta o sistema de processo eletrônico no escopo da UFRPE, visando uma melhor compreensão da implementação do SIPAC para a gestão de documentos. A abordagem será fundamentada nos resultados obtidos por meio da etapa de pesquisa documental.

4.1.2 Processo Administrativo Eletrônico no escopo da UFRPE

A UFRPE, instituição pública de ensino superior, no estado de Pernambuco, em atendimento ao disposto no Decreto 8.539/2015, e impulsionada pela pandemia decorrente da covid-19, implantou o processo administrativo eletrônico em abril de 2020, não só como forma de promover celeridade das instruções processuais, transparência e economicidade, mas também para garantir a continuidade das atividades administrativas da instituição no período de isolamento social (UFRPE, 2020b).

O sistema adotado pela instituição para gestão dos processos eletrônicos foi o Sistema Integrado de Patrimônio, Administração e Contratos (SIPAC) – Módulo Protocolo, um dos sistemas disponíveis no Sistema Integrado de Gestão (SIG) da Universidade Federal do Rio Grande do Norte (UFRN).

O SIPAC “é um sistema integrado de gestão, ou *Enterpise Resource Flanning* (ERP), que visa agregar todos os processos de trabalho de uma instituição para fins de maior controle e efetividade nas rotinas administrativas do usuário” (Pereira, 2022). Ou seja, é um sistema que controla e informatiza os fluxos da área administrativa por meio de módulos (subsistemas) voltados ao orçamento, almoxarifado, patrimônio, fluxo documental e processual, bem como às licitações, dentre outras funcionalidades.

O Módulo Protocolo do SIPAC tem por objetivo “auxiliar a gestão documental na instituição, abrangendo o controle de processos, documentos e memorandos eletrônicos com informações de registro, conteúdo, tramitações e despachos” (UFRPE, 2022).

Vale salientar que foi constatada uma divergência no marco temporal para formalização deste sistema, uma vez que, no portal da instituição, há uma incompatibilidade entre as datas relativas à sua disponibilização, constando os meses de março e abril do ano de 2020, o que evidencia a falta de clareza e uniformidade com a comunidade universitária.

Além da fragilidade na divulgação desse dado, a pesquisa documental não identificou uma resolução específica ou norma regulamentadora que indique o marco legal e discipline o uso do sistema no âmbito da instituição investigada, conforme previsto no Decreto 8.539/2015, que preconiza que "os órgãos ou as entidades deverão estabelecer políticas, estratégias e ações que garantam a preservação de longo prazo, o acesso e o uso contínuo dos documentos digitais" (Brasil, 2015).

Para o TCU (Brasil, 2021, p. 16), a ausência total ou parcial de norma regulamentadora "dos procedimentos relacionados ao processo eletrônico pode resultar na existência de processos e documentos não padronizados, na gestão documental ineficiente, em falhas quanto à segurança ou legibilidade da informação".

Nesse sentido, com a ausência de um instrumento normativo, não fica evidenciada de forma intuitiva, o marco legal da implementação do sistema, os setores responsáveis pela gestão dos módulos funcionais do sistema, pela gestão de documentos, pelas políticas, procedimentos, restrições e práticas específicas, pelos esclarecimentos de dúvidas (central de dúvidas), pela padronização dos documentos, dentre outros. Além desses pontos, a ausência desse instrumento fragiliza a gestão documental, uma vez que, no ano de 2020, houve abertura de processos administrativos em suporte físico e eletrônico.

Não obstante, a Pró-Reitoria de Administração (PROAD) e a Secretaria de Tecnologias Digitais (STD) disponibilizam informações, manuais e procedimentos relevantes para a correta utilização do sistema no portal da UFRPE e na Central de Ajuda da UFRPE-Digital.

Embora o Decreto 8.539/2015, tenha obrigado a implantação de meio eletrônico para tramitação de processos, tendo como marco o prazo de outubro/2017, não foi visualizada no PDI 2013-2020[6], ação estratégica para viabilizar esta ação na instituição, o que, de certo modo, configura-se como uma fragilidade no planejamento (UFRPE, 2013). Apesar disso, constatou-se sua efetivação no Relatório de Gestão referente ao exercício de 2020, o que é um indicativo do caráter de urgência, dada a necessidade de viabilizar as atividades administrativas de forma remota.

Nesse mesmo relatório, constam informações sobre o Comitê de Governança Digital da UFRPE, que tem como "finalidade promover o alinhamento da área de Tecnologia da Informação e Comunicação (TIC) e da Segurança da Informação (SI) às estratégias e prioridades organizacionais da instituição, por meio do estabelecimento de políticas e diretrizes de TIC" (UFRPE, 2021b, p. 116).

[6] Este documento foi revisado no ano de 2018, num processo democrático, com participação de toda a comunidade acadêmica.

Quanto à capacitação de servidores, os Relatórios de Gestão da UFRPE referentes aos exercícios de 2020, 2021 e 2022 e da Pró-Reitoria de Gestão de Pessoas (PROGEPE) - exercício 2023 - informam o quantitativo de capacitados de forma abrangente, sem detalhamento dos cursos que foram promovidos relacionados à utilização do SIPAC, à proteção de dados pessoais e à segurança da informação. Considerando que a ementa do curso ofertado pela UFRPE aborda critério para cadastro da natureza do documento (ostensivo e restrito), foi solicitado ao setor competente o quantitativo de capacitações realizadas, no período de 2020 a 2023.

A Tabela 1, constante a seguir, contém os dados obtidos:

Tabela 1 - Quantidade de servidores capacitados no curso do SIPAC/UFRPE

Ano	Quantidade de Capacitados
2020	669
2021	54
2022	67
2023	0
Total	**790**

Fonte: Dados da pesquisa (2024).

Isso atesta que, no período de 04 anos, foram emitidos 790 certificados internos, tendo seu quantitativo maior em 2020, ano da implementação do sistema. Salienta-se que a pandemia impôs grandes desafios à gestão das organizações, que, em virtude da restrição do contato presencial, direcionaram sua atuação para a modalidade virtual, com o suporte da tecnologia.

Referente às ações de capacitação, apesar de não ter sido identificado nenhum curso específico sobre proteção de dados ofertado pela UFRPE, foram promovidas palestras, a partir de 2022, referente à LGPD, sendo a primeira edição presencial no *campus* Dois Irmãos, e a segunda, em 2023, via *Youtube*, oportunizando a toda comunidade acadêmica.

Ainda, conforme o PDI (UFRPE, 2021a, p. 292), foi estabelecida como meta até 2025 realizar "treinamentos com alcance de, ao menos, 90% dos servidores", no que tange à capacitação em segurança da informação, com o objetivo de "conscientizar e capacitar usuário(a)s da UFRPE em segurança da informação e comunicação".

Quanto às boas práticas de governança, com base nos mecanismos de liderança, estratégia e controle, observou-se no PDI-2021-2030 que estão sendo implementadas pela UFRPE, no âmbito do SIPAC. Especificamente, quanto ao mecanismo de controle, constatou-se que, a fim de promover a transparência e *accountability,* têm-se como ação a implementação do SIG, com funcionamento do SIPAC (UFRPE, 2021a). O próprio TCU (Brasil, 2021, p. 3)

destaca que “a implantação de um sistema de processo eletrônico pressupõe ganhos de eficiência, economia, segurança, transparência, acesso e sustentabilidade ambiental. Esses impactos têm sido referidos na doutrina, e avaliados na prática por alguns entes”.

Ainda como ação de governança, a UFRPE, através da Resolução CONSU/UFRPE nº 103, de 14 de junho de 2021, criou o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) e instituiu a Política de Privacidade e Proteção de Dados Pessoais da UFRPE. Essas ações contribuem para a governança de dados, assegurando diretrizes para a conformidade e promoção da integridade no tratamento das informações.

Some-se a isto que foi publicada uma cartilha, com o intuito de apresentar à comunidade acadêmica os principais dispositivos e conceitos apresentados na LGPD. A cartilha foi publicada em março/2021, e apresenta em seu conteúdo os principais aspectos e conceitos apresentados pela referida lei, bem como os princípios estabelecidos para tratamento de dados, as sanções administrativas previstas no âmbito das entidades e órgãos públicos, etapas para implementação da LGPD e respostas para perguntas frequentes (UFRPE, 2021c). Apesar de ser uma boa iniciativa na disseminação do conhecimento acerca do tema, esse documento requer um maior aprofundamento sobre os procedimentos práticos para o tratamento de dados no âmbito da instituição.

Por fim, no PDI-2021-2030, foi estabelecido como um dos objetivos estratégicos à adequação à LGPD, o que é positivo. Outrossim, a instituição pretende alcançá-lo até o ano de 2025, a fim de que todos os serviços prestados estejam em conformidade com a supracitada normativa (UFRPE, 2021a).

Cabe ressaltar que o prazo estabelecido pela UFRPE ultrapassou em 05 anos a meta estabelecida na EGD 2020-2023, demonstrando que essa adequação demanda mudanças de paradigmas dentro da própria instituição, o que requer não somente cursos, mas palestras e conscientização, tendo em vista que é natural que os servidores, diante de mudanças nos procedimentos, tenham resistência cultural e que isso é um fator que exige tempo a ser superado.

4.1.2.1 Abertura e Instrução de Processo Administrativo Eletrônico - UFRPE

Uma particularidade identificada na implementação do SIPAC na instituição foi a centralização da abertura de processos nas unidades de protocolo, medida adotada inicialmente durante o período pandêmico e que persiste mesmo após o seu encerramento (UFRPE, 2020d). Apesar do sistema permitir a descentralização, a pesquisa documental revelou que, por opção

da Gestão Superior, essa permissão é centralizada. Apesar da possibilidade de interpretar esse fato como uma estratégia eficaz para a gestão processual, a fim de padronizar e minimizar erros no cadastro e no fluxo inicial, essa centralização também poderá gerar sobrecarga de trabalho, além de diminuir a autonomia dos agentes públicos.

No tocante à abertura de processos e documentos eletrônicos, foi publicada a Resolução 031/2020, do Conselho Universitário (CONSU), de 11 de agosto de 2020, de forma complementar à LAI e LGPD, que regula a proteção de dados pessoais no âmbito da UFRPE, restringindo "à divulgação de documentos que contenham dados pessoais de pessoa natural na utilização do SIPAC" (UFRPE, 2020a, p. 1).

