UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO – UNIRIO
CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS – CCJP
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

Patricia de Araujo Sebastião

POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS APLICADA ÀS INFORMAÇÕES PESSOAIS DE ESTUDANTES NA UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

Rio de Janeiro
2023

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO – UNIRIO
CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS – CCJP
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

Patricia de Araujo Sebastião

POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS APLICADA ÀS INFORMAÇÕES PESSOAIS DE ESTUDANTES NA UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

Dissertação apresentada ao Programa de Pós-Graduação *stricto sensu* em Direito (PPGD) na área de concentração Direito e Políticas Públicas na linha de pesquisa Direitos Humanos e Políticas Públicas como requisito parcial para a obtenção do título de mestre.

Orientador: Prof. Dr. Leonardo de Andrade Mattietto

Rio de Janeiro
2023

UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO – UNIRIO
CENTRO DE CIÊNCIAS JURÍDICAS E POLÍTICAS – CCJP
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

Patricia de Araujo Sebastião

POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS APLICADA ÀS INFORMAÇÕES PESSOAIS DE ESTUDANTES NA UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

Dissertação apresentada ao Programa de Pós-Graduação *stricto sensu* em Direito (PPGD) na área de concentração Direito e Políticas Públicas na linha de pesquisa Direitos Humanos e Políticas Públicas como requisito parcial para a obtenção do título de mestre.

BANCA EXAMINADORA

_____

Professor Dr. Leonardo de Andrade Mattietto

_____

Professor(a) Dr. Oswaldo Pereira de Lima Junior

_____

Professor (a) Dr. Marcelo Pereira dos Santos

Rio de Janeiro
2023

Dados pessoais são indicativos de aspectos de nossa personalidade, portanto merecem proteção do direito enquanto tais.

Danilo Doneda

RESUMO

Esta dissertação tem como objetivo analisar a implementação da política pública de proteção de dados na UFRRJ, considerando as exigências estabelecidas pela LGPD. Discutir-se-ão os fundamentos da proteção de dados como direito e garantia fundamental, bem como os principais aspectos da lei, incluindo conceitos relevantes, princípios e o tratamento de dados pessoais pelo poder público. Aborda-se a implementação das boas práticas e governança no poder público, destacando a importância dessas medidas por meio da análise do Decreto nº 9.203/2017. Ressalta-se a importância das boas práticas e governança para a proteção de dados, além do papel da ANPD e o estudo das sanções previstas na legislação. Será apresentado o panorama da universidade, o cenário atual em relação à adequação da LGPD, bem como a análise dos dados coletados através de questionários e entrevistas com diversos atores institucionais. Por fim, são apresentados os planos de ação propostos para a adequação e implementação da política de proteção de dados na instituição. O estudo adotou uma perspectiva teórico-empírica, transversal e descritiva, utilizando-se do método qualitativo e quantitativo, para a revisão teórica, valeu-se de estudo bibliográfico e legislativo. Ao final, espera-se fornecer percepções relevantes para a efetivação da proteção de dados na UFRRJ e contribuir para o desenvolvimento de práticas eficazes de gestão e governança de dados em instituições de ensino superior brasileiras.

Palavras-chave: Políticas Públicas; LGPD; Governança; dados pessoais dos estudantes; UFRRJ.

ABSTRACT

This dissertation aims to analyze the implementation of public data protection policy at UFRRJ, considering the requirements established by the LGPD. The foundations of data protection as a fundamental right and guarantee will be discussed, as well as the main aspects of the law, including relevant concepts, principles and the processing of personal data by public authorities. The implementation of good practices and governance in public authorities is discussed, highlighting the importance of these measures through the analysis of Decree No. 9,203/2017. The importance of good practices and governance for data protection is highlighted, in addition to the role of the ANPD and the study of sanctions provided for in the legislation. The university's panorama will be presented, the current scenario in relation to the adequacy of the LGPD, as well as the analysis of data collected through questionnaires and interviews with various institutional actors. Finally, the proposed action plans for the adaptation and implementation of the data protection policy at the institution are presented. The study adopted a theoretical-empirical, transversal and descriptive perspective, using the qualitative and quantitative method, for the theoretical review, using bibliographic and legislative studies. In the end, it is expected to provide relevant insights for the implementation of data protection at UFRRJ and contribute to the development of effective data management and governance practices in Brazilian higher education institutions.

Keywords: Public policy; LGPD; Governance; students' personal data; UFRRJ.

