



**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO PÚBLICA**



NATHAN DOS SANTOS KUSTER PINHEIRO

**APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 NOS REGISTROS
DE PROCEDIMENTOS DISCIPLINARES RELATIVOS A SERVIDORES LOTADOS
NA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO - UFES.**

VITÓRIA - ES
2023



**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO PÚBLICA**



NATHAN DOS SANTOS KUSTER PINHEIRO

**APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 NOS REGISTROS
DE PROCEDIMENTOS DISCIPLINARES RELATIVOS A SERVIDORES LOTADOS
NA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO - UFES.**

Dissertação apresentada ao Programa de Pós-graduação em Gestão Pública da Universidade Federal do Espírito Santo, para defesa, como um dos requisitos para a obtenção do grau de Mestre em Gestão Pública.

Orientadora: Prof. Dra. Margareth Vetis Zaganelli

VITÓRIA - ES

2023

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

P654a Pinheiro, Nathan dos Santos Kuster, 1993-
Aplicação da Lei nº 13.709, de 14 de agosto de 2018 nos registros de procedimentos disciplinares relativos a servidores lotados na Universidade Federal do Espírito Santo - UFES / Nathan dos Santos Kuster Pinheiro. - 2023.
73 f. : il.

Orientadora: Margareth Vetis Zaganelli.
Dissertação (Mestrado Profissional em Gestão Pública) - Universidade Federal do Espírito Santo, Centro de Ciências Jurídicas e Econômicas.

1. Proteção de dados. 2. Responsabilidade administrativa. 3. Banco de dados - Medidas de segurança. 4. Procedimento administrativo. I. Zaganelli, Margareth Vetis. II. Universidade Federal do Espírito Santo. Centro de Ciências Jurídicas e Econômicas. III. Título.

CDU: 35



UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO PÚBLICA



NATHAN DOS SANTOS KUSTER PINHEIRO

**APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 NOS REGISTROS
DE PROCEDIMENTOS DISCIPLINARES RELATIVOS A SERVIDORES LOTADOS
NA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO - UFES.**

Dissertação apresentada ao Programa de Pós-graduação em Gestão Pública da Universidade Federal do Espírito Santo, para defesa, como um dos requisitos para a obtenção do grau de Mestre em Gestão Pública.

COMISSÃO EXAMINADORA

Prof. Dra. Margareth Vetis Zaganelli

Orientadora

BRUNO GOMES
BORGES DA
FONSECA:07104794760

Assinado de forma digital por
BRUNO GOMES BORGES DA
FONSECA:07104794760
Dados: 2023.03.27 15:24:18 -03'00'

Prof. Dr. Bruno Gomes Borges da Fonseca
Membro interno

Prof. Dra. Miriam Coutinho de Faria Alves

Membro externo

À minha esposa, com amor.

AGRADECIMENTOS

A Deus, Supremo Benfeitor, amigo fiel e justo, que moveu todas as coisas para que hoje eu pudesse concluir essa etapa. A Ele sou eternamente grato.

À minha esposa, Rayanne, companheira de vida que o próprio Criador me concedeu, que me motivou em cada momento da jornada, com carinho, sorrisos e orações. Mais um objetivo que alcançamos juntos. Te amo.

Aos meus pais, por me ensinarem desde cedo os valores da honra, da ética e do saber. À minha irmã por todo auxílio prestado, principalmente na fase final da pesquisa.

À minha orientadora, Professora Dra. Margareth Vetis Zaganelli, que acreditou no potencial da minha proposta e me municiou com informações fundamentais para o desenvolvimento deste trabalho. Sempre acessível e atenciosa, a ela agradeço por todo empenho e dedicação. Aos Professores que se dispuseram a participar dos atos de qualificação e defesa desta pesquisa, Dr. Bruno Gomes Borges da Fonseca, Dra. Marilene Olivier Ferreira de Oliveira e Dra. Miriam Coutinho de Faria Alves. A estes sou grato pela pronta disponibilidade e pelos conselhos que muito contribuíram para o desenvolvimento e conclusão desta dissertação.

Ao Programa de Pós Graduação em Gestão Pública da Ufes, pela oportunidade concedida e pelo aprendizado através das aulas e trabalhos e pelas ferramentas oferecidas.

Ao querido amigo e primo, Eloy Paste Junior, por cada palavra de incentivo, pelas orações e conselhos que levarei para toda a vida.

RESUMO

PINHEIRO, Nathan dos Santos Kuster. **APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 NOS REGISTROS DE PROCEDIMENTOS DISCIPLINARES RELATIVOS A SERVIDORES LOTADOS NA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO - UFES.** 2023. 73 f. Dissertação de Mestrado Profissional em Gestão Pública – Universidade Federal do Espírito Santo, Vitória, 2023.

As Universidades Federais, na condição de órgãos públicos de relevante atuação nos cenários científico e social do Brasil, precisam se adequar a uma série de legislações específicas, dentre essas a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709, de 14 de agosto de 2018). Tal normativa traz um conjunto de mecanismos e conceitos cuja aplicação é de fundamental importância para a correta manipulação de tais dados. Em meio a todos os debates nas esferas pública e privada, aplicar padrões de segurança para os dados armazenados torna-se algo primordial, exigindo-se investimentos em capacitação dos colaboradores, *softwares*, implantação de políticas e práticas, objetivando minimização dos riscos de vazamentos de informações. **O problema**, em se tratando dos dados produzidos e armazenados nos servidores virtuais e computadores da Universidade Federal do Espírito Santo, se mostra no fato de não se saber ao certo quais níveis de segurança são aplicados para acesso, manipulação, divulgação e exclusão desses elementos, especificamente no que diz respeito aos procedimentos disciplinares. Logo, o **objetivo geral** é analisar a aplicação da Lei Geral de Proteção de Dados Pessoais nos registros de dados em Procedimentos Disciplinares da Ufes. O **aporte teórico** foi focado nos conceitos trazidos pela Lei nº 13.709/2018, principalmente no que se refere a dados pessoais, no contexto de atuação dos servidores técnicos da Ufes, na condição de geradores de dados e no advento da LGPD, levando-se em conta os desafios de sua implantação e aperfeiçoamento ao longo do tempo. Como **procedimentos metodológicos**, o estudo em tela se valerá de análise de dados levantados via consulta aos sítios eletrônicos e documentos relacionados às investigações administrativas em face de servidores, bem como análise de artigos científicos e livros publicados sobre o tema analisado. O **resultado** esperado é o apontamento de precariedades no tratamento de dados pessoais nos aludidos registros da Ufes, em virtude da pouca divulgação do tema na comunidade acadêmica dessa instituição até a presente data. Consoante tais informações, como **produto tecnológico** elaborou-se um manual de boas práticas para aplicação da LGPD no âmbito da Universidade Federal do Espírito Santo, atentando para as exigências da legislação ora analisada, nas responsabilidades dos servidores envolvidos e com sugestões de uso quanto aos procedimentos disciplinares.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais. Responsabilidade administrativa de Registros públicos. Lei de Acesso à Informação. Segurança da Informação. Procedimento disciplinar.

ABSTRACT

PINHEIRO, Nathan dos Santos Kuster. **Application of Law no. 13.709, of august 14, 2018 in the records of disciplinary procedures related to servants located at the Federal University of Espírito Santo - UFES.** 2023. Dissertation Project (Professional Master's in Public Management) – Federal University of Espírito Santo, Vitória, 2022.

Federal Universities, as public bodies with a relevant role in the scientific and social scenarios of Brazil, need to adapt to a series of specific legislations, among them the General Law for the Protection of Personal Data (LGPD) (Law nº 13.709, of 14 August 2018). This regulation brings a set of mechanisms and concepts whose application is of fundamental importance for the correct handling of such data. Amidst all the debates in the public and private spheres, applying security standards for stored data becomes paramount, requiring investments in employee training, software, implementation of policies and practices, with the aim of minimizing the risks of data leaks. information. The problem, when it comes to the data produced and stored on the virtual servers and computers of the Federal University of Espírito Santo, is shown in the fact that it is not known for sure which levels of security are applied for access, manipulation, disclosure and exclusion of these elements, specifically with regard to disciplinary procedures. Therefore, the general objective is to analyze the application of the General Law for the Protection of Personal Data in data records in Disciplinary Procedures of Ufes. The theoretical contribution was focused on the concepts brought by Law nº 13.709/2018, mainly with regard to personal data, in the context of performance of the technical servers of Ufes, as data generators and in the advent of the LGPD, taking into account takes into account the challenges of its implementation and improvement over time. As methodological procedures, the study on screen will make use of analysis of data collected via consultation to electronic sites and documents related to administrative investigations in the face of servers, as well as analysis of scientific articles and books published on the subject analyzed. The expected result is the indication of precariousness in the processing of personal data in the aforementioned Ufes records, due to the lack of dissemination of the subject in the academic community of that institution to date. Based on this information, as a technological product, a manual of good practices was prepared for the application of the LGPD within the scope of the Federal University of Espírito Santo, paying attention to the requirements of the legislation analyzed here, the responsibilities of the servers involved and with suggestions for use regarding the procedures disciplinary.

Keywords: General Personal Data Protection Law. Administrative responsibility for public records. Freedom of Information Act. Information security. Disciplinary procedure.

LISTA DE FIGURAS

Figura 1 – Esquematização geral da pesquisa.....	25
Figura 2 – Objetivos.....	42
Figura 3 – Tela inicial da plataforma Lepisma.....	51
Figura 4 – Inserção de peças na plataforma Lepisma.....	53
Figura 5 – Aba “consulta” e opções de busca.....	53
Figura 6 – Opção de busca “vocabulário controlado”.....	54

LISTA DE QUADROS

Quadro 1 – Matriz de amarração.....	43
Quadro 2 – Fontes e natureza dos dados.....	45
Quadro 3 – Coleta e forma de tratamento dos dados.....	46

LISTA DE TABELAS

Tabela 1 – Dados pessoais e sensíveis da UFRGS.....	40
--	----

LISTA DE SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

CGU – Controladoria Geral da União

CPF – Cadastro de Pessoa Física

CR – Constituição da República

DAP – Diretoria de Administração de Pessoal

DCOS – Diretoria de Contratações de Obras e Serviços

DDI - Diretoria de Documentação Institucional

DOU – Diário Oficial da União

Ferpa – Family Educational Rights and Privacy Act

GDPR – General Data Protection Regulation

IFES – Instituições Federais de Ensino

ITS – Instituto de Tecnologia e Sociedade

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

MEC – Ministério da Educação

MPF – Ministério Público Federal

NBR - Norma Brasileira

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

PDF - Portable Document Format

PDI – PLANO DE DESENVOLVIMENTO INSTITUCIONAL

PPGGP – Pós-graduação em Gestão Pública

PROAD – Pró-Reitoria de Administração

PROAECI - Pró-Reitoria de Assuntos Estudantis e Cidadania

PROEX - Pró-Reitoria de Extensão

Progep – Pró-reitoria de Gestão de Pessoas

PROGRAD - Pró-Reitoria de Graduação

PROPLAN - Pró-Reitoria de Planejamento e Desenvolvimento Institucional

RG – Registro Geral

SERPRO – Serviço Federal de Processamento de Dados

SGSI – Sistema de Gestão de Segurança da Informação

SPD – Seção de Procedimentos Disciplinares

STI – Superintendência de Tecnologia da Informação

TCU – Tribunal de Contas da União

UFBA – Universidade Federal da Bahia

Ufes – Universidade Federal do Espírito Santo

UFF – Universidade Federal Fluminense

UFMG – Universidade Federal de Minas Gerais

UFPE – Universidade Federal de Pernambuco

UFRGS – Universidade Federal do Rio Grande do Sul

UFRJ – Universidade Federal do Rio de Janeiro

UFRN – Universidade Federal do Rio Grande do Norte

SUMÁRIO

1	CONSIDERAÇÕES INICIAIS.....	13
1.1	PERCURSO ACADÊMICO E PROFISSIONAL.....	13
1.2	TEMA.....	14
1.3	CONCEITOS BÁSICOS.....	16
1.4	CONTEXTO E PROBLEMA.....	17
1.5	OBJETIVOS.....	20
1.6	PRODUTO TÉCNICO ESPERADO.....	20
1.7	LINHA DE PESQUISA E PROJETO ESTRUTURANTE.....	21
1.8	ALINHAMENTO AO PLANO DE DESENVOLVIMENTO INSTITUCIONAL (PDI) DA UFES.....	21
1.9	JUSTIFICATIVA.....	22
1.10	ESTRUTURA GERAL DA PESQUISA.....	25
2	APORTE TEÓRICO.....	27
2.1.	ABORDAGEM DO TEMA NO SETOR PÚBLICO.....	27
2.2	TEORIAS ASSOCIADAS AO TEMA.....	30
2.3	TRABALHOS CORRELATOS AO OBJETO DA PESQUISA.....	37
3	MÉTODOS E PROCEDIMENTOS.....	42
3.1	ABORDAGEM E TIPO DE PESQUISA.....	44
3.2	FONTE E NATUREZA DE DADOS.....	44
3.3	INSTRUMENTOS DE COLETA DE DADOS.....	47
3.4	FORMA DE TRATAMENTO DE DADOS PRETENDIDA.....	47
4	ANÁLISE E DISCUSSÃO DAS INFORMAÇÕES.....	48
4.1	A INSTITUIÇÃO PESQUISADA.....	48
4.2	MANUAIS E DOCUMENTOS ANALISADOS.....	49
4.3	PLATAFORMA LEPISMA.....	50
4.4	RESULTADOS.....	56
5	CONSIDERAÇÕES FINAIS.....	59

1. CONSIDERAÇÕES INICIAIS

1.1. PERCURSO ACADÊMICO E PROFISSIONAL

O pesquisador, atualmente, é servidor público federal desde setembro de 2018, atuando junto à Superintendência de Infraestrutura (antiga Prefeitura Universitária) da Universidade Federal do Espírito Santo (Ufes), lotado na Divisão de Gestão Administrativa. O exercício do cargo lhe proporciona interação com grande número de colaboradores e setores da instituição, inclusive com dados pessoais.

Antes de atuar como servidor, tendo em vista sua formação acadêmica em Direito, exerceu a advocacia em algumas demandas específicas, uma delas num caso de vazamento de dados pessoais envolvendo instituições bancárias, sendo que sua cliente foi vítima de golpistas que usaram informações para emissão de vários cartões de crédito, realizando uma série de compras *online*.

Durante a audiência no Juizado Especial Cível, a magistrada, ao ouvir a fala do hoje pesquisador explicando o caso e o pedido da parte autora, mostrou-se revoltada com a situação de modo geral, visto que também já havia sofrido dano com algo similar, fazendo uma espécie de desabafo em meio ao ato público. De certo modo, todos que acompanhavam a audiência balançavam as cabeças, confirmando as falas da juíza, como se tivessem plena ciência do sentimento expressado ali.

Dessa forma, ciente dos danos que o mau uso dessas informações pode causar e com o advento da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto 2018, julgou ser fundamental que se investigue se essa legislação tem sido observada nos procedimentos internos da Ufes, analisando se os servidores técnicos possuem ferramentas para operacionalizar as exigências do texto legal e suas implicações.

A Lei nº 13.709/2018 é a normatização, em nível federal, acerca da necessidade de tratamento de informações pessoais armazenadas em bancos de dados, sejam eles públicos ou privados. Embora seja uma diretriz relativamente recente, a abordagem das questões de dados já acontece há alguns anos e permeia o arcabouço legislativo do país. Destacam-se nesse aspecto a Lei nº 12.527, de 18 de novembro

de 2011, conhecida por Lei de Acesso à Informação (LAI) e a Lei nº 12.965, de 23 de abril de 2014, nomeada como Marco Civil da Internet (MCI).