A referida resolução exemplifica como tipo de dados pessoais:

> a) número de telefone de contato pessoal;
> b) endereço residencial;
> c) endereço de correio eletrônico pessoal;
> d) data de nascimento;
> e) RG;
> f) CPF;
> g) título de eleitor;
> h) estado civil (UFRPE, 2020a, p. 1).

Visando garantir à privacidade e à intimidade das pessoas naturais, a Resolução determina que:

> Art. 3º - Quando da criação ou inserção de documentos no SIPAC, os servidores da UFRPE devem observar a presença de informações que contenham dado pessoal ou dado pessoal sensível, selecionando as opções de restrição de acesso às peças documentais que contenham tais características, restringindo o seu acesso às unidades administrativas ou servidores que necessitem de tais dados, para o desempenho de suas atividades funcionais (UFRPE, 2020a, p. 2).

Conforme fragmento acima, foi destacada a importância de considerar a presença de informações que contenham dados pessoais, sensíveis ou não, durante o cadastro de documentação eletrônica no SIPAC, sendo responsabilidade e dever do servidor da instituição observar essas informações e, ao identificá-las, restringir o acesso a essas peças documentais. Vale destacar um alinhamento com os princípios da governança de dados relacionados à segurança e privacidade, garantindo que apenas pessoas autorizadas tenham acesso a essas informações, reduzindo, assim, o risco de violação de dados e protegendo a privacidade dos indivíduos.

Para cadastro de documentação, o usuário do sistema deverá acessar por meio da tela inicial, na qual é apresentada a interface de *login* do sistema SIPAC da UFRPE. Nela, é

evidenciado um formulário de acesso que requer o nome de usuário e a inserção de uma senha para autenticação.

Para adição de um novo documento em processos eletrônicos, é necessário que o usuário indique a natureza do documento, tipificado como ostensivo e restrito (Figura 2), a partir da observação das informações contidas nele.

Figura 2 - Tela para Adição de Documentos em processo eletrônico SIPAC/UFRPE

Fonte: Dados da pesquisa (2024).

Para os casos de documentos com natureza restrita, o usuário do sistema deverá justificar às hipoteses legais da restrição, selecionando uma das opções apresentadas pelo SIPAC/UFRPE, listadas no Quadro 10:

Quadro 10 - Hipóteses legais do SIPAC/UFRPE para documentação restrita

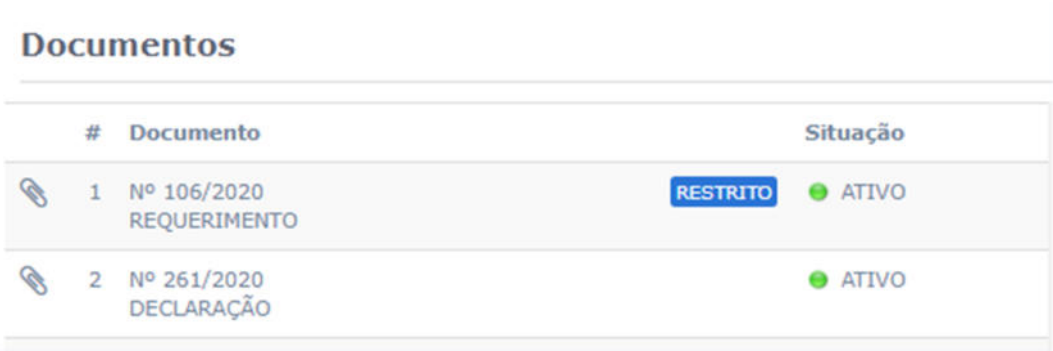
Item	Hipótese Legal
1	Controle Interno (Art. 26, § 3º, da Lei nº 10.180/2001)
2	Documento Preparatório (Art. 7º, § 3º, da Lei nº 12.527/2011)
3	Informação Pessoal (Art. 31 da Lei nº 12.527/2011)
4	Investigação de Responsabilidade de Servidor (Art. 150 da Lei nº 8.112/1990)
5	Sigilo Contábil (Art. 1.190 da Lei nº 10.406/2002)
6	Sigilo Empresarial (Art. 169 da Lei 11.101/2005)
7	Sigilo Fiscal (Art. 198, caput, da Lei nº 5.172/1966)

Fonte: Dados da pesquisa (2024).

Observa-se que, das setes hipóteses apresentadas pelo sistema para restrição de acesso à informação, apenas uma está relacionada à informação pessoal, em atendimento ao artigo 31 da LAI, que frisa, dentre outros, a restrição do acesso a informações pessoais a agentes públicos legalmente autorizados e à pessoa a que elas se referem (Brasil, 2011).

Para os documentos restritos de um processo eletrônico, o sistema apresenta um rótulo específico ao lado do documento correspondente, indicando que o conteúdo só poderá ser acessado pelas unidades nas quais são tramitados, pelos interessados e pelos assinantes do processo. Para documentação ostensiva, não há nenhum rótulo, conforme ilustra a Figura 3.

Figura 3 - Tela Consulta Pública: Documentos que compõem processo SIPAC/UFRPE com natureza "Restrito" e "Ostensivo"



Fonte: Dados da pesquisa (2024).

Ressalta-se que a administração do sistema permite a gestão da visualização pública para cada tipo de documento de forma prévia, por meio da funcionalidade "Público", que gerencia o acesso dos usuários externos aos documentos do sistema, conforme Figura 4.

Figura 4 - Tela SIPAC/UFRPE – Lista dos Tipos de Documentos cadastrados no sistema

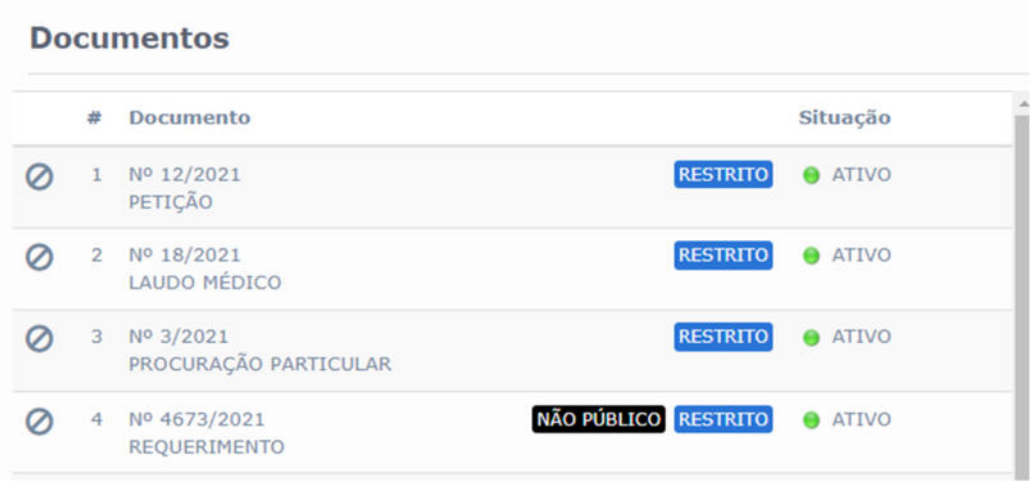
Fonte: Dados da pesquisa (2024).

Esse recurso pode ser interpretado como uma estratégia para mitigar possíveis erros no cadastro da natureza do documento e, de forma mais ampla, assegurar uma gestão documental efetiva, garantir transparência, acesso à informação e salvaguardar os dados pessoais.

Dessa forma, documentos rotulados previamente na funcionalidade "Público" com "Visualização Pública Bloqueada" terão seu conteúdo restrito na "Consulta Pública",

independente da natureza do documento (restrito ou ostensivo). Ressalta-se que, na "Consulta Pública", os documentos com "Visualização Pública Bloqueada" serão sinalizados com rótulo específico "NÃO PÚBLICO" conforme Figura 5 e Figura 6.

Figura 5 - Tela Consulta Pública: Documentos que compõem processo SIPAC/UFRPE com natureza "Restrito" e "Visualização Pública Bloqueada"



Fonte: Dados da pesquisa (2024).

Figura 6 - Tela Consulta Pública: Documentos que compõem processo SIPAC/UFRPE com natureza "Ostensiva" e "Visualização Pública Bloqueada"

Fonte: Dados da pesquisa (2024).

Ao total, são 394 tipos de documentos cadastrados no sistema, dos quais apenas o tipo "Documento Externo" e "Requerimento" possuem "Visualização Pública Bloqueada".

É importante destacar que a "Visualização Pública Bloqueada" apenas se aplica ao público externo na "Consulta Pública", ou seja, a documentação ostensiva com "Visualização Pública Bloqueada" poderá ser visualizada pela comunidade interna, via sistema. Nesse sentido,

conforme estabelecido pela Resolução interna 031/2020, do CONSU, a indicação correta da natureza do documento é importante, pois mesmo aqueles com “Visualização Pública Bloqueada”, cadastrados como ostensivos, ficarão disponíveis para livre consulta pelos usuários internos.

Quanto ao recurso para alteração/correção da natureza de um documento já cadastrado no sistema, era limitado apenas para os usuários com perfil para cadastrar processo, ou seja, apenas os servidores lotados nas unidades de protocolo. Em 15 de agosto de 2023, foi realizada uma atualização, atribuindo essa permissão para as demais unidades. Essas mudanças ocorreram após mais de três anos da implantação do sistema eletrônico no âmbito da UFRPE.

Salienta-se que, caso o cadastro da natureza do documento tenha sido feito de forma equivocada, o sistema permite a alteração nas seguintes condições:

> 1. Para que possa ser realizado essa operação, é necessário que **o documento ou processo esteja na unidade na qual o usuário possui acesso aos processos dentro da sua mesa virtual da sua unidade.**
> 2. Uma vez o processo na referida unidade, apenas a chefia ou o substituto da chefia da unidade em questão pode realizar tal operação.
> 3. O sistema possibilita também que o usuário criador do documento possa realizar a operação caso o processo esteja dentro da sua mesa virtual, ou seja, dentro da sua unidade (UFRPE, 2023).

Outro ponto importante é que subsiste a inabilitação para correção da natureza de documento cadastrada por outro setor por parte dos servidores das unidades de protocolo e arquivo, responsáveis pela gestão documental na instituição. Desse modo, as unidades a que competem essa gestão não têm habilitação para corrigir a natureza de documento cadastrada por outro setor, o que se configura como um aspecto que poderá ocasionar morosidade e retrabalho, já que detectado o erro, o colaborador deverá efetuar a devolução do processo à unidade de origem.