LISTA DE FIGURAS

LISTA DE SIGLAS

CIS	Comunicado de Incidente de Segurança
CEPE	Conselho de Ensino, Pesquisa e Extensão
CD	Conselho Diretor
CMPDPP	Conselho Municipal de Proteção de Dados Pessoais e da Privacidade
CGU	Controladoria Geral da União
CODEP	Coordenação de Desenvolvimento de Pessoas
CGF	Coordenador-Geral De Fiscalização
CCS	Coordenadoria de Comunicação Social
COTIC	Coordenadoria de Tecnologia da Informação e Comunicação
DOU	Diário Oficial da União
ENAP	Escola Nacional de Administração Pública
ESAMV	Escola Superior de Agricultura e Medicina Veterinária
IAMSPE	Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo
INC	Instrução Normativa Conjunta
LDB	Lei de Diretrizes e Bases da Educação Nacional
LGPD	Lei Geral de Proteção de Dados
MEC	Ministério da Educação
PDI	Plano de Desenvolvimento Institucional
PROAES	Pró-reitoria Assuntos Estudantis
PROAF	Pró-reitoria Assuntos Financeiros
PROGEP	Pró-reitoria de Gestão de Pessoas
PROPLADI	Pró-Reitoria de Planejamento, Avaliação e Desenvolvimento Institucional
PROEXT	Pró-reitoria de Extensão
PROGRAD	Pró-reitoria Graduação
PROPPG	Pró-reitoria Pesquisa e Pós-Graduação
PPSI	Programa de Privacidade e Segurança da Informação
RIPD	Relatório de Impacto à Proteção de Dados
REUNI	Reestruturação e Expansão das Universidades Federais
GDPR	Regulamento Geral de Proteção de Dados
SES-SC	Secretaria de Estado da Saúde de Santa Catarina

SGD	Secretaria de Governo Digital
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SISU	Sistema de Seleção Unificada
SIGAA	Sistema Integrado de Gestão de Atividades Acadêmicas
SIGRH	Sistema Integrado de Gestão de Recursos Humanos
SIPAC	Sistema Integrado de Patrimônio, Administração e Contratos
STF	Supremo Tribunal Federal
TI	Tecnologia da Informação
UFRN	Universidade Federal do Rio Grande do Norte
UFRRJ	Universidade Federal Rural do Rio de Janeiro

SUMÁRIO

INTRODUÇÃO

A Lei nº 13.709/2018, LGPD, representa um marco significativo na regulamentação da Política Pública de Proteção de Dados Pessoais dentro do arcabouço jurídico brasileiro. Tanto pessoas físicas quanto jurídicas, de natureza pública ou privada, envolvidas no tratamento de dados pessoais, estão obrigadas a se adaptar a essa nova realidade legal. A implementação das disposições legais é imperativa, visto que a entrada em vigor das sanções associadas à norma ocorreu em 1º de agosto de 2021.

Efetuar a adequação e implementação da LGPD exige mudança de cultura, de hábitos e de comportamento, o que requer conscientização e esforço coletivo, inclusive do titular dos dados pessoais, que precisa compreender a importância de resguardar suas informações pessoais. A efetividade da política pública de proteção de dados pessoais, demanda de todos os envolvidos com o tratamento uma conduta diligente pautada nas boas práticas e governança, além de uma atenção especial aos princípios orientadores do tratamento de dados pessoais.

A lei não tem por objetivo proibir o tratamento dos dados, mas sim regulamentar de forma geral como este deve ser realizado de modo a manter a segurança dos dados. Desta forma, a norma instituiu a ANPD, que tem um vasto rol de competências, entre elas está consagrado zelar pela proteção dos dados pessoais e promover na população o conhecimento da lei, das políticas públicas sobre proteção de dados pessoais e das medidas de segurança.

É com base neste novo cenário normativo que se pauta a investigação deste trabalho acadêmico, com foco nos desafios que o Poder Público vêm enfrentando para se adequar e implementar a legislação. Assim, a UFRRJ constitui-se como campo de estudo desta pesquisa que apresenta como problemática a adequação e implementação da política pública de proteção de dados pessoais na universidade à luz da LGPD, surgindo a seguinte questão central: quais as providências foram ou estão sendo tomadas para que ocorra a devida adequação às exigências legais e a prevenção dos riscos inerentes? Deste modo, a dissertação efetua uma investigação do problema apresentado com a finalidade de se chegar a um entendimento conclusivo quanto ao real cenário desta autarquia federal de ensino.

É crucial ressaltar que, dada a extensa quantidade de universidades públicas federais no país, a UFRRJ foi escolhida uma vez que a pesquisadora é Técnica Administrativa Educacional nesta instituição. Isso permitiu sua presença contínua no campo de estudo ao

longo de toda a pesquisa, o que representou uma vantagem significativa para os propósitos da pesquisa.

Buscando contribuir com o panorama anteriormente exposto através da pesquisa acadêmica, o estudo adotou uma abordagem teórico-empírica, transversal e descritiva, fundamentada na integração entre teoria e prática, visando fornecer uma compreensão abrangente do fenômeno investigado. A escolha pela natureza descritiva da pesquisa justifica-se pela sua abordagem exploratória, que buscou identificar e descrever os processos e práticas associados à proteção de dados dos alunos da universidade em questão.

Utilizaram-se métodos mistos, que combinam técnicas qualitativas e quantitativas, considerando fundamental para uma investigação completa e robusta sobre a proteção de dados dos estudantes. Assim, foram aplicados questionários para coletar dados quantitativos acerca das percepções e conhecimentos dos discentes em relação à proteção de dados, enquanto as entrevistas proporcionaram percepções qualitativas mais profundas sobre o panorama institucional, permitindo uma compreensão abrangente das práticas e desafios enfrentados pela universidade.

Os resultados obtidos foram, então, analisados e interpretados à luz da revisão teórica realizada previamente, permitindo a formulação de conclusões embasadas e recomendações pertinentes para aprimorar a proteção de dados na UFRRJ. Para respaldar a aludida revisão teórica, valeu-se de estudo bibliográfico e legislativo, consistindo na análise das principais doutrinas e artigos acadêmicos que abordam o tema, e exame das normas que regulamentam a privacidade e proteção de dados pessoais, em especial a LGPD.