No caso da Ufes, é de conhecimento interno que há outros servidores com acesso a informações desse caráter, seja no mesmo setor ou em outros, inclusive com maior quantidade de dados acessíveis para essas pessoas. O advento da LGPD trouxe grandes desafios e preocupações à época da sua promulgação. Esse modelo de regulação estatal se mostrou necessário em virtude das novas demandas que a sociedade desenvolveu nas suas relações.

O grau de comprometimento dos entes públicos se eleva com a aplicação da LGPD, quando se compara com a situação imposta pela Lei de Acesso à Informação (LAI), visto que esta lidava com dados já disponíveis à Administração Pública, sendo necessário dar a devida publicidade, enquanto aquela exige, agora, uma extensa gama de mecanismos de tratamento de dados que fogem da esfera habitual de atuação do poder público (PUGLIESI, 2020).

A digitalização dos procedimentos adotados pelos órgãos públicos é uma realidade. Não raro depara-se com uma série de atividades disponibilizadas pelos canais digitais das prefeituras, tribunais, instituições financeiras, dentre outros órgãos, como abertura de processos, protocolização e juntada de documentos, consulta de informações, marcação de consultas médicas e transações comerciais diversas.

1.2. TEMA

A jovem democracia brasileira sofre com a baixa credibilidade que muitos órgãos públicos apresentam perante a sociedade. Isso, obviamente, se aplica a instituições ligadas aos três poderes, em todas as esferas. Fatores como as altas tributações, elevados índices de corrupção e demora excessiva na prestação de serviços básicos figuram entre as razões desse sentimento generalizado.

A ausência de mecanismos práticos para execução daquilo que é demandado pelo povo, resulta numa enxurrada de processos judiciais, requerendo vagas em escolas e creches, tratamentos médicos, ressarcimentos por danos diversos, dentre outros tipos de lesões sofridas pela ausência de condutas que o texto constitucional

garante aos cidadãos, mas que os entes da federação costumeiramente falham em prover.

No que diz respeito às demandas do Poder Legislativo, há um fator peculiar em território brasileiro, designado por uma expressão popular que é: ‘essa lei não ‘pegou’’, numa alusão à falta de executoriedade de uma determinada norma jurídica, por razões diversas. Seja pela falta de agentes fiscalizadores para fazer cumprir o comando legal, por falta de recursos para bancar a estrutura necessária ou pelo conflito com outras normas pré-existentes, a presença do Estado para fazer valer as suas decisões fica prejudicada num cenário como esse. O governo edita a legislação, mas não tem condições imediatas de colocá-la em prática ou leva tanto tempo para fazê-lo que a situação se regulou por outros meios. A LGPD, nesse contexto, tornou-se um fantasma normativo, assombrando pessoas físicas e jurídicas, baseado numa punição severa que se manifestaria assim que o aparato estatal estivesse montado, sendo que isso se agravou no contexto da pandemia de Covid-19:

É preciso notar, por escrúpulo de equidade, que uma lei de dados é há anos necessária para o Brasil pelos motivos que todos estamos cansados de ler e não precisamos gastar rios de tinta para reproduzir. A nossa crítica é e sempre foi às suas severas inconsistências e o retardo do Executivo na criação do regulador que, combinados, geram um severo custo regulatório, sobretudo na maior crise de saúde dos últimos 100 anos (BECKER ET AL., 2020).

Fato é que os anos passaram desde a edição da Lei Geral de Proteção de Dados Pessoais e a vida da população foi mergulhada no meio virtual, em escala exponencial. Hoje o Brasil é o sétimo líder mundial em governo digital, alcançando mais de 115 milhões de cidadãos, via plataforma Gov.br, por meio da qual há acesso a vários serviços e documentos pessoais.

O fluxo de dados pessoais cresceu de maneira vertiginosa nos últimos anos, sendo alavancado por força da pandemia da Covid-19, que fez com que os governos de todo o mundo impusessem rotinas de distanciamento social, isolamento social e quarentena às suas populações.

Ante essa necessidade, a digitalização dos procedimentos de trabalho, consumo, comunicação e serviços diversos se aceleraram ainda mais. É comum hoje as pessoas indicarem em formulários *online* e aplicativos de *smartphones* os seus

dados bancários, o número do Cadastro de Pessoa Física (CPF), endereço de *email*, dentre outros dados que, se caírem em mãos erradas, podem trazer prejuízos significativos, fato que infelizmente já tem acontecido com grande frequência. Num cenário tão vasto e complexo, o controle de privacidade se faz cada vez mais necessário (OLIVEIRA, 2020).

O presente tema foi adotado, partindo-se da premissa de que os órgãos públicos, a exemplo das Universidades Federais, na condição de autarquias voltadas às atividades de ensino, pesquisa e extensão possuem vastos bancos de dados de pessoas físicas, contendo, inclusive, significativa quantidade de dados sensíveis, ou seja, qualquer informação pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2022h).

1.3. CONCEITOS BÁSICOS

Dentro da temática proposta, é fundamental estabelecer alguns conceitos que serão abordados ao longo do trabalho, para melhor compreensão das questões e desafios enfrentados. Como está em foco a Lei Geral de Proteção de Dados Pessoais, cabe primeiramente definir o que são dados pessoais, o que a própria lei, no art. 5º, I, indica como “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2022h), o que na prática pode ser o número do passaporte, endereço, *e-mail* ou do Cadastro de Pessoa Física - CPF.

Além dessa classificação, a lei também protege o chamado dado pessoal sensível que a lei define como:

II - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2022h).

Nesse caso, os dados sensíveis merecem proteção extra, visto que informações como as descritas no inciso II são, geralmente, questões de foro íntimo e podem ser utilizadas por terceiros a fim de prejudicar o titular. Além das hipóteses descritas

acima, segundo Vignoli e Vechiato (2018) são tidos como exemplos o contracheque, a declaração de imposto de renda e outros documentos particulares similares.

Outro conceito que a LGPD destaca em seu art. 12 é o de 'dado anonimizado', que é considerado como dado pessoal quando sofre algum tratamento (como por exemplo a criptografia) que irá cifrar os dados, sendo possível decodificar apenas com a chave própria para saber o seu teor (JUNIOR, 2020). Com relação ao chamado 'tratamento de dados, a lei indica que:

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

[...]

X - tratamento: toda operação realizada com dados pessoais, como as que se referem 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, 2022h).

O art. 7º da LGPD aborda as hipóteses para realização do tratamento de dados pessoais, com ênfase no consentimento explícito do titular dos dados, em variadas condições descritas no texto da lei.

1.4. CONTEXTO E PROBLEMA

O estudo em tela está em voga no cenário nacional, tendo em vista a necessidade de adequação por parte das instituições públicas e privadas, não apenas pelo cumprimento da nova legislação vigente, mas também pelas pesadas sanções aos que a descumprem, fato esse que tem causado inclusive uma série de movimentações no mercado de trabalho, com o surgimento de novas carreiras para profissionais especializados em análise de dados e privacidade, além dos cursos e seminários disponibilizados por instituições diversas, para fins de capacitação dos seus gestores e colaboradores.

A pesquisa incide sobre a necessidade da correta aplicação da Lei Geral de Proteção de Dados Pessoais na Universidade Federal do Espírito Santo, tendo em vista a exigência do aludido diploma normativo, frente ao cenário cada vez mais debruçado sobre o uso das variadas tecnologias de armazenamento e tratamento de

dados. Some-se a isso o fato de que cada vez mais a comunidade acadêmica faz uso de ferramentas digitais, seja para fins de gestão administrativa ou de ensino. Portanto, o volume de informações geradas no contexto universitário é gigantesco, carecendo de constante análise e proteção por parte dos servidores de todos os níveis envolvidos nas tarefas correlatas.

Desde a promulgação da Lei Geral de Proteção de Dados Pessoais, em se tratando do ambiente da UFES, as discussões acerca da aplicação desse diploma normativo se deram quase que exclusivamente em sede de reuniões fechadas, a exemplo das que ocorrem com membros do Gabinete da Reitoria e Pró-reitores, com pouca ou nenhuma divulgação formal da questão entre alunos, professores e técnicos. Como prova dessa deficiência, pode-se apontar o fato de que os servidores da UFES recebem frequentemente *e-mails* com convites para participação de capacitações sobre temáticas diversas (saúde laboral, legislações pertinentes ao ambiente administrativo, práticas de gestão pública, dentre outros), mas não há manifestações acerca de cursos sobre aplicação da LGPD no ambiente universitário.

Movimentação diversa pôde ser vista a partir de julho de 2021, quando a Ufes publicou o seu Plano de adequação à Lei Geral de Proteção de Dados Pessoais. Nesse plano há a proposta para definir a estrutura organizacional a partir do controlador (na figura do Reitor), enquanto a função de encarregado de dados será de responsabilidade da Ouvidoria, através do Ouvidor. Os comitês operadores e suas presidências seriam indicados pela Reitoria. Além disso, não se vê movimentação explícita ou razoavelmente divulgada na comunidade acadêmica.

Quanto aos procedimentos disciplinares a situação é ainda mais delicada, tendo em vista que se trata de um momento de investigação que pode culminar numa punição ao servidor analisado. Tais dados devem ser preservados de consultas externas ou interferências de determinados setores da instituição, pois do contrário pode haver prejuízos ao procedimento e à lisura do processo. No caso da UFES, a instituição utiliza a plataforma de protocolo denominada “Lepisma”, por meio da qual tramitam-se os processos físicos, digitais e digitalizados. Com frequência, é possível ler documentos que possuem dados pessoais de servidores, alunos e terceiros indicados sem qualquer restrição de acesso, podendo ser visualizados por qualquer

indivíduo externo à instituição, visto que o portal tem a modalidade de consulta pública, para fins de transparência.

Vê-se que a aplicação da LGPD demanda atuação multidisciplinar, posto que lida com questões de legislação, gestão de dados, gestão de pessoas, processos de tomada de decisão, dentre outras atividades dentro de uma organização (FERREIRA; OKANO, 2021). Logo, não seria diferente em âmbito universitário, razão pela qual o presente estudo versa sobre o tema. Do mesmo modo que ocorre com as pessoas jurídicas de direito privado, que lidam com dados pessoais de colaboradores e clientes, é preciso instaurar nas universidades federais (em especial na Ufes) um projeto de governança para garantir o mínimo de proteção e privacidade dos dados pessoais dos envolvidos (FLOWTI, 2020).

Ainda com esse déficit instrucional sobre a LGPD, algumas movimentações podem ser observadas no sentido de adequação dos procedimentos internos à legislação vigente. Dentre os manuais de gestão e fiscalização de contratos, disponibilizados pela Diretoria de Contratações de Obras e Serviços – DCOS/PROAD/UFES, as portarias para indicação de fiscais e gestores já não exigem a inserção do número de CPF dos servidores, apenas dados como nome, matrícula, setor de lotação e contato (institucional, de preferência), que são informações de livre consulta na internet, inclusive contidas na relação de servidores, divulgada pela Pró-reitoria de Gestão de Pessoas – PROGEP/UFES, em seu endereço na rede. As portarias acima mencionadas, além de ficarem registradas nos servidores de dados da Universidade, são publicadas no Diário Oficial da União, o que torna ainda mais problemático o fato desses documentos apontarem dados pessoais.

Importante destacar que, o atendimento à previsão da lei não se resume a utilizar *softwares* de segurança para prevenir vazamentos de dados, mas implica numa mudança de postura das instituições e das pessoas envolvidas nos processos, tornando o ambiente de trabalho mais seguro nesse aspecto.

O assunto ora analisado, no contexto organizacional das Universidades Federais, tem sido alvo de diversos estudos e publicações de caráter científico, por se tratar de um terreno fértil, cujo teor se aplica em várias demandas do meio acadêmico e ainda gera muitas dúvidas nos gestores públicos. Exemplo disso é a emissão de

diplomas em modo digital, que obedece aos ditames da portaria nº 554, de 11 de março de 2019 do Ministério da Educação (MEC), por meio da qual foram indicados os formatos dos documentos e o padrão de assinatura a ser adotado, levando-se em conta o teor dos diplomas, contendo dados pessoais dos formandos.

A LGPD estabelece uma série de diretrizes para tratamento, armazenamento e exclusão de dados pessoais em bancos de dados de pessoas jurídicas, todavia esse assunto não é muito debatido em discussões abertas sobre a temática no âmbito da universidade analisada. Resta saber, portanto, o que de fato acontece no tratamento das informações utilizadas em determinados processos da Universidade. Pode-se perguntar, então, quais mecanismos podem ser adotados na Ufes – em sede de investigação administrativa de responsabilidade de servidores – para correção de eventual não aplicação ou uso deficiente desse diploma normativo?

1.5. OBJETIVOS

Com base na proposta acima narrada e nos desafios apresentados, entende-se que o objetivo geral da presente pesquisa é analisar a aplicação da Lei Geral de Proteção de Dados Pessoais nos registros de dados em Procedimentos Disciplinares da Ufes.

Tendo em vista a necessidade de elucidar a questão, foram elaborados dois objetivos específicos, quais sejam (1) identificar em que grau a LGPD é citada ou aplicada nos procedimentos disciplinares, segundo as normativas internas da UFES; (2) apontar consequências de eventual omissão da LGPD nos expedientes administrativos de investigação.

1.6. PRODUTO TÉCNICO ESPERADO

Como resultado da pesquisa a ser desenvolvida a título de dissertação, o produto técnico/tecnológico será a elaboração de uma minuta de um Manual de boas práticas para a correta aplicação da Lei Geral de Proteção de Dados Pessoais, nos expedientes administrativos da UFES, incluindo observações específicas quanto aos

procedimentos disciplinares, protegendo informações pessoais de todos que porventura estejam sob investigação administrativa, zelando pela correta aplicação da legislação nacional, principalmente porque dentro de pouco tempo essa questão passará a ser demandada pelos órgãos de controle aos quais a instituição se submete.

1.7. LINHA DE PESQUISA E PROJETO ESTRUTURANTE

A presente pesquisa está inserida no Projeto Estruturante 2, denominado Governança e gestão no setor público - fundamentos da governança, no bojo da Linha de Pesquisa 1 do Programa de Pós-graduação em Gestão Pública (PPGGP), intitulada 'Política, planejamento e governança pública'.

No caso, a Lei Geral de Proteção de Dados Pessoais é a premissa maior da pesquisa, uma vez que é a partir desta norma que há de se iniciar a parte teórica do projeto; enquanto a Ufes representa a premissa menor, haja vista que será observada a aplicação da lei na instituição, suas vantagens e dificuldades, tendo direta relação com o cotidiano de trabalho da administração dos arquivos públicos.

A situação problema se enquadra nesse projeto estruturante pois sua discussão permeia o âmbito de análise legislativa, o monitoramento das atividades do setor e os riscos de seu exercício, bem como a definição de quais dados podem ser acessados livremente e quais demandam restrição.