4.1.3 Análise comparativa entre a UFRPE e as demais universidades do Nordeste

Após análise dos resultados expostos anteriormente, pode-se constatar que a UFRPE se encontra alinhada com as práticas comuns observadas nas demais universidades federais do Nordeste, no que diz respeito à implementação de sistemas eletrônicos para a gestão de processos administrativos. A relevância da análise reside no entendimento do panorama atual da gestão processual e proteção de dados pessoais no órgão, identificando áreas de melhoria e boas práticas.

Os resultados apontaram que, assim como as demais IFES, a UFRPE não implementou o sistema no prazo estabelecido pelo Decreto 8.539/2015. Ademais, foi possível observar que, na contramão da maioria das universidades, a IFES investigada mantém a centralização das atividades de cadastro de processo eletrônico nas unidades de protocolo, o que, futuramente, poderá gerar algumas limitações operacionais.

Outro ponto divergente refere-se à customização do sistema, uma vez que a instituição fez adaptação para o atendimento de procedimentos internos, dentre eles, a ampliação da permissão de correção da natureza documental para os servidores não cadastradores de processo que, no sistema nativo, estava habilitado apenas para os usuários cadastradores. Conforme já exposto, boa parte das entidades não personalizou o sistema de processo eletrônico que utilizam.

Verifica-se também que, no *lócus* da pesquisa, foi publicada uma resolução específica, que regulamenta a restrição à divulgação de documentos que contenham dados pessoais de pessoa natural no âmbito dos processos eletrônicos na instituição, divergente da maioria das IFES, que ainda não implementaram, evidenciando um compromisso com a proteção de dados pessoais dos titulares e com os direitos fundamentais.

Outrossim, apesar de ter extrapolado a meta estabelecida na Estratégia de Governança Digital (EGD) 2020-2023, o fato da UFRPE ter incluído no seu PDI a previsão de adequação à LGPD é um indicativo que reflete um compromisso da instituição com a governança de dados, sobressaindo-se em relação às demais IFES do Nordeste. Outro fator positivo refere-se à criação do Comitê Gestor de Privacidade e Proteção de Dados, bem como a instituição de uma política de privacidade interna, ações que também foram realizadas por boa parte das entidades consultadas.

4.2 LEVANTAMENTO DOS PROCESSOS SIPAC/UFRPE

Essa etapa teve como objetivo analisar a conformidade dos processos administrativos eletrônicos com relação às normas que regulamentam o tratamento de dados pessoais na UFRPE, a fim de identificar possíveis erros na indicação do nível de acesso do documento, público e restrito.

Foram observados os 79 processos eletrônicos de concessão de pensão civil, instruídos e arquivados no período de abril de 2020 a dezembro de 2022. Essa análise teve como foco a natureza dos documentos cadastrados pelos usuários do sistema.

A Tabela 2 ilustra a distribuição, por ano, desses processos.

Tabela 2 - Quantitativo anual de processos administrativos eletrônicos de concessão de pensão civil

ANO	QUANTITATIVO
2020	17
2021	29
2022	33
Total	**79**

Fonte: Elaborado pela autora (2024).

Nos casos em que foram identificadas ocorrências de não conformidade, verificou-se o titular, dividido entre público externo e interno (operador); o tipo de informação restrita ou exposta; bem como o formato de exposição do dado.

4.2.1 Total de Processos observados e a conformidade da natureza dos documentos

Inicialmente, foi observado se o processo estava em conformidade com a transparência ativa e as normas de proteção de dados pessoais da UFRPE, especificamente no tocante à natureza documental, conforme Tabela 3:

Tabela 3 - Quantidade anual de processos com ocorrência de não conformidade

Ano do Processo	Quantidade de Processos	Quantidade de Processos com natureza de documento não conforme	Percentual de Processos com natureza de documento não conforme
2020	17	16	94,1%
2021	29	28	96,6%
2022	33	29	87,9%
Total	**79**	**73**	**92,4%**

Fonte: Dados da pesquisa (2024)

Constatou-se que do universo de 79 processos, 73 (92,4%) apresentaram documentação não conforme de acordo com este parâmetro.

Com relação ao quantitativo, foram analisados 1.668 documentos, dos quais 132 (7,9%) apresentaram desconformidade com o nível de acesso do documento cadastrado, conforme apresentada na Tabela 4:

Tabela 4 - Quantidade anual de documentos com ocorrência de não conformidade

Ano do Processo	Quantidade Total de Documentos	Quantidade de Documentos com natureza não conforme	Percentual de Documentos com natureza não conforme
2020	492	29	5,9%
2021	649	50	7,7%
2022	527	53	10,1%
Total	**1.668**	**132**	**7,9%**

Fonte: Dados da pesquisa (2024)

Dos 132 documentos apresentados com inconsistência no cadastro da sua natureza, foi observado que 03 (2,3%) deles apresentavam restrição de acesso a informações públicas. Some-se a isto que ficou constatado que 129 (97,7%), originalmente, continham informações pessoais, porém foram classificados erroneamente como públicos, conforme demonstrado no Gráfico 3.

Gráfico 3 - Quantidade de documentos com ocorrência de natureza não conforme

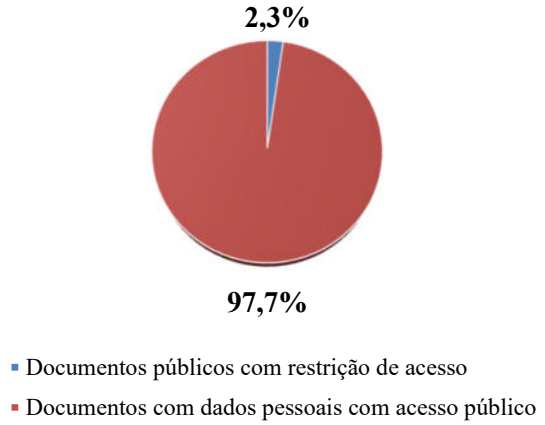
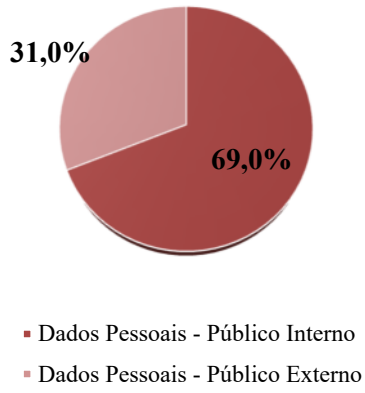


Gráfico 4 - Quantidade de documentos com ocorrência de natureza não conforme por titular



Fonte: Dados da pesquisa (2024)

Quanto à exposição de dados, observou-se que 39 (31%) desses documentos continham informações pessoais de "público externo", ao passo que 89 (69%) relacionavam-se ao "público interno" (operador), conforme representado no Gráfico 4.

Na próxima subseção, será apresentada a análise dos 132 documentos que apresentaram divergência na natureza do documento.

4.2.2 Documentação de interesse público cadastrado com natureza de documento "restrito"

Quanto à restrição de acesso a documentos de interesse público, foram observados que apenas 3 (0,2%) da amostra total dos documentos apresentaram essa não conformidade, Tabela 5:

Tabela 5 - Quantidade de documentos de interesse público cadastrados com nível de acesso "restrito"

Ano do Processo	Quantidade Total de Documentos	Quantidade de Documentos Públicos cadastrados com nível de acesso "restrito"	Percentual Documentos Públicos cadastrados com nível de acesso "restrito"
2020	492	2	0,4%
2021	649	1	0,2%
2022	527	-	-
Total	**1.668**	**3**	**0,2%**

Fonte: Dados da pesquisa (2024)

Isso evidencia que a grande maioria está classificada corretamente, em conformidade com as diretrizes da LAI, no que tange à transparência. Esses erros podem ter ocorrido devido a equívocos na indicação da natureza do documento.

4.2.3 Documentação com informações pessoais cadastrados com natureza "ostensivo"

Quanto à publicidade de documentos contendo informações pessoais registrados com natureza de documento ostensivo, constatou-se que 129 (7,7%) da amostra total dos documentos foram cadastrados com não conformidade, conforme apresentado na Tabela 6:

Tabela 6 - Quantidade de documentos com informações pessoais cadastrados com acesso "ostensivo"

Ano do Processo	Quantidade Total de Documentos	Quantidade de Documentos Públicos cadastrados com acesso "restrito"	Percentual Documentos Públicos cadastrados com acesso "restrito"
2020	492	27	5,5%
2021	649	49	7,6%
2022	527	53	10,1%
Total	**1.668**	**129**	**7,7%**

Fonte: Dados da pesquisa (2024)

Além disso, observa-se um aumento nas ocorrências ao longo dos anos.

Ao analisar essas desconformidades e filtrá-las pelo “tipo do titular”, observa-se que, para o “público externo”, foram identificados 39 (2,3%) documentos com erro no cadastro da natureza, conforme Tabela 7:

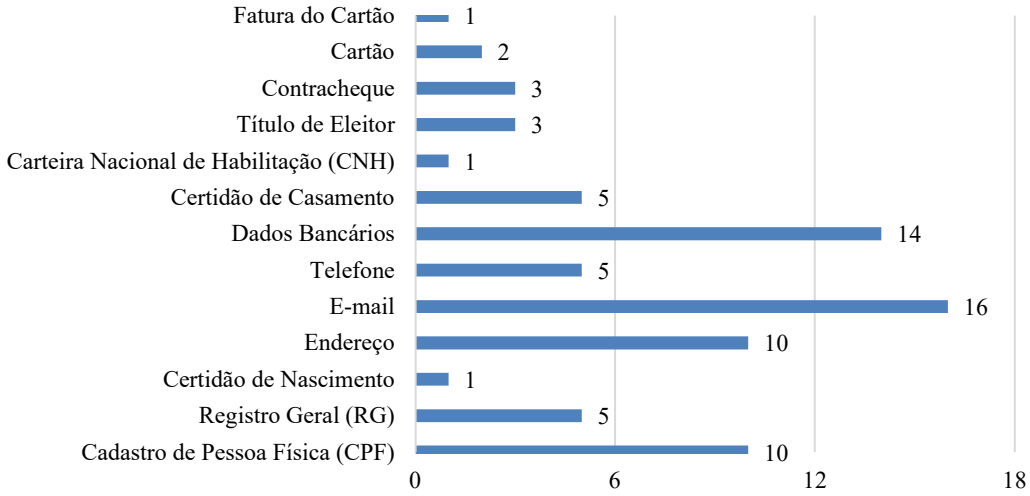
Tabela 7 - Quantidade de documentos com informações pessoais cadastrados com acesso “ostensivo” – Titular “público externo”

Ano do Processo	Quantidade Total de Documentos	Quantidade de Documentos com dados pessoais cadastrados com nível de acesso “ostensivo”	Percentual Documentos com dados pessoais cadastrados com nível de acesso “ostensivo”
2020	492	12	2,4%
2021	649	16	2,5%
2022	527	11	2,1%
Total	**1.668**	**39**	**2,3%**

Fonte: Dados da pesquisa (2024)

O Gráfico 5 apresenta a frequência e teor das informações expostas do “público externo”:

Gráfico 5 – Tipologia das informações pessoais com acesso “ostensivo” - Titular “público externo”



Fonte: Dados da pesquisa (2024)

Na análise referente a essas informações, observou-se uma maior exposição nos dados de endereço de *e-mail* e dados bancários, seguidos pelo endereço residencial e cadastro de pessoa física (CPF).