Deste modo, visando a contextualização da problemática proposta, a seção 2 da dissertação é intitulado “A Política Pública de Proteção de Dados” e busca traçar a evolução da Privacidade à Proteção de Dados Pessoais, com destaque para o emblemático artigo *The right to privacy*, escrito em 1890 pelos autores Brandeis e Warren. Esta contextualização vem demonstrar a importância da LGPD na contemporaneidade, fundamentada na Teoria dos Direitos da Personalidade e na Dignidade da Pessoa Humana.

Por conseguinte, visando uma melhor exposição do tema, a seção 2 apresenta subseções de fundamental importância para a compreensão da pesquisa. A 2.1 objetiva demonstrar a importância do reconhecimento da proteção de dados pessoais como direito fundamental constitucionalmente reconhecido. Na 2.2 foram apresentados os fundamentos necessários para o aprofundamento da investigação, trazendo o conceito dos principais termos referente a temática proteção de dados pessoais na subdivisão 2.2.1.

A subseção 2.2.2 efetua a análise dos princípios consagrados na LGPD e a 2.2.3 demonstra o panorama das exigências legais direcionadas aos órgãos e entidades públicas, entretanto, delimita a abordagem as implicações legais inerentes às autarquias ou ao Poder Público em sua totalidade, não se atendo a peculiaridades de outros órgãos ou entidades públicas, como por exemplo empresas públicas e sociedades de economia mista.

A seção 3 dedica-se à análise da implementação das boas práticas e governança no âmbito do poder público, destacando sua importância na efetivação da política pública de proteção de dados. Por meio de uma abordagem detalhada, serão explorados diversos aspectos relacionados a esse tema, visando compreender os mecanismos e instrumentos utilizados para garantir a segurança e privacidade dos dados pessoais.

A subseção 3.1 discute a relevância da adoção de boas práticas e governança no contexto do poder público. Serão apresentados argumentos que evidenciam a necessidade de uma gestão eficiente dos dados pessoais por parte das instituições governamentais, visando proteger os direitos individuais e promover a transparência e *accountability* na administração pública. Esta possui três subseções, a primeira é dedicada à análise do Decreto nº 9.203/2017 que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Serão abordados os princípios e diretrizes estabelecidos por esta normativa, destacando sua importância na promoção da segurança e proteção dos dados pessoais no contexto governamental.

A segunda subseção explora a relação entre as boas práticas de governança e os princípios estabelecidos pela lei. Serão identificados os requisitos e procedimentos que devem ser adotados pelas organizações públicas para garantir a conformidade com a legislação, promovendo a segurança dos dados pessoais. Já a terceira subseção focaliza no papel da ANPD quanto a fiscalização e aplicação das sanções previstas em lei. Discute-se a importância da adoção de regras de boas práticas e governança pelas instituições públicas como forma de mitigar riscos e garantir a conformidade com a legislação.

A subseção 3.2 dá ênfase à relevância da implementação das boas práticas e governança na proteção de dados, analisando os impactos positivos dessas medidas na promoção da segurança e privacidade dos dados pessoais, bem como na prevenção de incidentes de segurança e vazamentos de informações. Esta subdivide-se em duas partes, a primeira examina sanções aplicadas pela ANPD em decorrência de violações à LGPD. Será discutido o papel pedagógico dessas sanções, visando garantir a proteção efetiva dos dados pessoais.

Na segunda subseção é discutido o papel do encarregado, bem como a importância do relatório de impacto como instrumento de avaliação e gestão de riscos em projetos que envolvam o tratamento de dados pessoais, bem como a importância destes para a implementação das boas práticas e governança na proteção de dados.

Por fim, a seção 4 aborda as adequações necessárias para a implementação da política pública de proteção de dados na UFRRJ, esta é essencial para compreender como a instituição está se adaptando às exigências legais, bem como, identificar as medidas necessárias para assegurar a conformidade e a proteção dos dados pessoais dos seus discentes.

Diante da necessidade de detalhar a metodologia utilizada na investigação de campo, optou-se por apresentar na subseção 4.1 o desenho metodológico, este integra abordagens quantitativas e qualitativas visando uma investigação abrangente e aprofundada do cenário de proteção de dados na UFRRJ. A 4.2, fornece um panorama geral da instituição de ensino, incluindo informações relevantes sobre sua estrutura, funcionamento e características institucionais. Compreender o contexto institucional é fundamental para identificar desafios e oportunidades.

Já a 4.3 apresenta os resultados da investigação de campo, realizando uma análise detalhada dos dados coletados por meio de questionários aplicados aos estudantes, bem como das entrevistas com diferentes atores institucionais. Assim, na 4.3.1 é discutida a percepção dos estudantes sobre a proteção de dados pessoais e seu conhecimento em relação à LGPD. Este estudo é fundamental para compreender o nível de conscientização e engajamento dos discentes em relação à política pública de proteção de dados.