1.8. ALINHAMENTO AO PLANO DE DESENVOLVIMENTO INSTITUCIONAL (PDI) DA UFES

A Ufes, em seu plano de desenvolvimento institucional 2021-2030, trata, dentre outros assuntos, dos desafios que o cenário de pandemia, somado ao progressivo uso das tecnologias impôs ao ambiente acadêmico, conforme transcrito a seguir:

Cabe destacar que a STI auxilia a Administração Central na gestão acadêmica e administrativa da Ufes, focando nos sistemas corporativos de informação, no desenvolvimento e na manutenção das infraestruturas em TI, na aquisição e instalação de equipamentos e no suporte aos usuários, em uma abrangente gama de serviços e produtos. Há ainda um Comitê de Governança Digital, que é responsável pelas decisões estratégicas e críticas, e pela gestão de segurança da informação na instituição. A STI é responsável por implantar as decisões tomadas pelo Comitê. Em junho de 2020, o Comitê aprovou o plano de transformação digital da Ufes, que tem como objetivo ampliar a transparência, a economicidade e a eficiência nos processos de aquisição e no trato da informação (UFES, 2021, p. 109).

Hoje, para se ter noção da importância do domínio dos meios eletrônicos no âmbito administrativo da Ufes, as solicitações de informações encaminhadas por parte dos órgãos de controle, em sua maioria, são realizadas por meio digital. O mesmo ocorre com as respostas, que são enviadas pelas plataformas digitais, a exemplo do que é feito pelo Ministério Público Federal (MPF) e pelas manifestações de usuários abertas pelo sistema da Controladoria Geral da União (CGU).

Assim, dada a grande quantidade de dados gerados e armazenados, com o advento da lei geral de proteção de dados, vê-se a necessidade de análise aprofundada sobre o cumprimento desse ditame legal, resguardando informações em arquivo, zelando pelos servidores que lidam com ele. É preciso entender esse momento como sendo propício para atualização das rotinas e procedimentos de trabalho.

Nesse contexto, mais do que otimizar os trâmites de procedimentos por via digital, é preciso fazê-lo com um salto de qualidade nos moldes da LAI e da LGPD, concedendo mecanismos de controle efetivos, eventualmente por atuação da própria Superintendência de Tecnologia da Informação - STI, responsável também pela interface da plataforma Lepisma. Além disso, a Administração Central precisa promover, por meio da Pró-reitoria de Gestão de Pessoas - PROGEP, entre os servidores, uma cultura de zelo e proteção com os dados pessoais, oferecendo capacitação adequada, visando atender ao comando legal.

1.9. JUSTIFICATIVA

A LGPD foi promulgada com a intenção de resguardar as informações dos cidadãos, tratadas e compartilhadas pelas instituições privadas e públicas, com amparo no princípio da privacidade. Ocorre que as pessoas jurídicas de direito público, por

possuírem regime jurídico diverso das privadas, devem adaptar as normas e administração internas para que os dados dos acadêmicos e profissionais da instituição estejam escudados, não como uma relação consumerista, mas sim como elevação do princípio da supremacia do interesse público.

Infelizmente, no cenário atual brasileiro, embora seja necessária a divulgação em larga escala dos dados inerentes à transparência dos órgãos públicos, é comum a reclamação entre servidores no sentido de que não há treinamento específico para atender a essa demanda, o que fragiliza ainda mais algo que já é complexo por natureza. Acerca disso, a instituição deve promover análises críticas regulares da eficácia do seu sistema de gestão de segurança da informação - SGSI, considerando os resultados de auditorias e outros mecanismos similares (ABNT, 2006). Logo, é fundamental que assuntos desse calibre sejam alvo de qualificação das equipes de trabalho, tanto na esfera pública quanto na privada.

A aplicação da LGPD na Ufes precisa se dar de forma eficiente para que de fato cumpra seu papel no que se refere à gestão pública, visto que se trata de uma instituição pública de ensino superior, diretamente ligada ao Ministério da Educação. Além disso, assim como ocorre em outros ramos de pesquisa e desenvolvimento, há também um papel de vanguarda a ser desempenhado pela Universidade, devendo servir de exemplo para a comunidade capixaba.

Sendo os dados pessoais dos discentes, docentes e internos manipulados pela administração da instituição, faz-se necessário que seja atualizada com as modificações do ordenamento jurídico, de maneira que se torne qualificada e correta perante a lei. Ademais, os próprios servidores públicos são beneficiados pelas modificações desse diploma legal, protegendo-os dos vazamentos de dados internos.

Cabe frisar que a Universidade Federal do Espírito Santo, na qualidade de autarquia federal voltada às atividades de ensino, pesquisa e extensão, bem como demais entidades públicas de pesquisa, são abarcadas pela legislação ora analisada, consoante o Art. 5º da Lei nº 13.709/2018:

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

[...]

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; (BRASIL, 2022h)

Assim, é de crucial importância entender o alcance da LGPD no âmbito das universidades federais e que isso seja amplamente veiculado aos servidores, técnicos e professores, cujos dados são colhidos e tratados por vários setores das instituições, ainda que tal situação ocorra com sigilo e os devidos cuidados de segurança. É questão de cidadania e respeito aos titulares que já renunciam à parte da privacidade de suas informações que são divulgadas nos endereços eletrônicos dos seus órgãos, incluindo remunerações.

No que diz respeito aos procedimentos administrativos disciplinares, cabe ressaltar que a Seção de Procedimentos Disciplinares da Ufes é o setor de correição ligado ao Órgão Central do Sistema de Correição do Poder Executivo Federal. No âmbito da Universidade, é diretamente vinculada ao Gabinete da Reitoria. Sua atuação se baseia no Manual de Processo Administrativo Disciplinar, publicado pela CGU, o qual não faz menções expressas à LGPD, mesmo tendo sido atualizado até março de 2022, três anos e meio após a sanção do diploma legal.

Cabe ainda destacar a importância da ausência de divulgação das informações aos titulares dos dados pessoais daqueles envolvidos em procedimentos administrativos de investigação, como aponta Chaves:

[...] recomenda-se que a administração pública, em cumprimento ao inciso I do Art. 23 da LGPD, dê publicidade ampla aos titulares de dados que as investigações administrativas são uma das hipóteses de tratamento de dados pessoais. Essa informação, em conformidade com a lei, deverá estar exposta no sítio eletrônico dos órgãos, com a devida explicação acerca do amparo legal, do procedimento e das práticas adotadas (2021, p. 11).

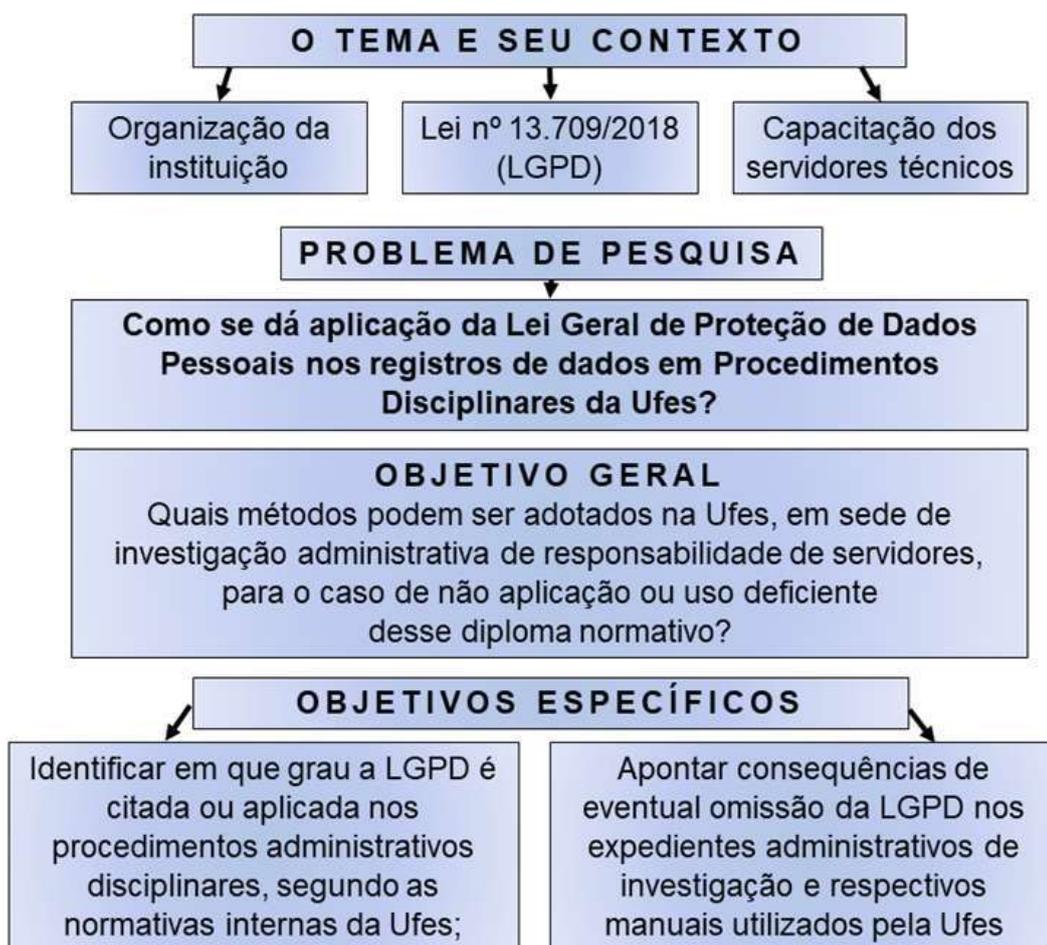
Tal omissão ainda se mostra recorrente nos portais de acesso à informação, o que, nos moldes da LGPD, representa risco para os titulares dos dados, bem como para os servidores públicos que manejam essas informações. Isso se aplica não apenas nas investigações em âmbito administrativo, como também em vários expedientes

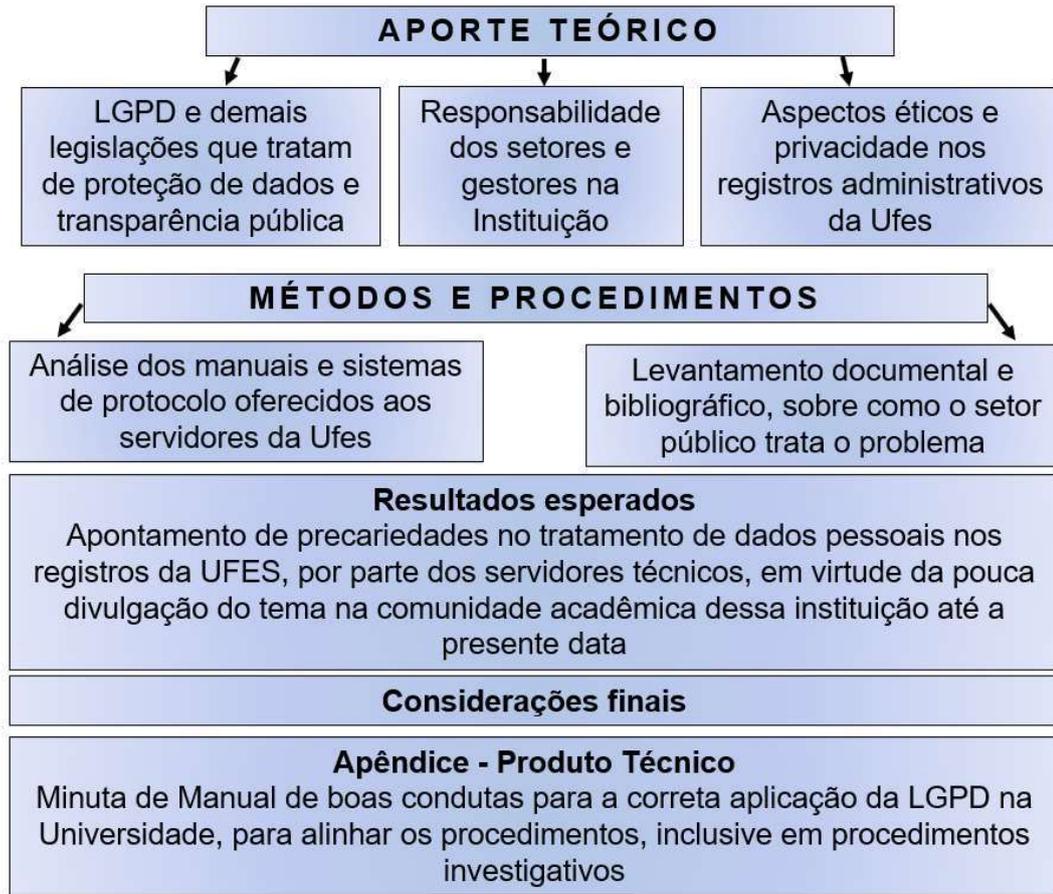
da universidade, como nas demandas de responsabilidade da Pró-Reitoria de Gestão de Pessoas (Progep/Ufes), que costumeiramente exigem dados que não podem ser de conhecimento público, os quais podem passar por vários servidores distintos – a depender do caso – sem restrições de controle de acesso ou de *download*. Isso traz insegurança aos envolvidos no processo e pode acarretar problemas futuros, seja com o próprio descumprimento da LGPD ou com as consequências advindas de mau uso dos dados vazados.

1.10. ESTRUTURA GERAL DA PESQUISA

Por fim, neste capítulo inicial, apresenta-se a estrutura geral da pesquisa na Figura 1.

Figura 1 - Esquematização geral da pesquisa





Fonte: Elaboração própria.

2. APORTE TEÓRICO

2.1. ABORDAGEM DO TEMA NO SETOR PÚBLICO

A sociedade moderna busca, de várias formas, otimizar os processos de busca, geração e armazenamento de informações, seja em dispositivos físicos ou em redes compartilhadas. Com um grande clamor popular por maior transparência dos órgãos públicos e seus respectivos gastos, tornaram-se rotina as consultas aos chamados “portais da transparência”, os quais indicam, dentre outras informações, dados de verbas obtidas pelos órgãos e como foram alocados tais recursos. Some-se a isso a enormidade de instituições de controle em todas as esferas de atuação, que geram relatórios detalhados sobre as condutas dos entes públicos e o grau de publicidade de seus atos.

A Lei Geral de Proteção de Dados em vigor no país aplica-se aos setores público e privado, trabalhando na linha tênue entre resguardar os dados dos jurisdicionados e, na esfera de atuação estatal, fazer um bom uso dessas informações, objetivando a execução de políticas e serviços públicos (ITS, 2019). Essa missão traz desafios visto que o acesso a dados pessoais para tais fins deve respeitar o direito à privacidade sem impossibilitar uma boa e transparente gestão pública. Inclusive esse aspecto do conflito de interesses público e privado é tratado pela Lei de Acesso à Informação (LAI), no seu artigo 31. (ITS, 2019).

Um caso comum de aparente conflito entre a LAI e a LGPD é a necessidade de se exibir nos portais de transparência a remuneração de cada servidor. Segundo a LAI, trata-se de uma necessidade para dar ao jurisdicionado o acesso pormenorizado do registro de gastos públicos. Perante a LGPD, poderia ser uma violação à privacidade de quem recebe a quantia:

Com respaldo na finalidade específica de tornar transparente os gastos efetuados pela Administração Pública com seu pessoal, para que qualquer cidadão possa fiscalizar eventuais abusos cometidos, como, por exemplo, o descumprimento do teto salarial constitucionalmente previsto. Todavia, embora estejam públicos tais dados ainda devem ser protegidos, visto que não podem ser utilizados para qualquer outra finalidade que não aquela prevista na LAI, não podendo um terceiro captá-los para fazer listas de fornecimento de crédito, por exemplo, ou a Administração Pública cedê-los para que terceiros os utilizem para qualquer fim (ROSSO, 2019).