Ao examinar a forma como esses dados foram expostos, constatou-se a ocorrência de exposição integral de documentos digitalizados de dados bancários, certidões de casamento, contracheques e cartão bancário, inclusive com o código de segurança. A divulgação integral desses documentos pode permitir o acesso a uma quantidade substancial de dados pessoais por parte de terceiros, aumentando a vulnerabilidade dos indivíduos a possíveis violações de privacidade e fraudes.

Apesar da diminuição da inconformidade da natureza de acesso ao longo dos anos, conforme Tabela 8, a exposição desses dados pessoais representa um risco significativo para a privacidade e a segurança dos indivíduos envolvidos, e demonstra uma fragilidade na forma de controle quanto à conformidade do cadastro dessas informações, o que torna imperativo a necessidade de fortalecer a cultura de proteção de dados e *compliance,* bem como a necessidade recorrente de treinamento e gerenciamento dos riscos. Vale destacar que esse cenário pode não apenas violar a lei de proteção de dados, mas também expõe a instituição a possíveis repercussões legais e danos à reputação.

Tabela 8 - Informação pessoal com acesso "ostensivo" - Titular "público externo"

Dado Pessoal	2020	2021	2022	Total
e-mail	0	9	7	16
Dados Bancários	6	4	4	14
Cadastro de Pessoa Física (CPF)	4	5	4	10
Endereço	3	5	2	10
Certidão de Casamento	4	1	0	5
Registro Geral (RG)	3	1	1	5
Telefone	2	2	1	5
Contracheque	1	2	0	3
Título de Eleitor	2	1	0	3
Cartão	1	1	0	2
Certidão de Nascimento	0	0	1	1
Carteira Nacional de Habilitação (CNH)	0	1	0	1
Fatura do Cartão	0	1	0	1
Total	**26**	**33**	**17**	**76**

Fonte: Dados da pesquisa (2024)

Acrescenta-se que a exposição dessas informações ocorreu tanto em formulários quanto em documentos digitalizados integralmente. Considerando que a abertura do processo é centralizada nas unidades de protocolo, e que o "público externo" não tem acesso ao sistema

para correção da natureza do documento, pode-se inferir que é necessário que a instituição invista em cursos destinados a setores estratégicos da gestão documental, o que permitirá uma maior conscientização dos operadores envolvidos no tratamento de dados.

Quanto aos documentos cadastrados com acesso "ostensivo" contendo informações pessoais, de titular "público interno" (operador) foram identificados 89 (5,3%) documentos com erro no cadastro da natureza. Cabe destacar que o teor desses documentos são de interesse público, e que se caracterizam na forma de despachos[7], no entanto, a exposição do dado foi decorrente à assinatura do operador, que utilizou certificado digital com exposição do CPF. Neste caso, embora seja uma assinatura digital, não se atentou que houve exposição de um dado pessoal; sendo assim, deveria estar com natureza de documento restrito, Tabela 9:

Tabela 9 - Quantidade de documentos com informações pessoais cadastrados com acesso "ostensivo" - Titular "público interno"

Ano do Processo	Quantidade Total de Documentos	Quantidade de Documentos com dados pessoais cadastrados com nível de acesso "ostensivo"	Percentual Documentos com dados pessoais cadastrados com nível de acesso "ostensivo"
2020	492	13	2,6%
2021	649	33	5,1%
2022	527	43	8,2%
Total	**1.668**	**89**	**5,3%**

Fonte: Dados da pesquisa (2024)

Ressalta-se que a inclusão dessa informação (número do CPF) é um excesso que vai de encontro ao princípio da necessidade da LGPD, considerando que deve haver limitação do tratamento de dados ao mínimo necessário para realização de suas finalidades (Brasil, 2018). A Tabela 10 apresenta a distribuição anual com o quantitativo das informações expostas:

Tabela 10 - Informação pessoal com acesso "ostensivo" - Titular "público interno"

Dado Pessoal	2020	2021	2022	Total
Cadastro de Pessoa Física (CPF)	14	33	56	**112**

Fonte: Dados da pesquisa (2024)

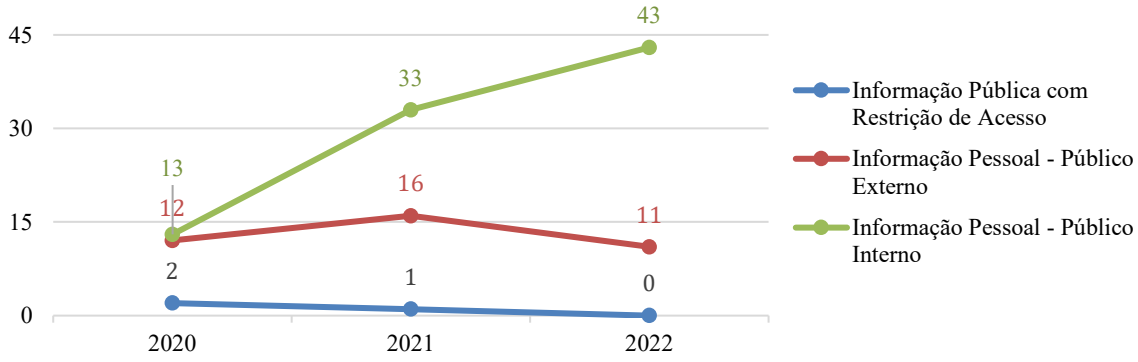
Desse modo, para instruir um processo e emitir despachos, o CPF do operador responsável pelo ato não é necessário, uma vez que sua matrícula já é suficiente para respeitar

[7] Despachos são "todos os atos praticados no curso de um processo ou de um procedimento que não possuem conteúdo decisório" (Brasil, 2024c).

o princípio da transparência e publicidade, bem como resguardar seus dados pessoais. A própria AGU orienta o uso da matrícula SIAPE ao invés do número do CPF em documentos e contratos relacionados a atividades da administração pública federal, tendo em vista que o SIAPE é suficiente para identificar o agente público responsável pelo ato. Segundo o órgão, apesar da matrícula ser um dado pessoal, não possui implicações além da esfera pública do servidor, o que significa que não há razões para restringir seu acesso (Brasil, 2021b).

De forma geral, conforme Gráfico 6, a pesquisa constatou que ocorreu uma diminuição na desconformidade quanto à restrição de acesso à informação pública ao longo dos anos de 2020, 2021 e 2022. Quanto à exposição de dados pessoais, há motivos para preocupação com a não conformidade na natureza dos documentos, uma vez que, para o titular "público externo", houve um pequeno crescimento de ocorrências de 2020 a 2021, com redução em 2022. No entanto, quando observado essa exposição para titular "público interno", essa desconformidade aumentou aos longos desses anos, o que atesta que o operador, muitas vezes, cuida de dados de terceiros, mas não tem conhecimento que deveria proteger o seu próprio dado.

Gráfico 6 - Quantidade de documentos com desconformidades no nível de acesso



Fonte: Dados da pesquisa (2024)

Destaca-se que, mesmo com a redução de exposição de dados pessoais do "público externo", em um contexto em que se espera a conformidade de todos os documentos, um único incidente sugere falha nos controles de segurança e na conformidade com as regulamentações de proteção de dados. Desse modo, uma única exposição poderá ter consequências significativas, tanto para o indivíduo cujo dado foi publicizado quanto para a instituição responsável pela sua proteção, resultando em danos à reputação, à confiança e até mesmo em ações legais, dependendo da gravidade do incidente. Frazão, Oliva e Abilio (2019) reforçam que, no contexto do meio digital, a velocidade de propagação das informações e os desafios

para sua contenção exigem a implementação de políticas de segurança rigorosas para prevenir acessos não autorizados aos dados.

Com base nesses resultados, é possível concluir que a proteção de dados pessoais no âmbito dos processos administrativos eletrônicos é um desafio para a universidade. Apesar da melhoria na restrição de acesso a informações públicas, as exposições persistentes dos dados indicam a necessidade de ações complementares para assegurar a conformidade com as normativas de proteção de dados.

4.3 DESDOBRAMENTOS RELEVANTES DA PESQUISA

Embora não tenha sido o foco da pesquisa, no decorrer da coleta e análise de dados, do terceiro objetivo específico, referente à análise da conformidade dos processos eletrônicos em relação às normas que regulamentam o tratamento de dados pessoais de pessoa natural na UFRPE, foi constatada a exposição de dados pessoais de pessoas falecidas (instituidores de pensão civil).

Não obstante a legislação ser direcionada à proteção de dados pessoais de pessoa natural, foi constado que 16 documentos de pessoas falecidas estavam com exposição não apenas da certidão de óbito[8], mas também da cópia de RG, CPF e Título de Eleitor. Apesar da LAI e LGPD serem omissas nos casos que se aplicam à proteção de dados da pessoa falecida, o Código Civil, no seu art. 12, parágrafo único, esclarece que o morto poderá sofrer violação aos direitos inerentes à sua personalidade (direito à honra, à privacidade, à imagem). Nesse sentido, a família da pessoa falecida "terá legitimidade para pleitear que cesse a ameaça e/ou lesão inerente à violação da personalidade", tendo em vista que o referido código protege os direitos *post-mortem*[9] inerentes à personalidade jurídica (Miranda, 2004).