Na 4.3.2 apresenta-se os resultados das entrevistas realizadas com diferentes atores institucionais da UFRRJ, incluindo a Pró-reitora Adjunta da PROPLADI, o Encarregado de Dados, o Coordenador da Coordenadoria de Tecnologia da Informação e Comunicação, a servidora responsável pela segurança da informação, a servidora responsável pelo Núcleo de Governança de Integridade e um servidor da Pró-Reitoria de Graduação. As entrevistas proporcionaram discernimento sobre as práticas e desafios enfrentados pela universidade, salienta-se que cada uma encontra-se em uma subseção.

Na 4.4 apresenta-se os planos de ação propostos para a adequação e implementação da política pública de proteção de dados na UFRRJ. Estes visam orientar a instituição na implementação de medidas concretas para garantir a conformidade com a LGPD e promover a proteção efetiva dos dados pessoais dos seus estudantes.

Neste contexto, o estudo efetua uma análise particularizada sobre a implementação da política pública de proteção de dados na UFRRJ. Foram explorados os principais aspectos relacionados às boas práticas, governança e adequações necessárias para assegurar a conformidade com a LGPD. Ao longo das seções, discute-se a importância da proteção de dados como um direito fundamental, a legislação aplicável, a adoção de boas práticas e governança no poder público, bem como o cenário atual da universidade em relação à implementação da lei. A integração de abordagens quantitativas e qualitativas permitiu uma análise abrangente da situação, fornecendo percepções para a elaboração de planos de ação direcionados à proteção efetiva dos dados pessoais dos discentes.

Por fim, os resultados obtidos e as recomendações apresentadas têm o objetivo de contribuir para o avanço do conhecimento científico sobre a proteção de dados e para a promoção de práticas eficazes de gestão e governança de dados na UFRRJ e, por extensão, em outras instituições federais de ensino brasileiras.

2. POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS

A humanidade vive em constante evolução e na contemporaneidade o mundo está na era da tecnologia, assim, a todo instante pessoas compartilham seus dados pessoais em aplicativos, redes sociais, smartphones, entre outros meios eletrônicos e digitais. Porém, independente do compartilhamento digital ou físico quem possui os dados do titular se torna responsável pelo tratamento desde a coleta até a eliminação, nos termos da LGPD.

Ainda não há uma conscientização em massa da importância da proteção efetiva dos dados pessoais, muitos titulares fornecem seus dados de maneira indiscriminada sem se preocupar como será efetuado o tratamento, é possível perceber que grande parte da população não tem conhecimento quanto a existência ou conteúdo da legislação. Dessa percepção surge a abordagem da pesquisa, abarcando os dados pessoais dos estudantes a partir da adequação à LGPD das instituições federais de ensino, adotando a UFRRJ como campo de estudo.

Como suporte teórico, é imperioso destacar que a proteção dos dados pessoais origina-se do processo evolutivo da privacidade, para sustentar esta afirmação a contextualização dar-se-á a partir do emblemático artigo *The right to privacy*, escrito em 1890 pelos autores Brandeis e Warren, este é o início da doutrina moderna sobre direito à privacidade conforme preceitua Danilo Doneda (2021, p. 30).

O artigo ressalta a privacidade como o "direito de ser deixado só", dialogando com o avanço tecnológico das fotografias instantâneas e os empreendimentos jornalísticos, relatando como os mesmos invadiram a vida privada do indivíduo, demonstrando que numerosos dispositivos mecânicos começam a ameaçar a proteção da pessoa. Enfatiza o artigo que o desenvolvimento da lei para alcançar essas demandas era inevitável, este descaracteriza a relação entre privacidade e propriedade (WARREN; BRANDEIS, 1890, tradução nossa):

> Este desenvolvimento da lei era inevitável. A intensa vida intelectual e emocional e o aumento das sensações que vieram com o avanço da civilização deixaram claro para os homens que apenas uma parte da dor, do prazer e do lucro da vida está nas coisas físicas. Pensamentos, emoções e sensações exigiam reconhecimento legal, e a bela capacidade de crescimento que caracteriza o direito consuetudinário permitiu aos juízes conceder a proteção necessária, sem a interposição do legislador. Recentes invenções e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para garantir ao indivíduo o que o Juiz Cooley chama de direito de "ser deixado em paz". As fotografias instantâneas e os empreendimentos jornalísticos invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam confirmar a previsão de

> que “o que é sussurrado no armário será proclamado dos telhados”. Durante anos, houve um sentimento de que a lei deveria fornecer algum remédio para a circulação não autorizada de retratos de pessoas particulares.[1]

Os autores argumentam que o crescimento da civilização e as mudanças na vida intelectual e emocional destacaram a necessidade de reconhecimento legal para pensamentos, emoções e sensações, não apenas para as coisas físicas. Essa perspectiva reflete a evolução da sociedade em reconhecer a importância da esfera pessoal na vida dos indivíduos.

O trecho salienta o papel do direito consuetudinário na concessão de proteção legal para as esferas mais íntimas da vida, ressaltando a capacidade flexível do sistema jurídico em adaptar-se às transformações sociais. A referência ao direito de "ser deixado em paz" indica uma preocupação crescente com a invasão da privacidade diante de inovações como fotografias instantâneas e empreendimentos jornalísticos.