O tema em questão é tratado como sendo uma nova etapa no setor público, partindo-se da premissa de que embora se esteja lidando com bancos de dados em órgãos voltados ao atendimento à população (ou seja, uma atuação com base no princípio da publicidade), há de se preservar informações relativas à pessoa natural, pois a legislação pátria aponta no sentido de que não há dados pessoais de menor importância (TEPEDINO; DE TEFFÉ, 2019). Nessa mesma linha de mitigação do aludido princípio, e já no âmbito universitário, há as pesquisas acadêmicas que se valem de informações pessoais, as quais por força da lei ora tratada, devem ser anonimizadas. Caso a pesquisa não demande tais dados ou se a coleta e tratamento destes forem em número desarrazoado, incorre-se em violação legislativa (CARNEIRO; SILVA; TABACH, 2019).

Uma situação preocupante se mostra num horizonte próximo, pois conforme dados apresentados pelo Tribunal de Contas da União, já no ano de 2015, à época, 74% das instituições analisadas não realizavam processos de gestão de riscos de segurança da informação, o que se mostra como uma falta grave, principalmente num momento de migração de conteúdo para plataformas digitais, deixando os dados expostos a ataques de cibercriminosos (TCU, 2015).

O mesmo órgão, já no ano de 2022, apontou que 76,7% das organizações vinculadas à Administração Pública Federal analisadas tinham nível de adequação à LGPD tido como 'inexpressivo' ou em 'fase inicial' de implantação (TCU, 2022), indicando que uma deficiência que persiste ao longo dos últimos anos em toda a esfera.

Sabe-se que esse momento de transição vai demandar adaptações em vários procedimentos nos órgãos públicos, passando pela cultura dos servidores e repartições, além da gestão e da governança acerca dos dados pessoais armazenados nos respectivos sistemas de informação (ITS, 2019).

O caminho da LGPD até a presente data foi consideravelmente tortuoso. Publicada em 14 de agosto de 2018, seguindo os passos da legislação europeia sobre o tema (GDPR), o diploma normativo pátrio teria *vacatio legis* de dezoito meses, a contar da data de sua publicação no Diário Oficial. Até esse ponto, nenhuma novidade, visto que é comum que novas leis possuam prazos significativos para entrada em vigor,

principalmente quando trazem tantas alterações, ainda mais em matérias que nunca haviam sido regulamentadas nesse nível de detalhes.

Com a sanção efetivada pelo então Presidente da República, Michel Temer, foram vetados os artigos relativos à criação da Autoridade Nacional de Proteção de Dados - ANPD, órgão responsável, dentre outros pontos, por fiscalizar a aplicação da LGPD no país, incluindo nesse bojo as temidas multas. Esse veto foi feito sob o argumento de que haveria vício de iniciativa por parte do Poder Legislativo, pois a criação da Autoridade Nacional deveria partir do Poder Executivo, na forma do art. 61, §1º, II, CR/88. Logo, no fim do ano de 2018, por meio da Medida Provisória nº 869/2018, foi instituída a ANPD.

Nesse período, no entanto, muitos debates foram travados, apontando a necessidade de se ter um prazo maior para garantir a adequação por parte das instituições afetadas, muito por conta do receio em relação às punições previstas para os que descumprissem a nova lei. Foi então que em julho de 2019 a Lei nº 13.853 estendeu a *vacatio legis* da LGPD por mais seis meses além do originalmente previsto, postergando a entrada em vigor para o mês de agosto de 2020. Como é de conhecimento geral, nesse mesmo ano, o mundo foi profundamente abalado pela pandemia de COVID-19, afetando todas as atividades do país. Por razões óbvias, o tema da proteção de dados pessoais ficou em segundo plano nas discussões políticas e sociais.

Em junho de 2020, a Lei 14.010 foi promulgada, prevendo que as sanções administrativas entrariam em vigor somente a partir de agosto de 2021. Ao final, essa foi a data em que as punições passaram a surtir efeito. Com um cenário social e político tão caótico, como o narrado acima, é compreensível a demora na implementação de práticas e cursos de capacitação para órgãos governamentais. A sensação que se transmite é justamente de que enquanto não há chance real de punições, não há sentido para mobilização dos setores e órgãos. Ainda assim, sabe-se que o tema já é abordado em trabalhos acadêmicos e cursos de qualificação aplicados junto à iniciativa privada.

No contexto da LGPD, ao poder público compete tratar dos dados pessoais pelo prisma de um ato administrativo, cuja validade está na observância da finalidade

pública, caminhando ao lado do interesse comum, para atingir os objetivos fundamentais do Estado, razão pela qual utiliza essas informações do particular (MURARI; SCHIAVON; BARRETO, 2021). Por consequência disso, eventual compartilhamento de dados pessoais pelo poder público deve ocorrer de modo que alcance finalidades específicas de execução de políticas públicas que deem motivo à essa disposição (TEPEDINO; TEFFÉ, 2019).

2.2. TEORIAS ASSOCIADAS AO TEMA

A promulgação da LGPD ocorre num momento singular da história recente, tendo em vista que há um volume incomensurável de informações pessoais disponíveis na rede mundial de computadores, sendo plenamente possível haver vazamento dos chamados dados pessoais e sensíveis, causando inúmeros danos aos respectivos titulares.

Sabe-se da importância da transparência para uma gestão bem quista pelos cidadãos e bem avaliada pelos órgãos de controle, pois é fruto de conquistas sociais e políticas ao longo das últimas décadas e serve de base para uma governança sólida, sabendo que “[...] o acesso à informação coloca o cidadão em pé de igualdade com a administração pública e aí se revela parte da força democratizadora da transparência e da publicidade.” (RODRIGUES, 2014, p. 94). Todavia, essa abertura exige limites de acesso para determinados casos, além de também proteger os cidadãos, cujas informações nem sempre podem ser livremente acessadas.

Some-se a isso o fato de que a matéria já estava em ampla discussão fora do Brasil:

Em 2016, o General Data Protection Regulation (GDPR) foi aprovado e em 2018 ele entrou em vigor. Com sua entrada em vigor, em 25 de maio de 2018, os legisladores brasileiros viram-se pressionados a agilizar a votação de um projeto de lei de dados pessoais, caso contrário as empresas brasileiras teriam enorme dificuldade em realizar negócios com europeus, porquanto o país seria considerado não adequado para tratar dados de cidadãos que estiverem localizados na Europa. (MACIEL, 2019. p. 17)

Quando se fala em tratamento de dados pessoais, não se trata de uma novidade trazida pela LGPD, visto que o tema já consta do art. 5º, X da CR/88, ao abordar os

direitos da personalidade, quando diz que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;” (BRASIL, 2022a). Nesse contexto, estão inseridos os dados pessoais.

A partir da previsão da Carta Magna, o ordenamento jurídico brasileiro passou a indicar, em vários diplomas, a necessidade de proteção dos direitos da personalidade, a exemplo do que acontece no Código de Defesa do Consumidor (Lei nº 8.078/1990), no Código Civil (Lei nº 10.406/2002), na Lei de Acesso à Informação (Lei nº 12.527/2011), no Marco Civil da Internet (Lei nº 12.965/2014), na Lei do Cadastro Positivo (Lei Complementar nº 166, de 2019) e na Lei de Governo Digital (Lei nº 14.129/2021), além é claro, da própria LGPD.

Inclusive, a partir de 2022, o art. 5º da CR/88, por meio da Emenda Constitucional nº 115, recebeu um novo inciso específico para o tratamento de dados pessoais: “LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”, explicitando a importância da matéria, alçando-a ao rol dos direitos fundamentais do cidadão brasileiro (BRASIL, 2022a).

A privacidade, do modo que conhecemos hoje, costumeiramente apontava para temas como a inviolabilidade de domicílio, o sigilo das comunicações ou das movimentações bancárias. Mas com a grande verticalização tecnológica, o tema subiu na escala de importância, abarcando também as informações pessoais salvas em servidores e bancos de dados digitais. Por conta desse fenômeno, não é raro ouvir as pessoas dizerem que não conseguem passar um dia sequer sem manusear o *smartphone*, acessar suas redes sociais por outros dispositivos ou mesmo por questões de trabalho, tamanha a dependência que a sociedade moderna possui em relação a esses meios de comunicação.

Por conta da capilaridade da LGPD (regulando não apenas relações entre indivíduos, bem como entre indivíduo e Estado) é que a lei tutela direitos fundamentais de modo transversal, ou seja, incide sobre relações jurídicas tanto de direito público quanto de direito privado (BASAN, 2021)

O Código Civil, em seu art. 21, caminha no mesmo sentido ao prever que “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado,

adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.” (BRASIL, 2022e).

Carlos Konder (2013, p.387) é enfático ao apresentar a privacidade como um ‘poder negativo’, apontando que ela deve ser entendida “não apenas como a ‘possibilidade’ de impedir que informações de seu conhecimento sejam acessadas por terceiros, mas também o direito de desconhecer certas informações a seu respeito que sejam de conhecimento de terceiros”.

Ao contrário do que possa parecer numa análise superficial, a LAI e a LGPD, são harmônicas entre si, coexistindo e tutelando o acesso a informações, dando a devida transparência, sem que haja prejuízo para a atividade estatal nem ao titular de dados:

Pode-se dizer que a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados surgem com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade com finalidade de garantir transparência, quanto à circulação de dados e informações, de forma clara, precisa e facilmente acessível. (SOUZA, BARRANCOS e MAIA, 2019. p. 240).

Obviamente, a implantação de tecnologias nos serviços à população é um caminho sem volta. Sabe-se que, para fins de gestão no serviço público, tem se mostrado cada vez mais evidente que o bom uso dessas ferramentas traz ganhos em efetividade, simplificação e economia de recursos, no tratamento dos registros e atividades correlatas, como ocorre nos atendimentos feitos pela *internet*. Este contexto claramente traz uma série de benefícios para o cidadão, que não precisa mais se deslocar para lugares específicos ou enfrentar filas (VARELLA; OLIVEIRA; MOESCH, 2017).

Avanços tecnológicos dessa magnitude demandam adaptações do entorno, o que inclui a legislação em vigor. Em âmbito acadêmico, por exemplo, dados dos alunos, como as notas, devem ser alvos de extrema proteção, como indica Stallings (2015, p. 08): “Nos Estados Unidos, a disponibilização de tais informações é regulamentada pelo Ato sobre a Privacidade e os Direitos Educacionais da Família (Ferpa – do acrônimo em inglês para Family Educational Rights and Privacy Act).”

Essa crescente necessidade de proteção culminou na sanção da LGPD, por meio da qual “todas as organizações brasileiras, seja de qual porte for (pequeno, médio e

grande), deverão fazer investimento em segurança tecnológica e executar técnicas de *compliance* existentes para impedir, detectar e corrigir violações de dados pessoais [...] (PEREIRA DA ROCHA, 2019). Assim, a Universidade Federal do Espírito Santo, na condição de órgão público detentor de um considerável banco de dados pessoais (desde contatos de *e-mail* e telefone até contas bancárias e laudos médicos de servidores e alunos), é fundamental alinhar os interesses da lei e dos usuários para que não ocorra vazamento ou mau uso dessas informações.

Ciente dessa demanda e de tudo que é necessário para o bom e correto manuseio deste diploma normativo, é preciso salientar que:

[...] a LGPD não é uma lei estanque, pois necessita de aplicabilidade técnica que perpassa ao conceito estritamente legal e incide em termos relacionados com o sistema de informação, ferramentas, procedimentos, normas, práticas negociais, elaboração de projetos, dentre vários outros fatores (SILVA, 2020, p. 20).

Além da abordagem legal acerca da proteção de dados pessoais pelos entes públicos (indicando o que se pode ou não fazer), há questões de ética envolvidas na discussão. A ética é um princípio fundamental a qualquer atuação estatal num estado democrático de direito, partindo do pressuposto de que cada movimento do poder constituído deve obedecer estritamente à legislação vigente (seguindo o princípio da legalidade, constante do art. 37, CR/88), zelando pela integridade do cidadão e dos bens públicos, com todos os valores constitucionais preservados.

Esse ponto, inclusive, é um dos fatores que norteia a aplicação da legislação de proteção de dados pessoais no Brasil e no mundo. O ponto é alvo de debates internacionais, envolvendo organizações de todas as esferas de poder. A Organização para a Cooperação e Desenvolvimento Econômico - OCDE (2020) já apresentou parecer sobre como a ética de tratamento de dados deve ser aplicada nas ações do poder público:

“[...] prevenir, evitar ou, pelo menos, limitar a ocorrência de danos intencionais a indivíduos, a grupos sociais e à sociedade [...]. Para alcançar esse objetivo, os governos devem realizar uma efetiva gestão ética dos dados, incluindo os de indivíduos e comunidades, ao longo de todo o seu ciclo de valor, visando ao fortalecimento das instituições democráticas e do Estado de Direito (por exemplo, no que concerne à privacidade e à proteção de dados pessoais). Isso ajudaria a ampliar a legitimidade do uso e do tratamento de dados pelos governos, inclusive no que concerne à entrega de políticas e serviços centrados no ser humano” [tradução livre]. (2020, p. 5).

O enfoque dessa manifestação é justamente a necessidade de tratar com zelo os dados pessoais armazenados, visto que o uso de dados pelos governos tem o dever de proporcionar o bem público, pois essa postura acaba por dar mais credibilidade à tarefa estatal que é extremamente complexa. O correto tratamento dos dados pessoais pelos entes governamentais é como um voto de confiança que, se bem aproveitado, pode gerar bons frutos para a gestão pública e para os agentes do estado, que terão bons resultados nos serviços prestados e nas políticas implementadas.

A ética para uso de dados na esfera estatal deve estar voltada a políticas em caráter macro, sendo capaz de produzir ferramentas úteis aos operadores da máquina pública, podendo ser aplicada para preservação da integridade dos procedimentos e das boas práticas perante a legislação vigente, como em processos de auditoria e investigação administrativa.

No que diz respeito aos ambientes públicos de ensino, Barbosa *et al.* (2021), aponta que as instituições dessa natureza não estão livres de passarem por essa adequação à nova lei. Isso se aplica, obviamente, aos processos e sistemas institucionais, sem esquecer da mudança de cultura com o tratamento dos dados pessoais, que devem ser revisados em face das novas exigências normativas.

No ambiente universitário, a título de exemplo, há grande importância das questões de ética relacionadas a pesquisas e coleta de dados, principalmente agora com a vigência da LGPD:

O modus operandi da ciência está em grande parte relacionado ao processo de coleta e análise de dados, componentes que são responsáveis por uma grande parte do tempo e dos recursos utilizados nas pesquisas. Uma parte das disciplinas científicas utiliza-se, em suas pesquisas científicas, de dados coletados no mundo natural, incluindo seres vivos não humanos. (BARRETO; ALMEIDA; DONEDA, 2019. p. 180)

Outro modo comum de se aplicar a LGPD é o ambiente de trabalho na iniciativa privada, já que há coleta de dados pessoais por parte dos empregadores, os quais pautam uma série de atividades da empresa, não apenas relacionadas às demandas de recursos humanos. Como se sabe, a lei exige o chamado consentimento livre do titular dos dados para que estes sejam tratados. Todavia, ciente de que há

disparidade de poderes entre empregador e empregado, isso pode acarretar certos problemas:

[...] é natural que tal suposição suscitará dúvidas sobre sua legitimidade no contexto de uma relação trabalhista, posto que essa é caracterizada pelo desequilíbrio de poder e, em regra, pela dependência econômica. Nesse cenário, as alegações de que o empregado não teve legítima escolha deverão ser frequentes, sob pretexto de que o consentimento foi utilizado como moeda de troca para a manutenção do vínculo empregatício. (ALCÂNTARA, 2021. p. 17)

Nesse caso, é extremamente difícil garantir que o consentimento do trabalhador seria livre, partindo-se do pressuposto de que a relação trabalhista, por sua natureza, é desbalanceada, face ao poder hierárquico exercido pelo empregador. Logo, ainda que não haja uma pressão explícita exercida pelo contratante, o contratado pode se sentir constrangido em assinar o termo, por receio de ser prejudicado num processo seletivo para vaga de emprego, ou mesmo quanto à sua manutenção no quadro, por exemplo.