Nesse contexto, a restrição de nível de acesso a esses dados não se constitui como um bloqueio ou negativa de acesso à informação, mas tão somente uma restrição na publicidade, condicionada a uma justificativa fundamentada, por parte do solicitante da informação. Cabe salientar que essa restrição se encontra amparada no Código Civil e Constituição Federal, e não visa abranger o escopo de proteção da LAI e LGPD.

[8] Cabe esclarecer que a solicitação da certidão de óbito está aberta a qualquer pessoa desde que demonstre interesse jurídico ou pessoal no documento (Azevedo, 2022).
[9] *post-mortem* – posterior a morte.

4.4 PROPOSTAS DE AÇÕES COMPLEMENTARES

Com base nos resultados da pesquisa e revisão bibliográfica, visando atender ao quarto objetivo delineado, esta subseção apresentará algumas sugestões para aprimorar a governança de dados e a proteção adequada das informações pessoais no âmbito dos processos administrativos eletrônicos da UFRPE, abaixo apresentadas:

a) **Capacitação:** Implementar programas de capacitação abrangentes para todos os servidores, com ênfase na sensibilização sobre a importância da proteção de dados pessoais. Apesar desta dissertação se revestir com caráter prático, alinhado a um escopo de mestrado profissional, foi proposto como produto técnico a ementa de um curso, conforme Apêndice B;
b) **Fortalecimento da Cultura de Proteção de Dados Pessoais**: Promover uma cultura organizacional que valorize e priorize a proteção de dados pessoais em todos os níveis da instituição, incentivando a conscientização e o engajamento dos colaboradores;
c) **Mapeamento dos Riscos:** Identificar os riscos relacionados ao tratamento de dados pessoais, a partir do mapeamento dos fluxos de dados, no âmbito dos processos eletrônicos;
d) **Programa de *Compliance* em Proteção de Dados Pessoais**: Desenvolver e implementar um programa de *compliance* dedicado à proteção de dados, com políticas, procedimentos e mecanismos de monitoramento para garantir o cumprimento das normativas de privacidade e segurança da informação;
e) **Incentivo às assinaturas pelo próprio SIPAC**: Incentivar o uso das funcionalidades de assinatura eletrônica disponíveis no SIPAC como alternativa ao uso do certificado digital, a fim de evitar a exposição do CPF do servidor. Nos casos em que a certificação for indispensável, promover o uso das assinaturas digitais oferecidas pelo *GOV.BR* ou aplicativo do SERPRO, nos quais não há divulgação do CPF;
f) **Atualização do recurso "Visualização Pública" de documentos no SIPAC**: Revisar e atualizar o recurso "Visualização Pública" dos documentos listados no SIPAC, que sugerem conter dados pessoais, a fim de gerenciar acesso externo ao sistema de documentos com equívoco no cadastro da natureza de acesso. No Apêndice C consta lista com sugestão de documentos para "Visualização Pública Bloqueada";
g) **Atualização do SIPAC para gerenciamento prévio da Natureza do Documento**: Atualizar o SIPAC para permitir o gerenciamento prévio da natureza do documento, de forma semelhante ao que ocorre na "Visualização Pública". Isso possibilitaria a

classificação dos documentos de acordo com sua natureza, permitindo um controle mais eficaz sobre quem pode acessar e manipular determinadas informações. Essa medida contribuiria para proteger os dados pessoais, especialmente para o "público interno" não interessado, reduzindo o risco de acesso não autorizado e uso indevido das informações.

h) **Atualização do SIPAC para habilitação de servidores para correção da Natureza do Documento:** Propor a habilitação de todos os servidores na correção da natureza do documento, independente do setor de origem. Na impossibilidade de habilitar todos os servidores, sugere-se habilitar especificamente os setores de protocolo e arquivo, uma vez que são os responsáveis pela gestão documental da instituição. Essa medida permitiria uma maior agilidade e eficiência na correção da natureza dos documentos, minimizando o tempo de exposição do dado.
i) **Restrição a dados pessoais de pessoais falecidas**: Ampliar a restrição de acesso nos documentos de processos eletrônicos referente a dados pessoais de pessoais falecidas. Essa iniciativa não apenas demonstraria o compromisso da instituição com a proteção da privacidade e dignidade dos indivíduos, mesmo após o falecimento, mas também ajudaria a mitigar o risco de uso indevido ou abuso desses dados.

Estas propostas foram elaboradas com base nas desconformidades identificadas durante o estudo, visando proporcionar medidas práticas e eficazes para subsidiar o tratamento responsável dos dados, promovendo, assim, uma complementação à conformidade em relação às normativas de privacidade e proteção de dados pessoais da instituição.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa objetivou diagnosticar o cenário da proteção de dados pessoais no escopo dos processos administrativos eletrônicos da UFRPE, à luz da governança de dados, visando observar a conformidade com as normas que regulamentam o tratamento de dados pessoais no âmbito da instituição e da administração pública.

O primeiro objetivo específico consistiu em verificar o cenário de implantação do processo eletrônico e da proteção de dados pessoais no âmbito das Universidades Federais do Nordeste, a fim de fazer um comparativo com a UFRPE. Por meio da consulta via questionário e análise documental, pode-se considerar que o órgão está alinhado com as práticas comuns observadas nas demais instituições, embora ainda existam áreas a serem melhoradas referentes às permissões no sistema, à correção de não conformidades no nível de acesso da informação e à falta de adequação nas documentações.

O segundo objetivo correspondeu à identificação de ações e investimentos promovidos pela universidade na área de proteção de dados pessoais, sendo constatado que a instituição designou um Comitê Gestor e criou uma Política de Privacidade e Proteção de Dados. Além disso, como mecanismo de boa governança, foi estabelecido como meta adequar, até o ano de 2025, todos os serviços ofertados pela universidade em seu plano estratégico, ainda que não tenha sido cumprido o prazo estabelecido pela EGD 2020-2023, o que demonstra o compromisso da instituição em promover tal adequação. Outro ponto a se destacar foi a edição de resolução específica para regular o cadastro de nível de acesso dos documentos no SIPAC, em observância à transparência ativa e proteção de dados pessoais no sistema.

Quanto às ações de capacitação, apesar de não ter sido identificado nenhum curso interno específico sobre proteção de dados, a instituição promoveu palestras a fim de reforçar a governança de dados e fortalecer a cultura organizacional.

O terceiro objetivo específico descreveu as desconformidades existentes referentes ao cadastro da natureza do documento. A partir da análise dos resultados, verificou-se que, quanto à transparência, as documentações estavam alinhadas às normas. Em contrapartida, quanto à publicação de documentos com informações pessoais, percebeu-se que o erro persistiu ao longo dos anos. Ademais, foi evidenciado uma menor ocorrência nos casos em que o titular era "público externo", quando comparado ao titular "público interno" (operador). Não obstante, é fundamental reconhecer que uma única exposição não apenas compromete a privacidade e segurança dos indivíduos afetados, mas também afetam a reputação e a credibilidade da instituição, some-se a isto que a rápida disseminação das informações no ambiente digital e os

desafios para sua contenção exigem a implementação de políticas de segurança rigorosas para prevenir acessos não autorizados aos dados.

Já para o quarto objetivo específico, foi percebido que a classificação de nível de acesso (publicidade ou restrição) ainda está muito concentrada nos operadores de tratamento de dados. Nesse sentido, é imperativo que a instituição realize o mapeamento de riscos, implemente programas de *compliance* e ofereça capacitação continuada e atualização dos sistemas de gestão de processos, a fim de disseminar o conhecimento e promover a cultura de proteção de dados no âmbito institucional.

Pode-se concluir que a instituição deve realizar uma análise mais aprofundada dos processos de coleta, armazenamento e compartilhamento de dados pessoais, a fim de identificar e corrigir quaisquer vulnerabilidades ou lacunas na proteção de dados. Ao tomar essas iniciativas, o órgão corrobora seu compromisso com a proteção da privacidade e segurança dos dados, fortalecendo assim a confiança e a credibilidade junto aos seus *stakeholders*.

5.1 LIMITAÇÕES DA PESQUISA E PROPOSTA DE ESTUDOS FUTUROS

Como limitação da pesquisa, não foi possível identificar as causas da desconformidade junto aos operadores do fluxo do processo, uma vez que foi direcionada para observação das legislações e normas sobre processo eletrônico e proteção de dados pessoais. A pesquisa ficou restrita ao escopo dos processos administrativos eletrônicos, e limitou-se a observar a classificação da natureza do documento em um único tipo de processo, na atividade-meio da instituição, não explorando processos da atividade-fim e demais atividades da instituição.

Considerando a complexidade do tema e a constatação de que este estudo não se propôs a esgotá-lo, recomenda-se que sejam realizadas outras pesquisas, envolvendo processos e documentos eletrônicos da atividade-fim; a verificação da adequação dos documentos; e estudos com os operadores dos fluxos processuais, a fim de identificar as possíveis causas da falta de conformidade.

Ainda, explorando a dimensão do assunto, sugere-se pesquisas que investiguem o impacto da implementação da proteção de dados pessoais na cultura organizacional, abrangendo sua influencia na conformidade e na eficácia das práticas de proteção de dados, e, estudos que explorem como as organizações podem integrar a gestão de risco e o *compliance* à sua cultura organizacional para garantir uma abordagem holística e eficaz na proteção desses dados.

REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. **Perspectivas em Ciência da Informação**, [S.L.], v. 27, n. 3, p. 26-45, set. 2022. Trimestral. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/1981-5344/25905.

AZEVEDO, Waldeli. **Certidão de óbito**: como tirar? veja quais documentos levar. Como tirar? Veja quais documentos levar. 2022. Disponível em: https://economia.uol.com.br/guia-de-economia/certidao-de-obito-como-tirar-o-que-levar.htm. Acesso em: 12 fev. 2024.

BARBIERI, Carlos. **Governança de Dados:** Práticas, conceitos e novos caminhos**.** Rio de Janeiro: Alta Books, 2019.

BARBOSA, Tatiane Santos; LOPES, Jerisnaldo Matos; PIAU, Deise Danielle Neves Dias; SILVA, Marcelo Santana; TELES, Eduardo Oliveira. A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS INSTITUIÇÕES PÚBLICAS DE ENSINO: POSSÍV

EIS IMPACTOS E DESAFIOS. In: ENPI - ENCONTRO NACIONAL DE PROPRIEDADE INTELECTUAL, 7., 2021, Aracaju. **Anais [...].** Aracaju: Enpi, 2021. v. 7, p. 2114-2123. Disponível em: https://www.api.org.br/conferences/index.php/ENPI2021/ENPI2021/paper/view/1455. Acesso em: 07 jan. 2024.