A apreensão com a circulação não autorizada de retratos de pessoas particulares aponta para a necessidade de remediar o impacto negativo das novas tecnologias na privacidade individual. Esse sentimento antecipa questões contemporâneas relacionadas à privacidade digital, indicando uma aflição contínua com a proteção da esfera pessoal diante dos avanços tecnológicos.

A citação enfatiza a importância histórica do reconhecimento da privacidade como um direito legalmente instituído, fornecendo percepções valiosas sobre os desafios enfrentados pelos juristas diante das mudanças sociais e tecnológicas no final do século XIX. Essas reflexões pioneiras continuam a influenciar as discussões contemporâneas sobre privacidade e direitos individuais. Cabendo citar Stefano Rodotá (2008, p. 23-25)

> As novas dimensões da coleta e do tratamento de informações provocaram a multiplicação de apelos à privacidade e, ao mesmo tempo, aumentaram a consciência da impossibilidade de confinar as novas questões que surgem dentro do quadro institucional tradicionalmente identificado por este conceito. Hoje, porém, o

---

[1] *“This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature. Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone”.” Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops”. For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons.”*

> problema não é adaptar uma noção nascida em outros tempos e em outras terras a uma situação profundamente modificada, respeitando suas razões e sua lógica de origem. Quem consegue decifrar o debate ora em curso percebe que ele não reflete somente o tema clássico da defesa da esfera privada contra as invasões externas, mas realiza uma importante mudança qualitativa que nos incita a considerar os problemas da privacidade de preferência no quadro da organização do poder, no âmbito do qual justamente a infra-estrutura da informação representa hoje um dos componentes fundamentais. Talvez seja possível traçar um esquema deste processo, ressaltando que parece cada vez mais frágil a definição de "privacidade" como o "direito a ser deixado só", que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito. Não que este último aspecto estivesse ausente das definições tradicionais: nelas, porém, ele servia muito mais para sublinhar e exaltar o ângulo individualista, apresentando a privacidade como mero instrumento para realizar a finalidade de ser deixado só; enquanto hoje chama a atenção sobretudo para a possibilidade de indivíduos e grupos controlarem o exercício dos poderes baseados na disponibilização de informações, concorrendo assim para estabelecer equilíbrios sócio-políticos mais adequados. Trata-se de uma tendência determinada por fenômenos interdependentes. Às novas formas de coleta e tratamento de informações, possibilitadas sobretudo pelo recurso a computadores, adicione-se a crescente necessidade de dados por parte das instituições públicas e privadas: como não é imaginável uma ação que vá de encontro a esta tendência, comum a todas as organizações sociais modernas, é necessário considerar de forma realista tal situação, analisando as transformações que causa na distribuição e no uso do poder pelas estruturas públicas e privadas. somente assim será possível desfazer o nó das relações entre a tutela das liberdades individuais e a eficiência administrativa e empresarial. Identificando as raízes do poder fundado na disponibilidade das informações e seus reais detentores, será possível não somente projetar formas de contra-poder e de controle, como também aproveitar as possibilidades oferecidas pela tecnologia da computação para tentar produzir formas diversas de gestão do poder, capazes de oferecer às liberdades individuais possibilidades de expansão antes impensáveis.

Destaca as transformações significativas nas dimensões da coleta e do tratamento de informações, gerando uma multiplicação de apelos à privacidade. O autor ressalta que essas mudanças não podem ser contidas dentro do quadro institucional tradicionalmente associado ao conceito de privacidade. Em vez de simplesmente adaptar uma noção concebida em tempos e contextos diferentes, Rodatá argumenta que enfrenta-se a necessidade de reconsiderar a privacidade no contexto da organização do poder, no qual a infraestrutura da informação desempenha um papel crucial.

A mudança qualitativa no debate sobre privacidade vai além da defesa clássica da esfera privada contra invasões externas. Ressalta a importância de considerar os problemas da vida privada dentro do quadro da organização do poder, em que a infraestrutura da informação é um componente fundamental. Sugere que a definição tradicional de "privacidade" como o "direito a ser deixado só" está se tornando cada vez mais frágil, dando

lugar a definições que enfatizam a capacidade de controle sobre o uso das informações pessoais. Essa mudança de ênfase indica uma transformação na percepção da privacidade, que deixa de ser um mero instrumento individualista para ser considerada como um meio de controlar o exercício do poder baseado na disponibilidade de informações.

Rodatá ressalta a interdependência de fenômenos que impulsionam essa tendência, como as novas formas de coleta e tratamento de informações facilitadas pela computação, juntamente com a crescente demanda por dados por parte de instituições públicas e privadas. Ele argumenta que não é realista opor-se a essa tendência, comum a todas as organizações sociais modernas, e propõe uma abordagem realista para analisar as transformações que ela impõe na distribuição e uso do poder por essas estruturas.

Enfatiza a necessidade de identificar as raízes do poder vinculado à disponibilidade de informações e seus verdadeiros detentores. A partir dessa identificação, sugere a possibilidade de projetar formas de contra-poder e controle, utilizando as oportunidades oferecidas pela tecnologia da computação para criar novas formas de gestão do poder. Essas novas formas, segundo Rodatá, podem expandir as possibilidades das liberdades individuais de maneiras antes impensáveis, abrindo espaço para uma reflexão crítica sobre as relações entre a tutela das liberdades individuais e a eficiência administrativa e empresarial.