Em virtude dessas dificuldades na interpretação e aplicação da norma, há recomendação nos seguintes termos:

Dessa forma, a utilização do consentimento não é recomendável no âmbito das relações de trabalho, em razão do risco de não ser considerado válido. Outro risco é a possibilidade de o empregado revogar o consentimento a qualquer momento, o que gera uma insegurança naquele tratamento. Além disso, a empresa precisa dispor de um procedimento gratuito e facilitado para operacionalizar tal direito do titular (LGPD BRASIL, 2021).

Tem-se aqui uma clara referência ao princípio da proteção, preceito que norteia a legislação brasileira nas questões trabalhistas, sendo resultado de regras de caráter imperativo, como resultado da ordem pública. Mostra-se como um verdadeiro obstáculo à autonomia da vontade. Esse basilar é o sustentáculo do contrato de trabalho, tanto que o caráter protetivo da legislação trabalhista é nítido quando se analisa o art. 7º, CR/88 (SUSSEKIND, 2020).

Outra temática onde há interferência direta da LGPD é com relação aos dados de crianças e adolescentes, não só por questões educacionais e informações contidas em arquivos de ambientes escolares, mas também em virtude da grande exposição dos menores aos dispositivos móveis com acesso à *internet*. As gerações mais recentes cresceram num contexto digital e os riscos dessa nova fase começaram a

despontar nos debates entre famílias, escolas e o setor público, visando a proteção dos menores.

O art. 227, CR/88, nos mostra a importância da proteção da instituição familiar e dos seus componentes, *in verbis*:

Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão (BRASIL, 2022a).

Segundo Botelho (2020), a previsão constitucional acima aponta para o princípio do melhor interesse da criança e do adolescente, logo, orientando como a legislação infraconstitucional deve tutelar os interesses da proteção à criança e ao adolescente. O artigo acima também abarca o chamado princípio da proteção integral, indicado no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), já em seu primeiro artigo, como norteador de todo o diploma.

Segundo Ferreira e Dói (2018) o princípio da proteção integral foi introduzido no ordenamento jurídico brasileiro via artigo 227, CR/88, o qual gera uma responsabilidade coletiva entre família, sociedade e Estado para preservação do menor, a fim de que haja compromisso total contra a negligência, discriminação, exploração, violência, crueldade e opressão. Logo, não é de surpreender que a LGPD traga uma seção inteira tratando das questões sobre dados pessoais de crianças e adolescentes:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

[...]

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (BRASIL, 2022h).

Destaca-se nesse fragmento da lei a necessidade de consentimento de, pelo menos, um dos pais (ou responsável legal), para que haja tratamento de dados dos menores, o que caminha ao lado da previsão do art. 227 da Constituição da República, bem como os preceitos que o balizam. Além disso, há a contextualização das atividades comumente desempenhadas pelos menores, conforme o parágrafo 4º, quando do uso de dispositivos eletrônicos para acessar conteúdos de jogos e demais aplicações via *internet*.

2.3 TRABALHOS CORRELATOS AO OBJETO DA PESQUISA

Consoante análise prévia à esta redação, verifica-se que há os seguintes trabalhos cujos temas abordam a mesma discussão ora apresentada, permeando o ambiente das universidades federais do Brasil e os desafios à adequação à LGPD:

- a) ALBUQUERQUE (2020): O objetivo desse trabalho foi auditar, com base nos riscos, a gestão das informações pessoais realizada na Diretoria de

Administração de Pessoal (DAP) da Universidade Federal do Rio Grande do Norte (UFRN), usando como instrumentos de coleta de dados a Pesquisa documental, a Observação Participante e a Entrevista e Grupo Focal. Como resultado da pesquisa, foi elaborada cartilha de acesso à informação pessoal, com um resumo da legislação e orientações da Controladoria Geral da União (CGU), para auxiliar os servidores da diretoria na execução de atividades e tomadas de decisões.

- b) SILVA (2021): Tratou da abordagem da Pró-reitoria de Gestão de Pessoas da UFPE, que mobilizou sua equipe para tornar possível a implementação da LGPD na referida instituição. Identificou que os sistemas de gestão da PROGEPE possuem grande fluxo de armazenamento de dados, sendo que antes da vigência da LGPD não havia critério para a distinção dos dados, se a informação apresenta dados sensíveis, se existe alguma restrição para acesso a essa informação, entre outros, por isso, há carência de capacitação com os servidores que manejam dados pessoais e dados sensíveis, além da criação de uma política interna visando proteção de dados, revisão de contratos, dentre outras condutas.
- c) MARQUES (2021): Por meio deste trabalho, indicou-se que o regime de informação da UFRGS é alcançado pela LGPD, gerando modificações nos hábitos e práticas acerca do tratamento de dados por parte dos servidores e chefias. A existência da LGPD proporcionou a criação de documentos institucionais, inseridos no fluxo de informações, para que houvesse adequação à norma vigente.

Os estudos indicados acima tratam justamente da importância com que a LGPD deve ser abordada nos órgãos públicos, com destaque para a administração pública federal. Há grande ventilação do tema no setor privado, pois a discussão é bastante comum em se tratando de grandes empresas dos setores financeiro e de telecomunicações, todavia as Universidades Públicas também possuem gigantescos bancos de dados acumulados ao longo de décadas, muitos em processo de digitalização. Dessa forma, nada mais coerente do que debruçar no assunto, a fim de contribuir com uma gestão universitária que garanta a integridade das informações pessoais armazenadas.

Além dos trabalhos acadêmicos que tratam do assunto, já existem alguns documentos produzidos por universidades públicas no Brasil, num movimento para adequação à LGPD, a exemplo do que acontece na Universidade Federal do Rio de Janeiro - UFRJ, onde já há desde 2020 um Comitê de Governança Digital, instituído pela reitora. Este órgão colegiado estratégico, permanente e de caráter deliberativo, com competências normativas, consultivas e deliberativas acerca das políticas gerais para governança digital, tecnologias da informação e comunicação e áreas afins (UFRJ, 2021).

A Universidade Federal Fluminense - UFF apresenta uma página pouco mais organizada que a instituição da capital do estado, pelo menos do que se depreende do *site* e sobre a temática de proteção de dados, visto que apresenta documentos relativos ao grupo de trabalho que estudou a aplicação da LGPD na universidade, bem como já indica logo abaixo o *link* para acesso a cursos gratuitos sobre a lei ora analisada (UFF, 2022).

A Universidade Federal da Bahia - UFBA também se destaca nesse quesito, indicando vários arquivos contendo manuais, guias e textos explicativos sobre a aplicação da LGPD. A Universidade Federal do Rio Grande do Sul - UFRGS, além dos tipos de documentos já citados, fez questão de elaborar uma planilha, inserida abaixo:

Tabela 1 - Dados pessoais e sensíveis da UFRGS

Vínculos com a UFRGS	Dados pessoais e dados pessoais sensíveis tratados pela UFRGS
Alunos	Dados para identificação, dados acadêmicos, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos, dados necessários ao cumprimento de obrigação legal ou regulatória e políticas públicas.
Servidores (ativo/inativo)	Dados para identificação, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos, dados necessários ao cumprimento de obrigação legal ou regulatória.
Colaboradores	Dados para identificação, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos, dados necessários ao cumprimento de obrigação legal ou regulatória.
Colaboradores Terceirizados	Dados para identificação, dados necessários a benefícios e direitos, dados necessários ao cumprimento de obrigação legal ou regulatória.
Fornecedores ou Conveniados	Dados para identificação, dados necessários à classificação da organização, dados necessários ao cumprimento de obrigação legal, financeira ou regulatória.
Candidatos em processos seletivos e licitatórios	Dados para identificação, dados necessários à reserva de vaga e política de cotas, dados necessários a benefícios e direitos.
Familiares de alunos	Dados para identificação do aluno, dados necessários à reserva de vaga e política de cotas, quando aplicável ao caso. Dados necessários ao cumprimento de obrigação legal ou regulatória e políticas públicas.
Familiares de servidores	Dados para identificação, dados necessários a benefícios e direitos, dados necessários ao cumprimento obrigação legal ou regulatória.

Familiares de candidatos em processos seletivos ou licitatórios	Dados para identificação, dados necessários à reserva de vaga e política de cotas, quando aplicável ao caso.
Participantes de eventos	Dados para identificação, dados necessários a benefícios e direitos.
Usuários de serviços disponibilizados pela UFRGS à comunidade	Dados para identificação, dados necessários ao uso do serviço.

Fonte: UFRGS, 2022.

Além disso, também apresenta de modo sucinto os tipos de tratamento de dados pessoais e dados pessoais sensíveis realizados: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência e extração (UFRGS, 2020).

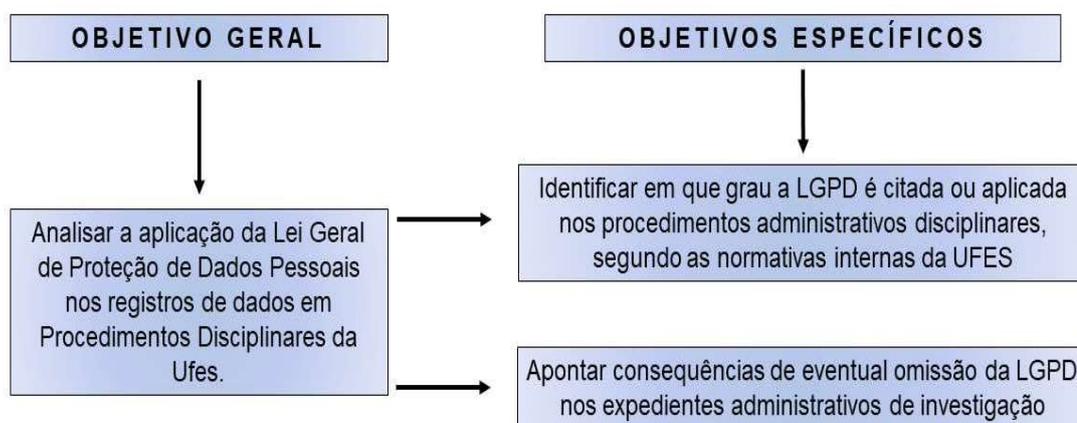
Outro caso interessante é o da Universidade Federal de Minas Gerais - UFMG, que possui um termo de consentimento para tratamento de dados pessoais, que é preenchido pelos candidatos de concurso público destinado aos cargos de magistério. Esse documento é gerado pela Pró-reitoria de Recursos Humanos da referida instituição (UFMG, 2021).

3 MÉTODOS E PROCEDIMENTOS

A presente seção trata dos aspectos metodológicos adotados na execução da pesquisa realizada no âmbito da instituição estudada, a Universidade Federal do Espírito Santo - Ufes.

A Figura 2 apresenta os objetivos buscados durante os procedimentos da pesquisa.

Figura 2 – Objetivos



Fonte: Elaboração própria

O quadro a seguir, demonstra de forma pormenorizada a conexão entre os objetivos específicos, os dados coletados, a forma de tratamento e os resultados obtidos através de cada caminho percorrido.

Quadro 1 - Matriz de amarração

MATRIZ DE AMARRAÇÃO				
Objetivos específicos	Conceitos	Coleta de dados	Tratamento de dados	Resultados
Identificar em que grau a LGPD é citada ou aplicada nos procedimentos administrativos disciplinares, segundo as normativas internas da UFES	Dados pessoais Dados sensíveis Tratamento de dados	Sites da Ufes Artigos e trabalhos acadêmicos Sistema de protocolo digital da Ufes	Leitura comparativa entre os documentos	Manuais utilizados não preveem a LGPD Sistema de protocolo possui brechas para vazamento de dados
Apontar consequências de eventual omissão da LGPD nos expedientes administrativos de investigação	Procedimentos correccionais	Manual da CGU Documentos gerados em outras universidades federais Artigos e trabalhos acadêmicos	Leitura comparativa entre os documentos	Manual da CGU ainda é falho nesse aspecto, podendo ocasionar vazamento de dados Pode gerar sanções e processos judiciais contra a Ufes

Fonte: Elaboração própria

3.1. ABORDAGEM E TIPO DE PESQUISA

Esta pesquisa foi elaborada dentro da abordagem qualitativa uma vez que demanda levantamentos de dados nominais, subjetivos e valorativos. Por meio desta é que se contextualiza o fenômeno, tornando viável a averiguação (GIL, 2019).

Em outra dimensão, a pesquisa realizada apresenta características descritivas, analíticas e bibliográficas, porque foram levantadas informações sobre as regras para processos investigativos em sede administrativa, com base na legislação vigente e nos manuais de procedimentos em uso na Ufes.

No caso da pesquisa bibliográfica, o aporte teórico deve conter três aspectos: as dificuldades de implementação de novas leis no serviço público (lapso temporal); aspectos da ética do uso de dados pessoais, o uso da LGPD em diversos segmentos tais como saúde, pesquisa com seres humanos, registros públicos, processos investigativos em sede administrativa e trabalhos que tenham tido como foco a aplicação da referida lei no âmbito de universidades federais.

3.2. FONTES E NATUREZA DE DADOS

Os dados de natureza qualitativa foram coletados em três fontes, conforme mostrado nos Quadro 2 e Quadro 3.

Quadro 2 – Fontes e natureza dos dados

Tipo da pesquisa	Fonte	Tipo do dado	Coleta dos dados
Descritiva	Constituição da República (1988), Lei nº 12.965/2014, Lei nº 12.527/2011 Lei nº 13.709/2018	Nominal	Levantamento no Diário Oficial da União (DOU)
	Livros, artigos, teses, dissertações e sites	Nominais	Levantamento das fontes em bibliotecas, sites, repositórios, etc
	Processos administrativos	Nominal	Levantamento no sistema de protocolo Lepisma, da Ufes
Bibliográfica	Legislações, livros, teses, dissertações, sites e manuais institucionais	Nominal	Levantamento das fontes em bibliotecas, sites, repositórios, etc
Analítica	Processos	Nominal	Levantamento no sistema de protocolo Lepisma, da Ufes

Fonte: Elaboração própria

Quadro 3 – Coleta e forma de tratamento dos dados

Coleta dos dados	Tratamento dos dados	Forma de tratamento dos dados
Levantamento no Diário Oficial da União (DOU).	Leitura geral para a compreensão; leitura acurada e crítica.	Análise qualitativa
Levantamento das fontes em bibliotecas, sites, repositórios, etc.	Leitura dos índices e resumos para seleção de material pertinente. Leitura acurada do material selecionado. Marcação dos fragmentos de textos para utilização como citações e excertos.	Análise qualitativa
Levantamento no sistema de protocolo Lepisma, da Ufes.	Verificar limitações de inserção e acesso de dados nos processos.	Análise de conteúdo

Fonte: Elaboração própria

Para localização dos trabalhos científicos e artigos que basearam este estudo, utilizou-se a plataforma Google Scholar (Google Acadêmico, no Brasil), valendo-se da combinação alternada entre os termos a seguir relacionados. Por vezes a pesquisa apontava repositórios de universidades brasileiras e sítios eletrônicos governamentais, com referências nacionais e estrangeiras, além de páginas tradicionais de conteúdo jurídico pátrio.