BARROS, Aidil Jesus da Silveira; LEHFELD, Neide Aparecida de Souza. **Fundamentos de metodologia científica**. 3. ed. São Paulo: Pearson Prentice Hall, 2007.

BIONI, Bruno Ricardo. **Proteção de Dados pessoais: funções e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BRASIL. **Plano Diretor da Reforma do Aparelho do Estado**. [1995]. Disponível em http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/plano-diretor-dareforma-do-aparelho-do-estado-1995.pdf/view. Acesso em: 23 nov. 2023.

BRASIL. **Lei n° 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, 24 jul. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 05 mar. 2023.

BRASIL. **Lei n° 9.784, de 29 de janeiro de 1999**. Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília, 29 jan. 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 20 set. 2023.

BRASIL. Congresso Nacional (2000). **Lei Complementar, nº 101, 4 maio 2000. LRF – Lei de Responsabilidade Fiscal**. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Brasília: 4 maio 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp101.htm. Acesso em: 01 mar. 2023.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Brasília: 4 maio 2000a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10332.htm. Acesso em: 27 mai. 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 02 abr. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#:~:text=L12965&text=Estabelece%20princ%C3%ADpios%2C%20garantias%2C%20direitos%20e,uso%20da%20Internet%20no%20Brasil.&text=Art.,Munic%C3%ADpios%20em%20rela%C3%A7%C3%A3o%20%C3%A0%20mat%C3%A9ria.. Acesso em: 02 mar. 2023.

BRASIL. **Decreto nº 8.539, de 8 de outubro de 2015**. Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. **Diário Oficial da República Federativa do Brasil**, Brasília, 9 out. 2015. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8539.htm>. Acesso em: 02 abr. 2022.

BRASIL, **Decreto nº 8.638, de 15 de janeiro de 2016**. (Revogado pelo Decreto nº 9.203, de 22 de novembro de 2017). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8638.htm. Acesso em: 02 abr. 2022.

BRASIL, **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm. Acesso em: 02 abr. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 abr. 2022.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU** / Tribunal de Contas da União. Edição 3 - Brasília: TCU, Secretaria de Controle Externo da Administração do Estado – SecexAdministração, 2020b.

BRASIL. Comitê Central de Governança de Dados. **Guia De Boas Práticas Lei Geral de Proteção De Dados (LGPD)**, de 14 de ago. de 2020. Brasília: 14 ago. 2020c. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 01 mar. 2023.

BRASIL. Ministério da Economia e Controladoria Geral da União. **Orientação Conjunta nº 1/2021/ME/CGU**. (2021a) Transparência no Processo Administrativo Eletrônico. Brasília: 24

mar. 2021. Disponível em: https://www.gov.br/mcom/pt-br/acesso-a-informacao/processo-eletronico/OrientaoConjunta_01_2021_ME_CGU.pdf. Acesso em: 01 mar. 2023.

BRASIL. Advocacia-Geral da União (AGU). Consultoria-Geral da União (CGU). Consultoria Jurídica junto à Controladoria-Geral da União (CONJUR). Coordenação-Geral de Matéria de Transparência e Administrativa (CGTA). **Parecer n. 00001/2021/CONJUR-CGU/CGU/AGU**. (2021b) Direito Administrativo e outras matérias de Direito Público. Disponível em: https://repositorio.cgu.gov.br/handle/1/67796. Acesso em: 12 dez. 2023.

BRASIL. Tribunal de Contas da União (TCU). **Acórdão 484/2021-Plenário**. (2021c). Relatório de auditoria integrada cujo objeto é avaliar a implementação de processo eletrônico nas Instituições Federais de Ensino (IFEs). Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A484%2520ANOACORDAO%253A2021%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acesso em: 12 dez. 2023.

BRASIL. Constituição (1988). **Emenda constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da República Federativa do Brasil, Brasília, 11 fev. 2022. (2022a) Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 02 abr. 2022.

BRASIL. **Lei nº 14.460, de 25 de outubro de 2022.** (2022b) Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7. Acesso em: 02 mar. 2023.

BRASIL, **Decreto nº 11.260, de 22 de novembro de 2022**. Dispõe sobre a elaboração e o encaminhamento da Estratégia Nacional de Governo Digital e prorroga o período de vigência da Estratégia de Governo Digital, instituída pelo Decreto nº 10.332, de 28 de abril de 2020. (2022c) Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11260.htm#:~:text=DECRETO%20N%C2%BA%2011.260%2C%20DE%2022,28%20de%20abril%20de%202020. Acesso em: 10 dez. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Resolução nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. **Diário Oficial da República Federativa do Brasil**, Brasília, 27 fev. 2023a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf. Acesso em: 02 out. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **ANPD publica regulamento de aplicação de sanções administrativas**. ANPD, 28 fev. 2023b. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria#:~:text=O%20Regulamento%20de%20Dosimetria%20e%20Aplica%C3%A7%C3

%A3o%20de%20San%C3%A7%C3%B5es%20Administrativas%20%C3%A9,de%20Prote%C3%A7%C3%A3o%20de%20Dados%20Pessoais. Acesso em: 02 out. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos (MGI). **Última semana para participar da consulta pública sobre Governo Digital**: os interessados em participar podem encaminhar suas sugestões até o dia 12 de janeiro na plataforma brasil participativo. Os interessados em participar podem encaminhar suas sugestões até o dia 12 de janeiro na plataforma Brasil Participativo. 2024a. Disponível em: https://agenciagov.ebc.com.br/noticias/202401/ultima-semana-para-participar-da-consulta-publica-da-estrategia-nacional-de-governo-digital#:~:text=Em%202024%20%2C%20o%20governo%20federal,%C3%A0%20tem%C3%A1tica%20de%20governo%20digital. Acesso em: 24 fev. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos (MGI). **O que é o SEI?**. 2024b. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/processo-eletronico-nacional/conteudo/SEI. Acesso em: 22/03/2024.

BRASIL. Conselho Nacional do Ministério Público (CNMP). **Glossário**. 2024c. Disponível em: https://www.cnmp.mp.br/portal/institucional/476-glossario. Acesso em: 24 fev. 2024.

BRESSER-PEREIRA, L. C. Democracia, Estado Social e Reforma Gerencial. **RAE-Revista de Administração de Empresas**, [S. l.], v. 50, n. 1, p. 112–116, 2010. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rae/article/view/31308. Acesso em: 29 jan. 2023.

CASTELLS, Manuel. **A sociedade em rede**. 3. ed. São Paulo: Paz e Terra, 2000.

CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede: do conhecimento à ação política**; Conferência. Belém (Por) : Imprensa Nacional, 2005.

CAVALIERI, Davi Valdetaro Gomes. Governança de dados e programa de compliance digital na administração pública: contribuições da LGPD para a integridade governamental. In: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020a.

CAVALIERI, Davi Valdetaro Gomes. **O compliance como mecanismo de combate à corrupção**. Fórum Administrativo [recurso eletrônico] : Direito Público. Belo Horizonte, v.20, n.227, jan. 2020b. Disponível em: https://dspace.almg.gov.br/handle/11037/37310. Acesso em: 10 out. 2023.

UNIÃO EUROPEIA. **Convenção Europeia dos Direitos do Homem e Liberdades Fundamentais**. Roma: Conselho da Europa, 1950.

CRESPO, Marcelo. Proteção de Dados Pessoais e o Poder Público: Noções Essenciais. In: CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael (org.). **Lei Geral de Proteção de Dados e o poder público**. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021.

CRESWELL, John W. **Projeto de Pesquisa**: métodos qualitativo, quantitativo e misto. 2. ed. Porto Alegre: Artmed, 2007. Tradução de: Luciana de Oliveira da Rocha.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 29 ed. Rio de Janeiro: Forense, 2016.

FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. **Governança corporativa**: avanços e retrocessos. São Paulo: Quartier Latin, 2007.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: Ana Frazão; Gustavo Tepedino; Milena Oliva (Org). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

FALEIROS JÚNIOR, José Luiz de Moura. Governança de dados e o poder público: perspectivas à luz da lei geral de proteção de dados pessoais. In: CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael (org.). **Lei Geral de Proteção de Dados e o poder público**. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 6. ed. – São Paulo: Atlas, 2017.

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal:** desafios, modelos e principais impactos com a nova Lei. Orientador Prof. Dr. Marcelo Dias Varella. Brasília: UniCEUB, 2019. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/14499/1/61600099.pdf. Acesso em: 27 maio 2022.

HONORIO, Roseli. **Modelo Conceitual de Governança de Dados como suporte à Governança do Conhecimento Organizacional**. 2022. 109 f. Dissertação (Mestrado) - Curso de Pós-Graduação em Engenharia e Gestão do Conhecimento, Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis, 2022. Disponível em: https://repositorio.ufsc.br/handle/123456789/243667. Acesso em: 07 set. 2023.

LEÃO, André Luiz Maranhão de Souza; MELLO, Sérgio Carvalho Benício de; VIEIRA, Ricardo Sérgio Gomes. O papel da teoria no método de pesquisa em Administração. In: LEÃO, André Luiz Maranhão de Souza; PAIVA JÚNIOR, Fernando Gomes de; MELLO, Sérgio Carvalho Benício de (org.). **Abordagens qualitativas na pesquisa em administração**. Recife: Editora UFPE, 2016. Cap. 1. p. 17-35.

LEÃO, Pablo Diego; CATOSSI JUNIOR, Ullisses; NASCIMENTO, Natália Talita Araújo; PASSOS, Rosália Maria; ARENAS, Marlene Valério dos Santos. Governança de dados na administração pública: um levantamento bibliométrico / *data governance in public administration.* ***Brazilian Journal Of Development***, [S.L.], v. 8, n. 4, p. 28072-28087, 19 abr. 2022. *South Florida Publishing LLC*. http://dx.doi.org/10.34117/bjdv8n4-347.