Tendo em vista as transformações significativas nas dimensões da coleta e do tratamento de informações, gerando uma multiplicação de apelos à vida particular e que a definição tradicional de "privacidade" como o "direito a ser deixado só" está se tornando cada vez mais frágil, dando lugar a definições que enfatizam a capacidade de controle sobre o uso das informações pessoais. É imperioso mencionar a obra "A Era do Capitalismo de Vigilância". O livro de Shoshana Zuboff analisa e critica profundamente o fenômeno contemporâneo do capitalismo de vigilância, um modelo econômico que se baseia na coleta massiva de dados pessoais para a previsão e modificação do comportamento humano.

A autora cunhou o termo "capitalismo de vigilância" para descrever uma nova fase em que as empresas, em particular as grandes corporações de tecnologia, se envolvem em práticas de vigilância que vão além do que tradicionalmente era associado ao mercado. Zuboff argumenta que este sistema econômico não apenas explora a mão de obra e os recursos, mas também busca monitorar e influenciar o comportamento humano de maneira sistemática.

Examina como as empresas de tecnologia, como Google e Facebook, coletam dados pessoais incessantemente, utilizando algoritmos avançados para analisar e prever o

comportamento dos usuários. Essas previsões são então utilizadas para personalizar anúncios e serviços, criando um ambiente em que a vigilância se torna uma ferramenta central para a maximização dos lucros.

Zuboff também destaca as implicações sociais e políticas desse modelo, incluindo a erosão da privacidade, o aumento da assimetria de poder entre as grandes corporações e os indivíduos, bem como o impacto na democracia e na autonomia. A autora adverte sobre os perigos do capitalismo de vigilância, chamando a atenção para a necessidade de regulamentações e uma reavaliação dos valores sociais em meio a essa transformação tecnológica.

"A Era do Capitalismo de Vigilância" efetua uma análise profunda e uma abordagem crítica sobre as questões éticas e sociais associadas à economia digital. A obra contribui significativamente para o entendimento das transformações sociais na era da tecnologia da informação e coloca importantes questionamentos sobre o equilíbrio entre inovação, privacidade e poder no cenário contemporâneo. Cabendo citar (ZUBOFF, 2021, p 754-755)

> O poder instrumentário reuniu força fora da humanidade, mas também fora da democracia. Não pode haver leis para nos proteger daquilo que não tem precedentes, e sociedades democráticas, como o mundo inocente dos tainos, são vulneráveis ao poder sem precedentes. Dessa forma, o capitalismo de vigilância pode ser encarado como parte de um alarmante voo global rumo ao que muitos cientistas políticos agora enxergam como um amolecimento das atitudes públicas em relação à necessidade e inviolabilidade da própria democracia. Muitos estudiosos apontam para uma “recessão democrática” global ou uma “desconsolidação” das democracias ocidentais que foram durante muito tempo consideradas impermeáveis a ameaças antidemocráticas.

A citação enfatiza a natureza do poder instrumental associado ao fenômeno contemporâneo do capitalismo de vigilância, destacando que esse poder não apenas se fortaleceu fora dos limites da humanidade, mas também além das fronteiras da democracia. A ausência de precedentes nesse contexto levanta desafios significativos, pois não existem leis estabelecidas para proteger as sociedades contra algo que não foi vivenciado anteriormente.

Zuboff recorre a uma analogia histórica, referindo-se ao "mundo inocente dos tainos", uma sociedade democrática vulnerável ao poder sem precedentes. Essa alusão sugere que as sociedades democráticas modernas podem compartilhar uma vulnerabilidade semelhante diante deste novo sistema econômico, destacando a necessidade de compreender e enfrentar as implicações desse fenômeno.

O termo "voo global" utilizado pela autora sugere uma tendência abrangente e preocupante em direção a uma transformação global que está desafiando as atitudes públicas em relação à democracia. A ideia de um "amolecimento das atitudes públicas" destaca uma mudança percebida na valorização da democracia por parte da sociedade. O capitalismo de vigilância é contextualizado como um componente desse processo, indicando que suas dinâmicas podem contribuir para uma revisão na forma como as sociedades encaram a importância e a inviolabilidade da democracia.

A menção à "recessão democrática" global e à "desconsolidação" dos regimes ocidentais destaca preocupações mais amplas sobre o estado atual do sistema político em escala global. A expressão "resistentes a ameaças antidemocráticas" indica uma percepção de mudança na capacidade desses regimes de resistir a desafios que anteriormente eram considerados improváveis.

Este trecho do livro de Zuboff instiga uma reflexão crítica sobre a interação complexa entre o capitalismo de vigilância, o poder instrumental, e os fundamentos democráticos. Proporciona uma base para discussões sobre os desafios emergentes para as democracias contemporâneas, destacando a necessidade de análises mais aprofundadas sobre como essas transformações impactam as atitudes públicas e as instituições em escala global.