- LGPD e LAI
- Estatuto da Criança e do Adolescente
- Relação trabalhista
- Proteção de dados pessoais
- Universidades federais
- GDPR
- Processo disciplinar / Sindicância
- Gestão de dados
- CGU / TCU

- Serpro
- Manual de boas práticas

No caso, verifica-se a necessidade de analisar a adequação (ou não) dos procedimentos em relação à legislação vigente. Além disso, foram estudadas publicações diversas sobre o tema, com foco no comportamento da Administração Pública ante às novas exigências da Lei Geral de Proteção de Dados, principalmente no que tange à investigação administrativa de responsabilidade de servidores públicos.

3.3. INSTRUMENTOS DE COLETA DE DADOS

Para atingir o objetivo esperado, foi realizada análise da legislação vigente, em especial a LGPD, a LAI e a Constituição da República, acompanhada de informações em sítios eletrônicos vinculados à Seção de Procedimentos Disciplinares da Universidade analisada, à Controladoria Geral da União e demais plataformas públicas que versam sobre a temática. Além disso, verificaram-se eventuais inconsistências no sistema de protocolo Lepisma, quanto à visibilidade indevida de dados pessoais. Foram abordados, também, artigos científicos, notícias e livros publicados sobre os temas abordados. Eventualmente, alguns dados quantitativos foram obtidos junto a tais fontes.

3.4. FORMA DE TRATAMENTO DE DADOS PRETENDIDA

De posse das informações obtidas pelos meios acima descritos, foi feita uma análise de conteúdo, com base na legislação vigente e no conjunto bibliográfico proposto, comparando o apontamento da norma e a realidade, a fim de apontar soluções para o problema em questão, além do produto técnico-tecnológico apresentado ao final da pesquisa.

4 ANÁLISE E DISCUSSÃO DAS INFORMAÇÕES

4.1 A INSTITUIÇÃO PESQUISADA

A Universidade Federal do Espírito Santo - UFES possui natureza jurídica de autarquia, vinculada ao Ministério da Educação, usufruindo de autonomia didático-científica, administrativa e de gestão financeira e patrimonial, atuando para execução de três basilares: ensino, pesquisa e extensão. É composta por onze centros de ensino, dispostos em três polos: Vitória, São Mateus e Alegre, com estruturas complementares em Aracruz, Jerônimo Monteiro e São José do Calçado, visando atender pesquisas específicas de certas áreas de estudo. A Administração Central é exercida pelo Gabinete da Reitoria, ao qual estão vinculadas as seguintes Pró-Reitorias: Pró-Reitoria de Administração (PROAD); Pró-Reitoria de Assuntos Estudantis e Cidadania (PROAECI); Pró-Reitoria de Extensão (PROEX); Pró-Reitoria de Gestão de Pessoas (PROGEP); Pró-Reitoria de Graduação (PROGRAD); Pró-Reitoria de Pesquisa e Pós-Graduação (PRPPG); Pró-Reitoria de Planejamento e Desenvolvimento Institucional (PROPLAN).

Alguns setores também vinculados ao Gabinete da Reitoria exercem atividades específicas, como é o caso da Seção de Procedimentos Disciplinares - SPD, que atua como órgão correcional quanto às demandas disciplinares referentes a condutas dos servidores públicos lotados na UFES. Sua atuação está indicada no Decreto nº 5.480, de 30/06/2055 e na Portaria Normativa CGU nº 27, de 11/10/2022 da Controladoria Geral da União – CGU.

Esta Seção concentra seus esforços em comissões de procedimentos administrativos investigativos, acusatórios, punitivos, processos administrativos disciplinares, designadas pelo Reitor, além de oferecer apoio técnico, dentro do que a lei determina, às demais comissões criadas pelo Reitor e demais Autoridades das Unidades Acadêmicas e Administrativas da Ufes.

No que se refere à plataforma de protocolo Lepisma, há duas frentes de trabalho envolvidas: a Diretoria de Documentação Institucional - DDI, vinculada à Pró-reitoria de Administração - PROAD, e a Superintendência de Tecnologia da Informação - STI, órgão suplementar, que responde diretamente ao Gabinete da Reitoria.

4.2 MANUAIS E DOCUMENTOS ANALISADOS

Conforme já mencionado no item anterior, cabe à SPD, na qualidade de verificador dos procedimentos administrativos disciplinares, basear sua atuação por meio do Manual de Processo Administrativo Disciplinar, documento produzido pela Controladoria-Geral da União, em Brasília. A edição em uso é a que fora publicada em maio de 2022, atualizada até o mês de março do mesmo ano.

Pelas informações do próprio *site* da SPD, a edição de 2022 do manual chega com as seguintes atualizações:

- a) Revogação do Decreto nº 5.483, de 30 de junho de 2005, pelo Decreto nº 10.571, de 9 de dezembro de 2020 (p. 15, 54/58, 249/252);
- b) revisão das referências às unidades correccionais, conforme alteração no Decreto nº 5.480, de 30 de junho de 2005, promovida por meio do Decreto nº 10.768, de 13 de agosto de 2021 (p. 13/14, 252);
- c) inovações decorrentes da Lei nº 14.230, de 25 de outubro de 2021, que incorporou relevantes alterações à Lei de Improbidade Administrativa, Lei nº 8.429, de 2 de junho de 1992 (p. 15, 23, 28, 54, 209, 217/218, 225/230, 241/246, 250, 258);
- d) inclusão de referência ao artigo “Dosimetria das Sanções Administrativas Disciplinares – Advertência e Suspensão”, de autoria dos servidores Amanda Patrícia Souza Dutra Melo, José Ernane Barbosa de Castro e Cláudia Raquel Leão Brizolla (p. 290, 377);
- e) ajuste ao quadro que apresenta as diferenças entre abandono de cargo e inassiduidade habitual (p. 239);
- f) ajustes gerais na formatação e na pontuação (UFES, 2022).

Em caráter paralelo, há também disponível no sítio eletrônico da SPD o Manual de Conduta do Agente Público Civil do Poder Executivo Federal, que não versa sobre as questões procedimentais investigativas e punitivas, mas sobre o padrão de comportamento a ser adotado pela categoria. Este documento foi disponibilizado pela Secretaria de Gestão e Desempenho de Pessoal, vinculada ao Ministério da Economia, publicado em 2020, sendo essa a 1ª edição.

Como o documento que pauta o procedimento investigativo é gerado pela CGU, é válido efetuar busca junto ao repositório desta, a fim de que se verifique se há algo mais específico que, eventualmente, a Universidade tenha deixado de fora. Na parte do *site* que trata do tema “Correição”, há uma série de documentos dispostos em

ordem cronológica de publicação, com manuais, orientações, coletâneas e cursos de assuntos relacionados ao escopo do órgão. Entretanto, para surpresa do pesquisador, mesmo nesse endereço, apenas um dos documentos trazia alguma previsão acerca da LGPD, qual seja o Manual de Responsabilização de Entes Privados, aplicado a pessoas jurídicas de direito privado. Ainda assim, a menção é extremamente rasa:

A Lei nº 13.709/2018 (Lei de Proteção de Dados Pessoais) dispôs sobre o conceito de dado pessoal sensível, “(...) sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (inciso II do artigo 5º). (CGU, 2020)

No caso, a menção à LGPD é apenas para resgatar o conceito de dado pessoal sensível, que já era trazido pela LAI, cujo teor deve ser restringido, na forma do texto legal. Mas além disso, nada mais é mencionado no referido manual. Vale frisar que a edição 2022 deste manual repete o mesmo texto acima descrito, sem trazer maiores informações sobre o tema. A CGU, claro, possui um manual próprio para a LGPD, com disposições gerais, chamado Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD), publicado em 14 de agosto de 2020. Apesar de ser bastante extenso o conteúdo, ele traz aspectos gerais da lei, pois é destinado a todos os integrantes da administração pública federal. Logo, de certa forma é compreensível o fato de não caber nesse documento uma abordagem com tamanha especificidade.

4.3 PLATAFORMA LEPISMA

No âmbito da Ufes, a plataforma *online* de protocolo, denominada Lepisma, é o meio pelo qual são tramitados os processos administrativos, físicos e digitais. A imagem abaixo representa a tela inicial do sítio eletrônico <https://protocolo.ufes.br/>. A página é aberta ao público, para a modalidade ‘consulta’, sendo possível visualizar os documentos em tramitação ou mesmo arquivados.

Para os servidores da Ufes, técnicos ou professores, existe a possibilidade de fazer acesso com a senha única (*login* e senha individuais de cada servidor), permitindo acessar outras funcionalidades como autuação de novos documentos, assinar

arquivos digitalmente, gerar relatórios de tramitações, reencaminhar documentos, dentre outros a depender do nível de acesso que o servidor possua. Esse nível muda conforme as necessidades do setor de lotação, do cargo e da função. Chefes de setor costumam usufruir desse maior número de possibilidades na plataforma.

A página inicial oferece algumas opções: (a) protocolo, opção exclusiva para servidores, a fim de autuar, tramitar e consultar documentos; (b) consulta, opção de uso livre, sem necessidade de realizar *login*, que qualquer cidadão pode acessar; (c) utilitários, sem realizar *login*, permite consolidar as peças de um processo em um único documento em formato PDF; (d) ajuda, disponibiliza material de suporte e tira dúvidas quanto ao uso do sistema; (e) legislação, abre uma página do *site* da DDI/PROAD, que menciona todas as legislações aplicáveis aos registros de informações na Administração Pública Federal.

Figura 3 - Tela inicial da plataforma Lepisma



Fonte: UFES, 2023^a

O servidor, quando está manuseando os processos na plataforma, estando o documento em sua caixa postal, consegue inserir novas peças (ofícios, relatórios, portarias, imagens, dentre outros), consoante imagem abaixo. Ao fazê-lo, o sistema pergunta o tipo de documento (Cópia autenticada administrativamente de via original, Cópia autenticada administrativamente de via autenticada em cartório,

Cópia simples ou Via original nato-digital). Ao lado, insere-se a informação se aquela peça deve ser nível de acesso público ou restrito.

Ao escolher a opção 'restrito', abre-se um campo para indicar o motivo da restrição. O sistema apresenta as seguintes justificativas: (1) Controle interno (Art. 26, § 3º, da Lei nº 10.180/2001); (2) Direito autoral (Art. 24, Inciso III, da Lei nº 9.610/1998); (3) Documento preparatório (Art. 7º, § 3º, da Lei nº 12.527/2011); (4) Informação pessoal (Art. 31 da Lei nº 12.527/2011); (5) Informações privilegiadas de Sociedades Anônimas (Art. 155, § 2º, da Lei nº 6.404/1976); (6) Interceptação de comunicações telefônicas (Art. 8º, caput, da Lei nº 9.296/1996); (7) Investigação de responsabilidade de servidor (Art. 150 da Lei nº 8.112/1990); (8) Livros e registros contábeis empresariais (Art. 1.190 do Código Civil); (9) Operações bancárias (Art. 1º da Lei Complementar nº 105/2001); (10) Proteção da propriedade intelectual de software (Art. 2º da Lei nº 9.609/1998); (11) Pendente de análise de restrição de acesso (Art. 6º, Inciso III, da Lei nº 12.527/2011); (12) Segredo de Justiça no Processo Civil (Art. 189 do Código de Processo Civil); (13) Segredo de Justiça no Processo Penal (Art. 201, § 6º, do Código de Processo Penal); (14) Segredo industrial (Art. 195, Inciso XIV, da Lei nº 9.279/1996); (15) Sigilo das comunicações (Art. 3º, Inciso V, da Lei nº 9.472/1997); (16) Sigilo de empresa em situação falimentar (Art. 169 da Lei nº 11.101/2005); (17) Sigilo do inquérito policial (Art. 20 do Código de Processo Penal); (18) Situação econômico-financeira de sujeito passivo (Art. 198, caput, da Lei nº 5.172/1966); (19) Laudo de avaliação de uso restrito (NBR 14653-1 Item 10.3); (20) Pesquisa com animais (Art. 6º, § 4º, da Res. Normativa 1/2010). Ou seja, dentre os motivos de restrição de peças num documento, não há nenhuma menção expressa à LGPD, embora apresente uma vasta gama de opções a serem indicadas, com motivos diversos.

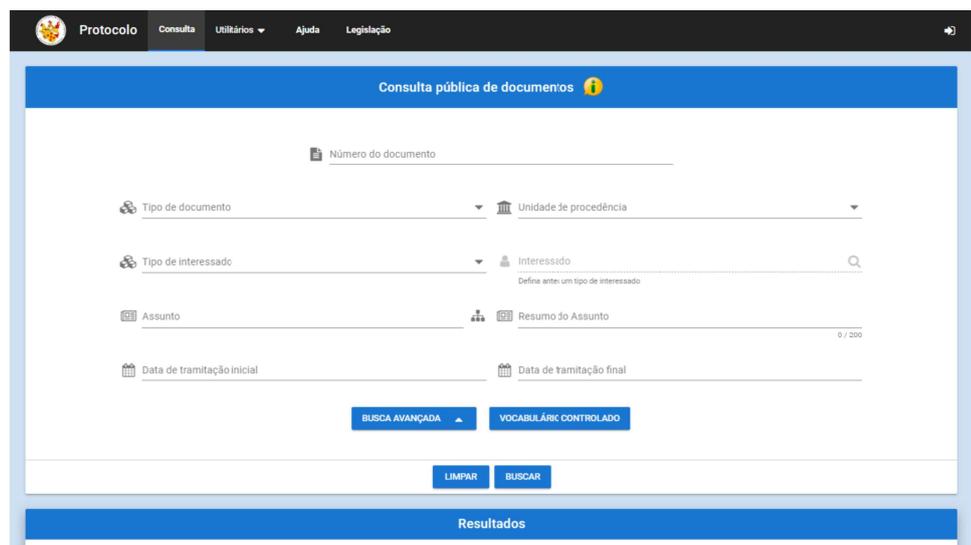
Figura 4 - Inserção de peças na plataforma Lepisma



Fonte: UFES, 2023a

Para os fins da presente pesquisa, com o propósito de simular a possibilidade de exposição de dados pessoais principalmente ao público externo, foi utilizada a opção ‘consulta’ vista na barra superior de cor preta.

Figura 5 - Aba “consulta” e opções de busca

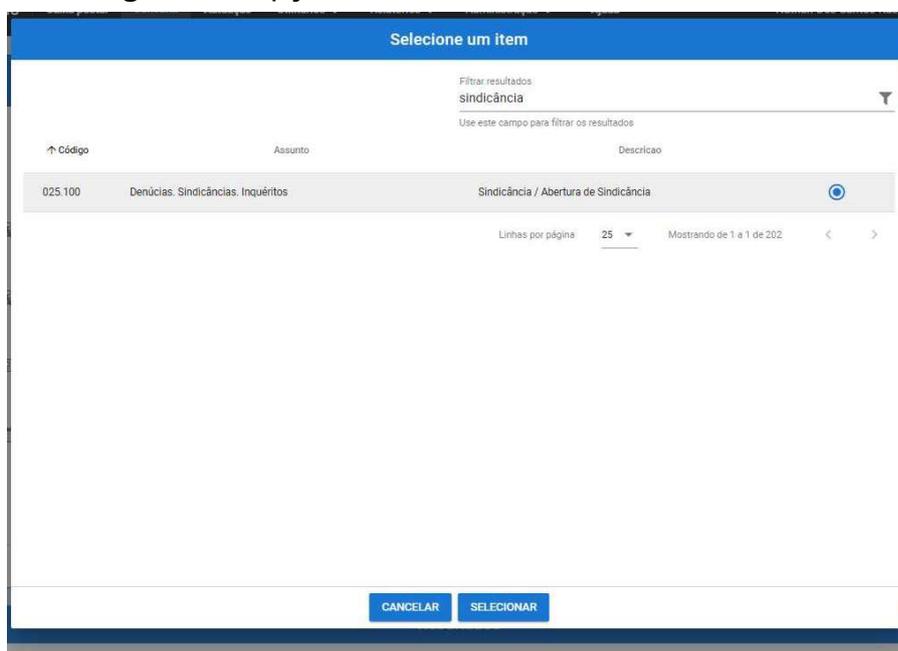


Fonte: UFES, 2023b

Utilizando a opção 'consulta', aparecem vários critérios de pesquisa que podem ser usados cumulativamente: tipo de documento, unidade de procedência, tipo de interessado, nome do interessado, dentre outros.