LIMA, Paulo Ricardo Silva; PRESSER, Nadi Helena. **A Lei Geral de Proteção de Dados e os desafios para a gestão nas organizações brasileiras na era do Big Data**. P2P E INOVAÇÃO, Rio de Janeiro, RJ, v. 8, n. 2, p. 109–120, 2022. DOI: 10.21721/p2p.2022v8n2.p109-120. Disponível em: https://revista.ibict.br/p2p/article/view/5918. Acesso em: 15 out. 2023.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. A LGPD e a construção de uma cultura de proteção de dados. **Revista de Direito**, [S.L.], v. 14, n. 01, p. 01-20, 29 jun. 2022. Revista de Direito. Disponível em: http://dx.doi.org/10.32361/2022140113764. Acesso em: 22 mar. 2024.

MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato. **Metodologia de investigação científica para as ciências sociais aplicadas**. São Paulo: Atlas, 2007.

MAGACHO, Bruna Toledo Piza; TRENTO, Melissa. LGPD e compliance na Administração Pública: o Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público? .... **Revista Brasileira de Pesquisas Jurídicas (Brazilian Journal Of Law Research)**, [S.L.], v. 2, n. 2, p. 7-26, 25 maio 2021. Revista Brasileira de Pesquisas Jurídicas. http://dx.doi.org/10.51284/rbpj.02.trento. Disponível em: https://ojs.eduvaleavare.com.br/index.php/rbpj/article/view/30. Acesso em: 17 mar. 2023.

MIRANDA, Marcelo Barça Alvez de. **Proteção post-mortem envolvendo os direitos da personalidade**. Jusbrasil, 2004. Disponível em: https://www.jusbrasil.com.br/artigos/protecao-post-mortem-envolvendo-os-direitos-da-personalidade/121944063. Acesso em: 12 fev. 2024.

MIRANDA, Rodrigo Fontenelle de A. **Implementando a gestão de riscos no setor público**. Belo Horizonte: Fórum, 2017.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. **Em Questão**, Porto Alegre, v. 29, p. 127314, 2023. DOI: 10.1590/1808-5245.29.127314. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/127314. Acesso em: 7 dez. 2023.

NARDES, João Augusto Ribeiro; ALTOUNIAN, Cláudio Sarian e VIEIRA, Luis Afonso Gomes. **Governança Pública: o desafio do Brasil**. 3 ed. revista e atualizada. Belo Horizonte: Fórum, 2018.

PAES, Marilena Leite. **Arquivo**: teoria e prática. Rio de Janeiro: Editora FGV, 2004.

PETERS, Brainard Guy. O que é Governança? **Revista do TCU**, Brasília, v. 1, n. 127, p. 29-33, 01 maio 2013. Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/87. Acesso em: 20 ago. 2023.

SANTOS, Matheus Henrique de Souza. **Aspectos da Governança Digital da Administração Pública Federal do Brasil sob a Luz das Orientações da OCDE**. Revista tempo do mundo. n. 25. abr. 2021. Disponível em: http://dx.doi.org/10.38116/rtm25art12. Acesso em: 27 maio 2022.

SILVA, Bárbara Stephany de Souza. **O impacto da LGPD no desenho da política de governança de dados nos municípios**: o caso de belo horizonte. 2021. 60 f. Dissertação (Mestrado) - Curso de Mestrado em Políticas Públicas e Governo, Fundação Getúlio Vargas, Brasília, 2021. Disponível em: https://hdl.handle.net/10438/31853. Acesso em: 17 mar. 2023.

TAPSCOTT, Don. WILLIAMS, Anthony D. **Wikinomics: como a colaboração em massa pode mudar o seu negócio**. Tradução Marcello Lino. Título original: Wikinomics. Rio de Janeiro: Editora Nova Fronteira S.A, 2006.

PEREIRA, Raiane Nayara Silva. **A gestão da educação superior no contexto dos sistemas de informações gerenciais: uma abordagem sociotécnica**. 2022. 97 f. Dissertação (Mestrado) - Curso de Mestrado em em Políticas Públicas, Gestão e Avaliação da Educação Superior, Universidade Federal da Paraíba, João Pessoa: 2022. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/24027. Acesso em: 17 mar. 2023.

EU General Data Protection Regulation (EU-GDPR). **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 10 mar 2023.

RODRIGUES, Cristina Barbosa; CAMMAROSANO, Flávia Giorgini Fusco. Governança Digital. **Revista de Direito Internacional e Globalização Econômica**, [S.L.], v. 9, n. 9, p. 198-219, 17 set. 2022. Pontifical Catholic University of Sao Paulo (PUC-SP). http://dx.doi.org/10.23925/2526-6284/2022.v9n9.58939.

SARAIVA, André. **A implementação do SEI – Sistema Eletrônico de Informações**. ENAP – Casoteca de Gestão Pública, 2018. Disponível em: https://repositorio.enap.gov.br/bitstream/1/3455/4/SEGES%20%20Enap.%20SARAIVA%20Andr%C3%A9.%20SEI.%20estudo%20de%20caso.%202018.%20portug%C3%AAs.pdf. Acesso em: 20 jan. 2024.

TENÓRIO FILHO, Luiz; FERREIRA, Pollyana Cassia Gonzaga; MOTA, Francisca Rosaline Leite; SOUZA, Edivanio Duarte de. **Os desafios da implementação da Lei Geral de Proteção de Dados nas Universidades Públicas Federais** d. In: Encontro Nacional de Pesquisa em Ciência da Informação, 21., 2021, Rio de Janeiro. Artigo. Rio de Janeiro: Ancib, 2021. p. 1-11. Disponível em: https://enancib.ancib.org/index.php/enancib/xxienancib/paper/viewFile/456/346. Acesso em: 05 jan. 2023.

UFRPE. Universidade Federal Rural de Pernambuco. Administração Superior. **Plano de Desenvolvimento Institucional – UFRPE: 2013-2020**. UFRPE. Recife: UFRPE, 2013. Disponível em: http://www.proplan.ufrpe.br/br/node/561. Acesso em: 02 dez. 2023.

UFRPE. Universidade Federal Rural de Pernambuco. Conselho Universitário. **Resolução nº 031/2020, de 11 de agosto de 2020** [2020a]. Recife: UFRPE, 2020. Disponível em: http://www.acessoainformacao.ufrpe.br/sites/ww2.acessoainformacao.ufrpe.br/files/Resolu%C3%A7%C3%A3o%2031-2020%20-%20divulga%C3%A7%C3%A3o%20de%20documentos%20%28LGPD%29.pdf. Acesso em: 27 maio 2022.

UFRPE. Universidade Federal Rural de Pernambuco. **UFRPE divulga orientações sobre o Sistema Integrado de Patrimônio, Administração e Contratos (SIPAC)** [2020b]. Disponível em: https://www.ufrpe.br/br/content/ufrpe-divulga-orienta%C3%A7%C3%B5es-sobre-sistema-integrado-de-patrim%C3%B4nio-administra%C3%A7%C3%A3o-e-contratos. Acesso em: 27 nov. 2023.

UFRPE. Universidade Federal Rural de Pernambuco. **UFRPE inicia Sistema Integrado de Patrimônio, Administração e Contratos (SIPAC) no dia 27/04** [2020c]. Disponível em: https://www.ufrpe.br/br/content/ufrpe-inicia-sistema-integrado-de-patrim%C3%B4nio-administra%C3%A7%C3%A3o-e-contratos-sipac-no-dia-2704. Acesso em: 27 nov. 2023.

UFRPE. Universidade Federal Rural de Pernambuco. **Processo Eletrônico** [2020d]. Disponível em: https://ufrpe.br/br/processoeletronico. Acesso em: 27 nov. 2023.

UFRPE. Universidade Federal Rural de Pernambuco. Pró-reitora de Planejamento e Desenvolvimento Institucional. **Plano de Desenvolvimento Institucional – UFRPE: 2021-2030**. UFRPE. PROPLAN. - Recife: UFRPE, 2021a. Disponível em: http://www.proplan.ufrpe.br/br/node/561. Acesso em: 13 dez 2023.

UFRPE. Universidade Federal Rural de Pernambuco. **Relatório de Gestão do exercício 2020.** UFRPE. Recife: UFRPE, 2021b. Disponível em: http://ww2.proplan.ufrpe.br/sites/ww2.proplan.ufrpe.br/files/RG%202020_UFRPE%2011_03_21%202.pdf. Acesso em: 13 jan 2024.

UFRPE. Universidade Federal Rural de Pernambuco. **Cartilha LGPD**: o que é e para que serve. [2021c]. In: Emerson Marinho Pedrosa (Org). Recife, EDUFRPE, 2021. Disponível em: http://www.editora.ufrpe.br/cartilha_LGPD. Acesso em: 28 abr. 2023.

UFRPE. Universidade Federal Rural de Pernambuco. [#] **O que é SIPAC?** [2022]. Disponível em: https://servicosdigitais.ufrpe.br/help/pt-br/10-sipac/19-o-que-e-sipac. Acesso em: 27 nov. 2023.

UFRPE. **Como tornar um documento ostensivo em restrito?** 2023. Disponível em: https://ajuda.ufrpe.br/article/como-tornar-um-documento-ostensivo-em-restrito. Acesso em: 16 ago. 2023.

APÊNDICE A – ROTEIRO DO QUESTIONÁRIO

Consulta nas Universidades Públicas Federais do Nordeste a fim de identificar o cenário de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) dos processos administrativos eletrônico, como parte da metodologia da pesquisa de dissertação intitulada "PROTEÇÃO DE DADOS PESSOAIS: um estudo sobre a proteção de dados pessoais nos processos eletrônicos de uma Instituição Pública Federal (2020-2022)", do programa Mestrado em Gestão Pública para o Desenvolvimento do Nordeste/UFPE.