O que é vivenciado hoje na era digital, já era prenunciado no final do século XIX em *The right to privacy,* demonstrando uma continuidade histórica nas discussões sobre privacidade. Doneda (2021, p. 126) ressalta que o artigo “reflete a tendência a uma fundamentação diversa para a proteção da privacidade, desvinculada do direito de propriedade”. Um dos pontos centrais do artigo de Warren e Brandeis, segundo Doneda, é justamente que o princípio a ser notado na proteção da privacidade não caminha pela propriedade privada, mas pela “inviolate personality”. De acordo com o autor, “nessa evocação de um direito de natureza pessoal encontramos (...) o eixo em torno da proteção da pessoa humana que será determinante na proteção da privacidade no século seguinte.”

Essa perspectiva destaca a importância da integridade pessoal e da inviolabilidade da personalidade como princípios fundamentais na proteção da privacidade. Ao invocar um direito de natureza pessoal, o artigo estabelece um eixo central em torno da proteção da pessoa humana, o qual se tornará determinante na concepção da vida particular ao longo do século seguinte.

A referência à "inviolate personality" enfatiza a proteção da individualidade e da esfera pessoal como elementos-chave na preservação da privacidade. Essa ênfase sugere uma

compreensão mais ampla e holística da privacidade, indo além das considerações puramente patrimoniais. A análise ressalta a importância de considerar as origens conceituais da proteção à privacidade, remontando ao século XIX. Isso oferece uma perspectiva histórica valiosa para compreender a evolução do pensamento sobre privacidade e destaca a relevância contínua dos princípios fundamentais estabelecidos por Warren e Brandeis. A observação de Doneda proporciona uma base crítica para explorar as raízes do direito à privacidade e sua adaptação aos desafios contemporâneos, especialmente na era digital.

É relevante pontuar que Doneda esclarece em sua obra que não houve uma ruptura com a "privacidade de outras épocas", mas o que ocorreu foi o reposicionamento do centro de gravidade em razão dos múltiplos interesses que estavam relacionados e na sua importância quanto a tutela da pessoa humana, o autor reafirma "a existência de uma continuidade histórica e uma tendência integrativa das diversas manifestações da tutela da privacidade", o que estrutura a privacidade na teoria dos direitos da personalidade (DONEDA, 2021, p. 41, 42):

> A privacidade, nas últimas décadas, passou a se relacionar com uma série de interesses e valores, o que modificou substancialmente o seu perfil. E talvez a mais importante dessas mudanças tenha sido essa apontada por Stefano Rodotà, de que o direito à privacidade não mais se estrutura em torno do eixo "pessoa-informação-segredo", no paradigma da zero-relationship, mas sim no eixo "pessoa-informação-circulação-controle". Nessa mudança, a proteção da privacidade acompanha a consolidação da própria teoria dos direitos da personalidade e, em seus mais recentes desenvolvimentos, afasta a leitura segundo a qual sua utilização em nome de um individualismo exacerbado alimentou o medo de que eles se tornassem o "direito dos egoísmos privados". Algo paradoxalmente, a proteção da privacidade na sociedade da informação, a partir da proteção de dados pessoais, avança sobre terrenos outrora improponíveis e nos induz a pensá-la como um elemento que, mais do que garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade – isto é, de forma que a tutela da privacidade cumpra um papel positivo para o potencial de comunicação e relacionamentos do indivíduo.

De acordo com a referida exposição é possível compreender a afirmação feita inicialmente nesta seção, qual seja, que a proteção dos dados pessoais origina-se do processo evolutivo da privacidade. Isto porque a citação aborda a evolução da concepção de privacidade nas últimas décadas, destacando as transformações em seu perfil devido à complexidade de interesses e valores envolvidos. O autor aponta para uma mudança fundamental delineada por Stefano Rodotà, que sugere uma transição do paradigma tradicional "pessoa-informação-segredo" para o paradigma "pessoa-informação-circulação -controle". Essa mudança implica que o direito à privacidade não é mais centrado apenas na

preservação do segredo, mas também na gestão e controle da circulação de informações.

Destaca que essa evolução está associada à consolidação da teoria dos direitos da personalidade. Na sociedade da informação, a proteção da privacidade avança para territórios anteriormente inexplorados, sendo percebida como um elemento essencial para proporcionar ao indivíduo os meios necessários à construção e consolidação de sua esfera privada.

A abordagem de Doneda enfatiza que a tutela da privacidade desempenha um papel positivo no potencial de comunicação e relacionamentos individuais. Essa função é considerada crucial para a personalidade como um todo, ganhando ainda mais importância quando fatores como a vida e escolhas pessoais estão em jogo, abrangendo aspectos das relações privadas, uso de novas tecnologias, política e até mesmo na esfera pública. Demonstra a complexidade e a relevância contínua do tema, indicando como a proteção de dados pessoais se torna uma ferramenta fundamental na contemporaneidade.

Considerando que a proteção dos dados pessoais origina-se do processo evolutivo da privacidade, cabe citar Daniel Solove (2008, pg 756, tradução nossa)

> Em outras palavras, privacidade não é redutível a uma essência singular; é uma pluralidade de coisas diferentes que não partilham um elemento em comum, mas que, no entanto, carregam uma semelhança entre si (...) a coleta e uso de dados pessoais informações em bancos de dados apresentam um conjunto de problemas diferente do que o governo de vigilância.[2]

Este aborda a complexidade e a multifacetada natureza da privacidade. O autor argumenta que a privacidade não pode ser reduzida a uma essência única ou universal, mas sim compreendida como uma variedade de elementos distintos, que, embora não compartilhem um traço comum específico, possuem semelhanças entre si. Esse entendimento ressalta a diversidade de preocupações e contextos que envolvem a noção de privacidade.