Para uma busca mais precisa, e considerando que o documento de investigação administrativa foi autuado com essa identificação, usa-se a opção 'vocabulário controlado', que permite escolher o código, assunto e descrição dos documentos que se deseja encontrar. Ao se buscar por 'sindicância', o sistema identifica o código 025.100, Assunto 'Denúncias. Sindicâncias. Inquéritos', com a descrição 'Sindicância / Abertura de Sindicância'.

Figura 6 - Opção de busca 'vocabulário controlado'



Fonte: UFES, 2023b

Após, escolheu-se a data de tramitação inicial como 01 de fevereiro de 2022 e a data de tramitação final como 02 de maio de 2022. Com essas especificações, o primeiro resultado da busca foi o processo nº 23068.080941/2021-72, cujo assunto é 'ADMINISTRAÇÃO GERAL: Pessoal: Apuração de responsabilidade e ação disciplinar: Denúncias. Sindicâncias. Inquéritos' e resumo 'Instaura Sindicância Investigativa.'. Ao analisar as peças do processo, vê-se que algumas peças constam como restritas, indicando o seguinte: 'Informação pessoal (Art 31 da Lei nº 12.527/2011) fazendo menção ao artigo da LAI que diz o seguinte:

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem (BRASIL, 2022f)

Outro documento restrito consta o seguinte: 'RESTRITO - Motivo: Investigação de responsabilidade de servidor (Art 150 da Lei nº 8.112/1990)'. Nesse caso, a restrição se deu em virtude da previsão da lei que institui o Regime Jurídico dos Servidores Públicos Federais, *in verbis*:

Art. 150. A Comissão exercerá suas atividades com independência e imparcialidade, assegurado o sigilo necessário à elucidação do fato ou exigido pelo interesse da administração.

Parágrafo único. As reuniões e as audiências das comissões terão caráter reservado (BRASIL, 2022).

Em ambos os casos, provavelmente, o mecanismo de restrição foi aplicado de maneira correta, sendo um dos documentos um Termo de Ajuste de Conduta contendo dados dos envolvidos. Ocorre que, bastando uma breve análise dos autos é possível encontrar outras peças que contém o nome do investigado, seu número de matrícula SIAPE, telefone de contato pessoal, *email* pessoal, dentre outras informações.

O segundo resultado da busca é o processo digitalizado nº 23068.015580/2018-98. Digitalizado porque o início de sua tramitação se deu por meio de autos físicos, mas que durante o seu desenrolar foi digitalizado, para facilitar seu manuseio. No caso desse processo, há uma série de peças com acesso restrito, por conta do Art 26, §3º, da Lei nº 10.180/2001, que diz:

Art. 26. Nenhum processo, documento ou informação poderá ser sonegado aos servidores dos Sistemas de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, no exercício das atribuições inerentes às atividades de registros contábeis, de auditoria, fiscalização e avaliação de gestão. [...]

§ 3º O servidor deverá guardar sigilo sobre dados e informações pertinentes aos assuntos a que tiver acesso em decorrência do exercício de suas funções, utilizando-os, exclusivamente, para a elaboração de pareceres e relatórios destinados à autoridade competente, sob pena de responsabilidade administrativa, civil e penal (BRASIL 2022d).

Entretanto, seguindo o padrão do primeiro caso exposto, logo no início do processo há uma peça contendo uma listagem de nomes de servidores com seus respectivos números de CPF. Há também um formulário de bolsista, contendo número de telefone pessoal, endereço residencial, *email* pessoal, número de CPF e RG.

O terceiro resultado da busca é um processo digital 23068.022955/2021-71, mais especificamente uma comissão de sindicância para analisar um processo de prestação de serviço de vigilância patrimonial no campus da Ufes em São Mateus/ES. Tal qual os outros dois processos anteriores, há uma série de peças com restrição de acesso, visto que se trata de apuração de responsabilidade de servidor, o que por si só já demanda sigilo de certos documentos. Entretanto há uma grande quantidade de peças com dados pessoais dos empregados, como CPF, conta bancária, holerites, dentre outros. E isso ocorre algumas vezes ao longo do processo, erro cometido por servidores distintos, de setores diversos.

4.4 RESULTADOS

Nota-se, portanto, um padrão entre os processos pesquisados: há restrição das peças contendo dados pessoais (sensíveis ou não), todavia esse filtro é falho, visto que depende da análise do servidor e o sistema de protocolo não faz distinção entre as informações, mas apenas as insere no processo. Além disso, vê-se que boa parte das restrições se dá em virtude de outros fatores que não sejam necessariamente a existência de dados pessoais nos documentos.

Outro ponto importante a ser considerado é que, com os parâmetros de busca adotados, encontramos apenas os processos que foram cadastrados formalmente

como Denúncias/Sindicâncias/Inquéritos. Se porventura foram abertos documentos avulsos ou processos digitais comuns, por certo serão encontradas outras inconsistências e erros por parte dos servidores envolvidos.

Com tantas brechas no cadastro processual para comissões e investigações administrativas, fica o questionamento: como reduzir essa exposição massiva de dados pessoais? Restringir o acesso ao processo inteiro seria inviável, por ir de encontro ao conceito de transparência pública, afinal nem todos os dados inseridos são passíveis de restrição. Primeiro ponto a ser levado em conta é a necessidade urgente de capacitação do corpo de servidores, questão já tratada anteriormente nesta pesquisa. Tanto acerca do bom uso da plataforma (conhecendo suas ferramentas e funcionalidades) quanto à necessidade de dominar a inserção de informações. Por vezes é possível ver dados pessoais nos textos de despacho (para estes não há possibilidade de restrição de acesso), até mesmo dados envolvendo questões de saúde das pessoas interessadas, como laudos médicos. Isso tudo por descuido de quem fez a tramitação.

Outro ponto seria, eventualmente, a Auditoria Interna da Ufes realizar análise processual por amostragem, com processos dessa natureza, para mitigar erros como os narrados acima, visto que as peças cadastradas como públicas podem ser restringidas posteriormente à sua inserção. Outra opção seria de responsabilidade da STI e da PROAD, definindo um fluxo fechado para os processos de investigação, impedindo que seu manuseio (inserção de despachos, documentos e tramitações) se dê por pessoas alheias à averiguação. No que se refere à legislação, já se falou acerca da importância da ANPD para fiscalização e sanção das entidades infratoras. Entretanto, como já visto, além da extensa *vacatio legis* conferida à legislação, a estruturação tardia da autoridade competente criou um terreno fértil para vazamento de dados, mesmo com a lei em vigor:

Ainda que a presença de um regulamento que trate da fiscalização e aplicação de sanções pela autoridade seja de extrema importância, uma vez que proporciona ao administrado proteção e segurança jurídica pela observância do princípio do devido processo legal adjetivo, revela-se uma contradição: como haverá a efetivação dos procedimentos de fiscalização e de sanção sem a existência de uma norma que estabeleça previamente a tipificação das condutas ilícitas passíveis de sanção? Ressalte-se que a falta de previsão de infrações causa a judicialização de questões que envolvem a LGPD, mas que deveriam ou poderiam ser solucionadas na esfera administrativa. (OLIVEIRA; PIRES, 2022, s.p.).

Basicamente, criou-se um cenário no qual há uma norma a ser cumprida, há um órgão competente para fiscalizar e punir, mas as punições respectivas costumam a acontecer. Não se trata de um tema de pequena relevância, nem de consequências desprezíveis quando há o descumprimento dessa norma. Essa demanda ainda carece de cuidados por parte do Governo Federal, da ANPD e das entidades públicas e privadas, especialmente a Ufes.

5 CONSIDERAÇÕES FINAIS

Neste trabalho, pôde-se perceber a necessidade real de adequação à LGPD, em todos os campos, visto que afeta temas tão delicados como a ética e a privacidade dos indivíduos. E isso vai além do cidadão, perpassando as instituições que compõem nossa sociedade, como bem prevê a lei em questão.

Sabe-se que o uso indiscriminado de dados pessoais, sem o consentimento dos titulares, é extremamente nocivo à sociedade, tanto que há anos temos inúmeros casos de vazamentos de dados pessoais, com consequências nas esferas civil, penal e administrativa. E isso afeta também as universidades públicas federais, em virtude da grande quantidade de pessoas que têm suas rotinas vinculadas a estas, seja por estudo, trabalho ou conexão com os projetos que são desenvolvidos.

Foi visto que a ética e a privacidade são dois valores constitucionais que norteiam a LGPD, temas caros ao constituinte pátrio e que estão sendo colocados em xeque com os avanços tecnológicos cada vez mais céleres, o que costuma não dar tempo ao legislador para adequar a norma vigente aos impactos que as mudanças causam, trazendo grande desconforto ao jurisdicionado, que se vê sem mecanismos legais para se defender ante às ofensas sofridas, e às relações sociais, que ficam estremecidas e sem garantias básicas contra os que operam na ilegalidade.

A Ufes nesse contexto ainda caminha a passos lentos. Como foi mencionado na pesquisa, embora haja um plano de adequação à Lei Geral de Proteção de Dados Pessoais, envolvendo os altos cargos da instituição e uma divisão de atribuições, essa discussão não desce para as camadas mais baixas, o 'chão de fábrica', onde há contato direto com dados pessoais de alunos, professores, técnicos e até mesmo da sociedade que usufrui dos serviços prestados pela universidade. Quando o assunto é mais espinhoso, no caso dos procedimentos investigativos, a situação se agrava, pela falta de informação e de mecanismos que a Ufes oferece aos servidores, bem como da legislação aplicável.

Quanto aos sistemas que a Universidade utiliza nos seus expedientes administrativos, destaca-se a plataforma de protocolo Lepisma que, como já visto no presente trabalho, carece de mecanismos de proteção contra vazamento de informações. Qualquer pessoa pode acessá-la de seu *smartphone*, *tablet* ou

computador, podendo consultar informações dos processos que tramitam na Ufes. Caso o servidor tenha inserido documentos com dados pessoais, sem colocar restrição de acesso, ele fica visível para todos e disponível para *download*, independentemente de *login* com senha Ufes.

Caso pior pode ocorrer quando o servidor insere dados pessoais no corpo do despacho, para os quais a visualização sempre é livre. São questões que competem ser resolvidas pela STI e pela DDI, possivelmente determinando que haja tramitação em fluxo fechado para procedimentos investigativos e exigindo que as peças desse tipo de procedimento sejam restringidas à consulta livre.

O cenário é ainda mais preocupante, tendo em vista que a proteção de dados pessoais alcança, sim, os procedimentos administrativos, mas também afeta diretamente as pesquisas acadêmicas de vários cursos distintos e atinge também as questões de saúde pública, considerando que a Ufes não só possui cursos dessa área, mas também faz atendimentos diários à população (notadamente na medicina e odontologia). Essa interseção sociedade-Ufes precisa de cuidados quanto à proteção dos dados sensíveis.

Outras universidades federais, como mostrado na pesquisa, embora já disponibilizem mais lastro aos seus colaboradores, ainda falta especificidade quanto aos procedimentos investigativos, o que parece que ainda vai levar algum tempo para que o tema alcance todas as discussões e processos de trabalho no meio acadêmico, como já ocorre com a pesquisa científica e com a área de tecnologia da informação.

Um tópico que merece destaque é a postura dos órgãos de controle e correção, principalmente da CGU, pelo menos quanto ao material publicado em seu sítio eletrônico. A impressão que há é a de que todos estão se adequando a passos lentos: quem fiscaliza (ANPD, CGU, ...) faz 'vistas grossas' e os fiscalizados (empresas, universidades, ...) apresentam pouco a pouco algumas adequações, como forma de prestação de contas ao Estado e à sociedade civil. Fato é que sem as devidas mudanças, projetos maiores que porventura envolvam instituições de fora do país, ficam prejudicados.

No cenário europeu, a GDPR já exige harmonia das entidades em relação à legislação vigente e, caso as universidades brasileiras não estejam respeitando a LGPD, a cooperação para fins de pesquisa fica bastante prejudicada. No final das contas, quem perde com isso? Alunos, professores, universidades e, por consequência, o Brasil.

Vê-se que o tema já é de franca discussão, dentro e fora do setor público, todavia, há campos da legislação nos quais os juristas, especialmente das áreas de Direito Administrativo e Constitucional precisam se posicionar e isso também se aplica para o Poder Judiciário, em todas as suas esferas, no intuito de estabelecer entendimentos mais sólidos sobre os institutos legais ora analisados.

Ao longo do presente trabalho, foi possível verificar que mesmo após quatro anos da sanção da Lei Geral de Proteção de Dados Pessoais, ainda há muitos questionamentos sem respostas e desafios a serem vencidos. No contexto universitário embora haja movimentações muito positivas, ainda serão necessários alguns anos para adequação dos procedimentos administrativos e sistemas digitais, de modo que o respeito e zelo com os dados pessoais se torne algo orgânico do serviço público nas instituições federais de ensino, inclusive na Ufes.

O produto técnico-tecnológico gerado a partir da presente pesquisa é uma proposta para, enfim, tornar a discussão do tema mais próxima de onde há constante atividade com dados pessoais, podendo, inclusive, servir de base até mesmo para um futuro curso de capacitação. A mudança cultural é o termo chave para vencer essa pendência.

O manual de boas práticas gerado a partir deste trabalho está apto ao uso imediato e apresenta um panorama da legislação e sua aplicação em expedientes internos da Ufes. Com esse documento objetiva-se veicular, entre os servidores da UFES, informações básicas acerca da aplicação da lei de proteção de dados quanto aos registros de informações, com um tópico específico acerca dos processos disciplinares, visto que o trabalho de origem identificou pontos frágeis na plataforma de protocolo Lepisma, que permitem vazamento de dados pessoais, caso haja manuseio descuidado do sistema. O fato de conter um tópico específico quanto a processos disciplinares é um diferencial, não encontrado em documentos similares

produzidos por outras universidades no país. Obviamente, o material pode ser melhorado com o passar do tempo, adequando-se a determinadas situações e necessidades futuras.

Os impactos pretendidos são voltados a uma melhor compreensão dos aspectos legislativos por parte da comunidade universitária, prevenindo contra violações da LGPD, sendo ponto de partida para uma mudança cultural entre os servidores que utilizam os sistemas da UFES. Como os dados tratados dizem respeito não só aos servidores, mas também a todos da sociedade que utilizam as dependências e serviços da Universidade, trata-se de um projeto cujos resultados extrapolam os limites do campus, trazendo benefícios coletivos.

REFERÊNCIAS

ALBUQUERQUE, Ruth Mayara Guedes de Andrade. **Gestão da informação pessoal realizada em universidade federal**: resultado de auditoria baseada em riscos. 2020. 185f. Dissertação (Mestrado Profissional em Gestão da Informação e do Conhecimento) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2020.