QUESTIONÁRIO

QUANTO AO SISTEMA DE PROCESSO ADMINISTRATIVO ELETRÔNICO

1. **A instituição já utiliza o processo eletrônico para tramitação dos processos administrativos, conforme previsto no Decreto 8.539/2015?**

( ) Sim
( ) Não
( ) Parcialmente

2. **Caso a resposta anterior tenha sido "sim" ou "parcialmente", qual(is) o(s) sistema(s) adotado(s) pela Instituição?**

( ) SIPAC
( ) SUAP
( ) SEI
( ) Outro (especifique):

3. **Informe o ano de implantação do sistema de processo eletrônico na Instituição?**

_____

4. **Foi realizada alguma customização do sistema adquirido para atender o Regimento Interno, Rotina Administrativa e/ou alguma necessidade específica da Instituição?**

( ) Sim
( ) Não
( ) Outro (especifique):_____

QUANTO ÀS PERMISSÕES DOS USUÁRIOS E À NATUREZA DO ASSUNTO NO SISTEMA DE PROCESSO ELETRÔNICO

5. **Quais usuários/unidades têm permissão para realizar abertura de processo administrativo eletrônico?**

( ) Apenas os servidores dos setores de Protocolo, a abertura é centralizada no setor de protocolo
( ) Qualquer servidor ativo da Instituição, independente da unidade de lotação
( ) Outro (especifique):

6. **No sistema de processo eletrônico há um recurso para indicar a natureza do documento/processo entre Ostensivo, Restrito e Sigiloso?**

Descrição: considere **Ostensivo**: cujo teor deve ser do conhecimento do público em geral e ficará disponível para consulta na área pública do sistema; **Restrito**: cujo teor não deve ser do conhecimento do público em

geral, sendo acessados apenas pelas unidades nas quais são tramitados, interessados e assinantes; **Sigiloso**: que requer rigorosas medidas de segurança, cujo teor deve ser, exclusivamente, do conhecimento de pessoas credenciadas.

( ) Sim
( ) Não

7. **Caso a resposta anterior tenha sido "sim", o usuário precisa justificar ou indicar alguma previsão legal para o cadastro de documentos registros/sigilosos no sistema?**

( ) Sim
( ) Não

8. **Quando há um erro na indicação da natureza do documento, o sistema permite a correção?**
   Exemplo: se o documento foi cadastrado no processo com a natureza de assunto pública, é possível corrigir a natureza para restrita/sigilosa após inclusão/ativação/assinatura do documento?

( ) Sim
( ) Não
( ) Outro (especifique):

9. **Caso a resposta anterior tenha sido "sim", essa permissão é habilitada para quais usuários:**

( ) Usuário assinante do documento
( ) Chefe de setor de origem do documento
( ) Servidores lotados no Protocolo, independente do setor e assinante do documento
( ) Qualquer usuário do setor de origem do documento
( ) Não se aplica
( ) Outro (especifique):

QUANTO À GOVERNANÇA

10. **A adequação dos serviços da instituição à Lei Geral de Proteção de Dados (LGPD) está prevista no Plano de Desenvolvimento Institucional (PDI) vigente?**

( ) Sim
( ) Não
( ) Outro (especifique):
*Se positivo, qual a previsão para conclusão da adequação?

11. **Há comitê/comissão responsável pela implantação da LGPD na Instituição?**

( ) Sim
( ) Não

12. **Há portaria de designação de Encarregado pelo tratamento de dados pessoais?**

( ) Sim
( ) Não

QUANTO À PROTEÇÃO DE DADOS PESSOAIS

13. **Há algum instrumento institucional que regulamenta a proteção de dados pessoais no âmbito do sistema de Processo Eletrônico da Instituição?**
    Exemplo: manual/portaria interna/resolução/outros

( ) Sim
( ) Não

( ) Outro (especifique):

14. **Há algum instrumento norteador institucional para registro de incidentes de exposição e vazamento de dados pessoais provenientes de documentos eletrônicos publicados em Processos Eletrônicos na Instituição?**
    Exemplo: manual/portaria interna/resolução/outros

( ) Sim
( ) Não
( ) Outro (especifique):

15. **A Instituição realizou adequação de documentos (requerimento padrão, formulários internos, etc) para atender de forma mais eficaz os princípios da LGPD?**

( ) Sim
( ) Não
( ) Outro (especifique):

QUANTO À CAPACITAÇÃO DOS SERVIDORES

16. **A instituição promoveu curso de capacitação referente à Proteção de Dados Pessoais?**

( ) Sim
( ) Não

17. **A instituição promoveu palestras e/ou outras ações voltadas à divulgação da Proteção de Dados Pessoais e Sensíveis?**

( ) Sim
( ) Não
( ) Outro (especifique):

APÊNDICE B - SUGESTÃO DE EMENTA DE CURSO CAPACITAÇÃO

Curso prático de Proteção de Dados Pessoais na UFRPE

1. EMENTA:
Aborda a Lei de Acesso à Informação (LAI), Lei Geral de Proteção de Dados (LGPD), Resolução CONSU/UFRPE Nº 103/2021, Resolução Nº 031/2020 CONSU/UFRPE e Orientação Conjunta nº 1/2021/ME/CGU no contexto dos processos eletrônicos da UFRPE.

2. CARGA HORÁRIA: 20 horas.

3. OBJETIVOS:
3.1 Objetivo geral:
Capacitar os servidores da UFRPE na compreensão e aplicação prática dos princípios e normas transparência ativa e da proteção de dados pessoais no âmbito da UFRPE.

3.2 Objetivos Específicos:

- Apresentar as legislações de transparência e proteção de dados pessoais no escopo da UFRPE;
- Promover boas práticas no tratamento de dados.

4. CONTEÚDO:
Módulo 1 - Introdução à Proteção de Dados Pessoais:

- Conceitos fundamentais de dados pessoais, sensíveis e tratamento de dados.
- Contextualização da importância da proteção de dados na UFRPE.

Módulo 2 - Legislação Aplicável:

- Lei de Acesso à Informação (LAI): transparência e restrição de informações pessoais.
- Lei Geral de Proteção de Dados (LGPD): fundamentos, princípios e diretrizes para a Administração Pública.

Módulo 3 - Proteção de Dados Pessoais em Processo Administrativo Eletrônico:

- Análise Orientação Conjunta nº 1/2021/ME/CGU.
- Análise das resoluções da instituição, incluindo diretrizes e procedimentos específicos.
- Cadastro da Natureza do Documento no SIPAC.

Módulo 4 - Gestão de Dados Pessoais na UFRPE:

- Processos de coleta, armazenamento, tratamento e compartilhamento de dados pessoais na UFRPE.
- Boas práticas de gestão de dados e segurança da informação.

Módulo 5 - Atividades Práticas:

- Identificação e mitigação de riscos de não conformidade.

- Análise de casos reais e situações hipotéticas relacionadas à proteção de dados na UFRPE.

5. METODOLOGIA:
O curso será realizado na modalidade a distância, com encontros síncronos, utilizando estudos de caso, exercícios práticos, discussões em grupo e simulações de situações reais para promover a aplicação dos conceitos teóricos da proteção de dados pessoais na rotina institucional.

6. PÚBLICO-ALVO:
Servidores da UFRPE.

7. AVALIAÇÃO:
A partir da participação nas aulas e atividades proposta.

8. CERTIFICAÇÃO:
O certificado será emitido pela PROGEPE. Para obtenção do certificado, o cursista deverá ter participação igual ou superior a 75% no curso, que será avaliada através de:

- Frequência nos encontros síncronos;
- Participação nas atividades propostas;

9. REFERÊNCIAS

BRASIL. Comitê Central de Governança de Dados. **Guia De Boas Práticas Lei Geral de Proteção De Dados (LGPD)**, de 14 de ago. de 2020. Brasília: 14 ago. 2020c. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 02 fev. 2024.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 03 fev. 2024.

BRASIL. **Decreto nº 8.539, de 8 de outubro de 2015**. Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. **Diário Oficial da República Federativa do Brasil**, Brasília, 9 out. 2015. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8539.htm>. Acesso em: 04 dez. 2023.

BRASIL, **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm. Acesso em: 02 abr. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 abr. 2022.

BRASIL. Ministério da Economia e Controladoria Geral da União. **Orientação Conjunta nº 1/2021/ME/CGU**. Transparência no Processo Administrativo Eletrônico. Brasília: 24 mar. 2021. Disponível em: https://www.gov.br/mcom/pt-br/acesso-a-informacao/processo-eletronico/OrientaoConjunta_01_2021_ME_CGU.pdf. Acesso em: 01 mar. 2023.

UFRPE. Universidade Federal Rural de Pernambuco. Conselho Universitário. **Resolução nº 031/2020, de 11 de agosto de 2020** [2020]. Recife: UFRPE, 2020. Disponível em: http://www.acessoainformacao.ufrpe.br/sites/ww2.acessoainformacao.ufrpe.br/files/Resolu%C3%A7%C3%A3o%2031-2020%20-%20divulga%C3%A7%C3%A3o%20de%20documentos%20%28LGPD%29.pdf. Acesso em: 27 maio 2022.

UFRPE. Universidade Federal Rural de Pernambuco. Conselho Universitário. **Resolução nº 103/2021, de 14 de junho de 2021** [2021]. Recife: UFRPE, 2021. Disponível em: http://seg.ufrpe.br/content/res-no-1032021. Acesso em: 10 fev. 2024.

APÊNDICE C - TIPOS DE DOCUMENTOS PARA RESTRIÇÃO DE ACESSO

Relação dos documentos que possuem “Visualização Pública Permitida” que poderiam constar previamente com “Visualização Pública Bloqueada”:

Denominação
ATESTADO MÉDICO
AUTODECLARAÇÃO DE SAÚDE
AUXÍLIO-NATALIDADE/DEPENDENTES PARA IMPOSTO DE RENDA
AVALIAÇÃO DE CAPACIDADE FÍSICA
AVALIAÇÃO DE CAPACIDADE LABORATIVA
AVALIAÇÃO DE SAÚDE OCUPACIONAL
AVALIAÇÃO MÉDICA
CERTIDÃO DE CASAMENTO
CERTIDÃO DE NASCIMENTO
CERTIDÃO DE ÓBITO
CERTIDÃO DE REGULARIDADE DO FGTS
CERTIDÃO DE TEMPO DE SERVIÇO
CERTIDÃO TRABALHISTA
COMPROVANTE DE RESIDÊNCIA
CONTRACHEQUE
CÓPIA DE CERTIFICADO INTERNACIONAL DE VACINAÇÃO
CÓPIA DE CNH
CÓPIA DE CPF
CÓPIA DE IDENTIDADE
CÓPIA DE PASSAPORTE CARIMBADO
COPIA DE TÍTULO DE ELEITOR
CÓPIA DO DOCUMENTO MILITAR
DECLARAÇÃO DE BENS
DECLARAÇÃO DE DEPENDÊNCIA ECONÔMICA
DECLARAÇÃO DE IMPOSTO DE RENDA
DECLARAÇÃO DE UNIÃO ESTÁVEL
DECLARAÇÃO SOCIOECONÔMICA
EXAME MÉDICO
FICHA DE IDENTIFICAÇÃO
FICHA DE INSCRIÇÃO
LAUDO MÉDICO
REGISTRO DE NASCIMENTO