ALCÂNTARA, C. D. G. de. **Impactos da Lei Geral de Proteção de Dados nas relações de trabalho**. Monografia em Direito – Pontifícia Universidade Católica de Goiás. 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1472>. Acesso em 09 nov. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2013. Tecnologia da informação. Técnicas de segurança. **Sistemas de gestão da segurança da informação**. Requisitos. Rio de Janeiro: 2006.

BARRETO, M. L.; ALMEIDA, B. de A.; DONEDA, D. Uso e Proteção de Dados Pessoais na Pesquisa Científica. In: **Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias**. RDU, Porto Alegre, Volume 16, n. 90, 2019, 179-194, nov-dez 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3895/Doneda%3B%20Barreto%3B%20Almeida%2C%202019>. Acesso em: 28 dez. 2022.

BARBOSA, Tatiane Santos et al. A Lei Geral de Proteção de Dados (LGPD) nas instituições públicas de ensino: possíveis impactos e desafios. In: VII ENPI-Encontro Nacional de Propriedade Intelectual. 2021. **Anais Eletrônicos**. Disponível em: <https://www.api.org.br/conferences/index.php/ENPI2021/ENPI2021/paper/viewFile/1455/768>. Acesso em 03 dez. 2022.

BASAN, A. P. A Lei Geral de Proteção de Dados Pessoais e a tutela dos direitos fundamentais nas relações privadas. **Revista Jurídica Eletrônica da Universidade Federal do Piauí**, v. 8, n. 1, jan/jun 2021. Disponível em: <https://revistas.ufpi.br/index.php/raj/article/view/10578/8047>. Acesso em: 18 dez. 2022

BECKER et al. **Ensaio sobre a cegueira**: Covid-19 e postergação da vacatio legis da LGPD. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/ensaio-sobre-a-cegueira-covid-19-e-postergacao-da-vacatio-legis-da-lgpd-20032020>. Acesso em: 22 dez. 2022.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas– Unifafibe**, v. 8, n. 2, p. 18, 2020. Disponível em: <https://apshotspot.com.br/wp-content/uploads/elementor/forms/Botelho,Marcos-C%C3%A9sar-A-LGPD-e-prote%C3%A7%C3%A3o-dados-crian%C3%A7as-e-adolescentes-artigo.pdf>. Acesso em: 28 nov. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 dez. 2022a.

_____. **Lei nº 8.069**, de 13 de julho de 1990. Estatuto da Criança e do Adolescente. Planalto, 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8069compilado.htm. Acesso em: 21 nov. 2022b.

_____. **Lei nº 8.112**, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Acesso em: 05 dez. 2022c.

_____. **Lei nº 10.180**, de 06 de fevereiro de 2001. Organiza e disciplina os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10180.htm. Acesso em: 28 dez. 2022d.

_____. **Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Planalto, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 24 dez. 2022e.

_____. **Lei nº 12.527**, de 18 de novembro de 2011. Acesso à Informação. Planalto, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 dez. 2022f.

_____. **Lei nº 12.965**, de 23 de abril de 2014 nº 12.965, de 23 de abril de 2014. Lei do Marco Civil da Internet. Planalto, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965htm. Acesso em: 12 nov. 2022g.

_____. **Lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 23 maio 2022h.

_____. Ministério da Economia. Secretaria de Gestão e Desempenho de Pessoal. **Manual de Conduta do Agente Público Civil do Poder Executivo Federal**. Brasília, 2020. Disponível em: <https://spd.ufes.br/sites/spd.ufes.br/files/field/anexo/manual-de-conduta-do-agente-publico-civil.pdf>. Acesso em: 11 dez. 2022i.

_____. **Portaria nº 554, de 11 de março de 2019**. Dispõe sobre a emissão e o registro de diploma de graduação, por meio digital, pelas Instituições de Ensino Superior - IES pertencentes ao Sistema Federal de Ensino. Disponível em:

<https://abmes.org.br/legislacoes/detalhe/2710/portaria-mec-n-554>. Acesso em: 12 dez. 2022j.

CARNEIRO, Isabelle da Nóbrega Rito; SILVA, Luiza Caldeira Leite; TABACH, Danielle. Tratamento de dados pessoais. In: FEIGELSON, Bruno; SIQUEIRA, Henrique Albani (Coord.). **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019.

CHAVES, Joe Luis de Sousa. O impacto da Lei Geral de Proteção De Dados (LGPD) nas investigações administrativas. **Revista Caderno Virtual**. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/download/5362/2135>. Acesso em 29 maio 2022.

CONTROLADORIA GERAL DA UNIÃO – CGU. **Manual de Processo Administrativo Disciplinar**. Brasília, 2021. Disponível em: https://spd.ufes.br/sites/spd.ufes.br/files/field/anexo/manual_pad_2021_1.pdf. Acesso em 29 maio 2022.

CONTROLADORIA GERAL DA UNIÃO - CGU. **Manual de Responsabilização de Entes Privados**. Brasília, 2020. Disponível em: <https://repositorio.cgu.gov.br/handle/1/45545>. Acesso em: 15 jan. 2023.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, v. 9, n. 1, p. 1-38, 2020.

FERREIRA, Lamara; OKANO, Marcelo T. **Um panorama da implementação da LGPD no Brasil: uma pesquisa exploratória com 216 profissionais**. 2021. Disponível em: https://www.researchgate.net/profile/Marcelo-Okano-2/publication/356555146_Um_p_anorama_da_implementacao_da_LGPD_no_Brasil_uma_pesquisa_exploratoria_com_216_profissionais/links/61a05cb83068c54fa51db117/Um-panorama-da-implementacao-da-LGPD-no-Brasil-uma-pesquisa-exploratoria-com-216-profissionais.pdf. Acesso em 28 mar 2022.

FERREIRA, Luiz Antonio Miguel; DOI, Cristina Teranise. **A proteção integral das crianças e dos adolescentes vítimas**. Sl: sn, 2018. Disponível em: https://crianca.mppr.mp.br/arquivos/File/doutrina/protecao_integral_ferreira.pdf. Acesso em 18 dez. 2022.

FLOWTI. **Como escolas e universidades devem se preparar para a LGPD?: As escolas e universidades precisam estar preparadas para a Lei Geral de Proteção de Dados (LGPD), que entrará em vigor em breve**. 2020. Disponível em: <https://flowti.com.br/blog/como-escolas-e-universidades-devem-se-preparar-para-a-lgpd>. Acesso em 28 maio 2022.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

_____. **Métodos e técnicas de pesquisa social**. 7. ed. - São Paulo: Atlas, 2019.

INSTITUTO DE TECNOLOGIA E SOCIEDADE - ITS. **Lei Geral De Proteção de Dados Pessoais (LGPD) e Setor Público: Um guia da Lei 13.709/2018, voltado**

para os órgãos e entidades públicas. 2019. Disponível em: <https://itsrio.org/wp-content/uploads/2019/05/LGPD-vf-1.pdf>. Acesso em 4 abril 2022.

JUNIOR, Fretz Sievers. Lei Geral De Proteção de Dados, Lei de Acesso à Informação e a improbidade administrativa: Um Novo Cenário Para O Agente Público Na Sociedade Da Informação. **Conhecimento Interativo**, São José dos Pinhais/PR, v. 14, n. 2, p. 292-307, jul/dez. 2020. Disponível em: <http://app.fiepr.org.br/revistacientifica/index.php/conhecimentointerativo/article/view/460/474>. Acesso em: 12 jan. 2022.

KONDER, Carlos. Privacidade e corpo: convergências possíveis. **Pensar**, Fortaleza, v. 18, n. 2, maio-ago. 2013, p. 354-400. Disponível em: <https://periodicos.unifor.br/rpen/article/view/2696/pdf>. Acesso em: 15 jan. de 2023.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. RM Digital Education. 2019.

MURARI, G. A. C.; SCHIAVON, I. N.; BARRETOS, R. A. Dados pessoais: tratamento realizado pelo poder público à luz da Lei Geral de Proteção de Dados. **Revista Judiciária**, 2021. Disponível em: <http://www.revistajudiciaria.com.br/wp-content/uploads/2021/12/Revista-Judiciaria-22-Novembro-2021-PRONTA-19-10-2021-10hs.pdf#page=245https://conteudojuridico.com.br/consulta/artigos/55320/os-impactos-da-lei-geral-de-proteo-de-dados-lgpd-na-administrao-pblica-federal>. Acesso em: 15 dez 2022.

OCDE. **Good Practice Principles for Data Ethics in the Public Sector**. 2020. Disponível em: <https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf>. Acesso em: 07 jan. 2023.

OLIVEIRA, Geveson de Souza. Os impactos da Lei Geral de Proteção de Dados (LGPD) na Administração Pública Federal. **Conteúdo Jurídico**, Brasília-DF: 13 out 2020. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/55320/os-impactos-da-lei-geral-de-proteo-de-dados-lgpd-na-administrao-pblica-federal>. Acesso em: 28 mar 2022.

OLIVEIRA, J. R. P.; PIRES, M. F. da C. **Atraso na tipificação de condutas pela ANPD prejudica a desejada responsividade**. 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/atraso-na-tipificacao-de-condutas-pela-anpd-prejudica-a-desejada-responsividade-23092022>. Acesso em: 25 jan. 2023.

PEREIRA DA ROCHA, Camila et al. Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará**, v. 2, n. 3, p. 78-97, ago. 2019. Disponível em: <http://revistasfap.com/ojs3/index.php/tic/article/view/285>. Acesso em: 26 maio 2021.

PUGLIESI, Rodrigo. **A LGPD e seus desafios no setor público**. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-desafios-setor-publico-serpro>. Acesso em: 16 maio 2022.

RIBEIRO, Renato Carauta. **Assinatura digital no padrão XAdES como um serviço REST**: um estudo de caso na Universidade de Brasília. 2021. 101 f., il. Dissertação (Mestrado Profissional em Computação Aplicada) – Universidade de Brasília, Brasília, 2021. Disponível em: <https://repositorio.unb.br/handle/10482/42417>. Acesso em 28 mar. 2022.

RODRIGUES, João Gaspar. Publicidade, transparência e abertura na administração pública. RDA: **Revista de Direito Administrativo**, Rio de Janeiro, v. 266, p.89-123, mai/ago 2014, p. 94.

RODRIGUES, Laura Secfém. **LGPD**: consentimento nas relações trabalhistas. 2021. Disponível em: <https://www.lgpdbrasil.com.br/lgpd-consentimento-nas-relacoes-trabalhistas/>. Acesso em 10 jan. 2023.

ROSSO, Angela Maria. **LGPD e setor público**: aspectos gerais e desafios. 2019. Acesso em: 15 jan. 2023. Disponível em: <https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios>. Acesso em: 12 dez. 2022.

SOUZA, P M. de; BARRANCOS, J. E.; MAIA, M. E. Acesso à informação e ao tratamento de dados pessoais pelo poder público. **Inf. & Soc.:Est.**, João Pessoa, v.29, n.1, p. 237-251, jan./mar. 2019. Disponível em: <https://repositorio.ufpb.br/jspui/handle/123456789/25232>. Acesso em 11 jan. 2023.

SILVA, Daniel Cavalcante. **Manual da Lei Geral de Proteção de Dados para Instituições de Ensino**. Brasília, 2020, p. 20.

SILVA, Itapoã Fortunato da. **Proteção de Dados Pessoais**: o processo de implementação da LGPD em uma Universidade Pública Federal. 2021. 59f Trabalho de Conclusão de Curso – Universidade Federal de Pernambuco. Disponível em: <https://repositorio.ufpe.br/handle/123456789/41227>. Acesso em: 08 dez. 2022.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

SUSSEKIND, Arnaldo. Os Princípios do Direito do Trabalho e a Constituição de 1988. **Revista da Academia Nacional de Direito do Trabalho**, ano 8, n. 8, 2000, p. 33. Disponível em: <http://www.ablj.org.br/revistas/revista15/revista15%20%20ARNALDO%20%20%20E2%80%93%20Os%20Princ%20%20ADpios%20do%20Direito%20do%20Trabalho%20e%20a%20Constitui%20%20A7%20%20A3o%20de%201988.pdf>. Acesso em: 18 dez. 2022.

TEPEDINO, Gustavo; DE TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.

TRIBUNAL DE CONTAS DA UNIÃO. **Relatório sistêmico de fiscalização de tecnologia da informação**. Brasília: TCU, 2015, p. 39. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/sumario-relatorio-sistemico-de-fiscalizacao-de-tecnologia-da-informacao-fiscti.htm>. Acesso em: 19 nov. 2022.

TRIBUNAL DE CONTAS DA UNIÃO. **TCU verifica risco alto à privacidade de dados pessoais coletados pelo governo**. Brasília: TCU, 2022. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>. Acesso em 18 dez. 2022.

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO. **PLANO DE DESENVOLVIMENTO INSTITUCIONAL 2021-2030**. Disponível em: https://pdi.ufes.br/sites/pdi.ufes.br/files/field/anexo/minuta_pdi_2021-2030.pdf. Acesso em 01 de jun. 2021

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO. **Manual de Processo Administrativo Disciplinar - Controladoria-Geral da União (CGU)**. Seção de Procedimentos Disciplinares. 2022. Disponível em: <https://spd.ufes.br/manual-de-processo-administrativo-disciplinar-controladoria-geral-da-uniao-cgu>. Acesso em 12 jan. 2023.

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO. **Protocolo Ufes – Lepisma**. Disponível em: <https://protocolo.ufes.br/#/home>. Acesso em: 12 fev. 2023a.

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO. **Protocolo Ufes – Lepisma – Consulta pública de documentos**. Disponível em: <https://protocolo.ufes.br/#/busca>. Acesso em: 12 fev. 2023b

UNIVERSIDADE FEDERAL DE MINAS GERAIS. **Termo de consentimento para tratamento de dados pessoais**. Pró-reitoria de Recursos Humanos. 2021. Disponível em: <https://www.ufmg.br/prorh/wp-content/uploads/2021/11/Termo-de-Consentimento-para-Tratamento-de-Dados-Pessoais-Lei-Geral-de-Protecao-de-Dados-Pessoais-LGPD.pdf>. Acesso em: 19 jan. 2023.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2021. Disponível em: <https://ufrj.br/acesso-a-informacao/lgpd/>. Acesso em 03 jan. 2023.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. **Tratamento de dados pessoais**. 2020. Disponível em: <http://www.ufrgs.br/ufrgs/acessoainformacao/tratamento-de-dados-pessoais>. Acesso em: 13 dez. 2022.

UNIVERSIDADE FEDERAL FLUMINENSE. **Lei Geral de Proteção de Dados**. 2022. Disponível em: <https://www.uff.br/?q=lgpd>. Acesso em 03 jan. 2023.

VARELLA, Marcelo D.; OLIVEIRA, Clarice G.; MOESCH, Frederico. Salto digital nas políticas públicas: oportunidades e desafios. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, p. 560-583, 2017. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4808/0>. Acesso em: 26 mar. 2021.

VIGNOLI, Richele Grengé; VECHIATO, Fernando Luiz. Dados sensíveis no contexto dos dados de pesquisa: um olhar na perspectiva da ciência da informação. In: CONGRESSO ISKO ESPANHA, 14., 2019, Barcelona. Comunicação oral. Center For Open Science, 2019. **Anais eletrônicos**. Disponível em:

https://fima.ub.edu/isko2019/sites/isko2019/files/2019-05/isko119_0.pdf. Acesso em: 20 dez. 2022.