Solove exemplifica essa diversidade ao destacar a coleta e uso de dados pessoais por entidades em bancos de dados com a vigilância governamental. Ele sugere que essa situação apresenta um conjunto distinto de desafios e implicações, destacando que a vigilância governamental levanta questões relacionadas a direitos individuais, liberdades civis e potencial abuso de poder estatal.

---

[2] *In other words, privacy is not reducible to a singular essence; it is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other. (...) the collection and use of personal information in databases presents a different set of problems than government surveillance.*

Essa questão ressalta a necessidade de uma abordagem contextualizada e flexível para lidar com as questões de privacidade, reconhecendo as diferentes nuances e dimensões que permeiam esse conceito. A compreensão desta como uma pluralidade de elementos semelhantes, mas distintos, contribui para uma análise mais abrangente e precisa das complexidades envolvidas na proteção dos direitos individuais em diversos contextos sociais, econômicos e políticos.

Na visão de Doneda, a privacidade acompanha a consolidação da teoria dos direitos da personalidade, assim, garantir a dignidade da pessoa humana através da proteção dos dados pessoais não gera um "individualismo exacerbado", mas no atual contexto social é fundamental para gerar segurança no compartilhamento de informações pessoais do indivíduo. Ainda quanto ao instituto da personalidade destaca-se o que preceitua Doneda (2021, p. 84):

> O instituto da personalidade era o que apresentava vocação mais forte para se tornar o centro de irradiação, no direito privado, dessa nova dogmática voltada à proteção da pessoa. A introdução dos direitos da personalidade no direito privado representa, nesse contexto, um caso exemplar de uma – algo dolorosa – modificação de uma estrutura cujo desenho era por demais rígido para atender a demandas que não pareciam contempladas em seu projeto original. Com o instrumento disponível – entre os mais caros aos códigos oitocentistas, o direito subjetivo – estruturado em torno da tutela da propriedade, ocorreu que a personalidade e seus vários aspectos, como o nome, a honra, imagem e outros, acabaram sendo abordados pelo direito civil do modo que ele poderia conceber: como direitos subjetivos da pessoa que, caso ofendidos, ensejariam reparação. (...) Nessa perspectiva, a multiplicação dos direitos subjetivos referentes aos aspectos da personalidade levou alguns juristas habituados à sistematização a procederem à realização de um verdadeiro inventário de quais seriam os direitos da personalidade previstos pelo ordenamento, enquanto outros juristas denunciaram o que viam como uma profusão inadequada desses direitos. Tornou-se uma solução frequente classificar esses direitos, particularizá-los, ressaltando características que os diferenciassem dos demais direitos subjetivos.

A referência aborda a inserção dos direitos da personalidade no contexto do direito privado, destacando a transformação dessa área jurídica para atender às demandas emergentes relacionadas à proteção da pessoa. O autor observa que o instituto da personalidade emergiu como o principal centro de irradiação dessa nova dogmática voltada à salvaguarda da pessoa no âmbito do direito privado. Essa mudança representa um exemplo notável de adaptação de uma estrutura legal que, inicialmente rígida, revelou-se insuficiente para abranger questões não contempladas em seu desenho original.

Doneda enfatiza que a introdução dos direitos da personalidade no direito privado reflete uma modificação estrutural, muitas vezes dolorosa, devido à rigidez da estrutura

anterior, centrada na tutela da propriedade. Os direitos da personalidade, incluindo aspectos como nome, honra e imagem, foram abordados dentro do direito civil como direitos subjetivos da pessoa, passíveis de reparação em caso de violação.

Na perspectiva apresentada, a proliferação dos direitos subjetivos relacionados à personalidade levou alguns juristas a realizar um inventário abrangente desses direitos no ordenamento jurídico, enquanto outros criticaram o que perceberam como uma profusão excessiva. Diante desse cenário, tornou-se comum classificar e particularizar esses direitos, destacando características distintivas que os diferenciassem de outros direitos subjetivos.

A observação de Doneda proporciona percepções sobre a dinâmica evolutiva do direito privado, evidenciando como a inclusão dos direitos da personalidade representou uma adaptação necessária para enfrentar novos desafios. A abordagem de inventariar e classificar esses direitos reflete a busca por uma compreensão mais clara e sistemática diante da multiplicidade de aspectos envolvidos na proteção da personalidade no contexto jurídico.

No que tange a teoria do direito geral da personalidade, o autor Mattietto (2017) pontua que esta se desenvolveu mais na Alemanha, mesmo havendo antecedentes na Áustria e na Suíça, "não obstante a projeção alcançada no espaço jurídico germânico, a teoria do direito geral de personalidade não teve a mesma envergadura no restante da Europa." Na Itália foi adotado o direito da personalidade em espécie, de modo que o Brasil se espelhou em tal modelo, relata o autor:

> Na Itália, embora seja intenso o debate entre a defesa de um único direito da personalidade ou a de uma série de direitos da personalidade, o legislador, ao editar o Código Civil de 1942, em plena época de regime fascista, preferiu tipificar alguns direitos da personalidade em espécie (...) O Código Civil Brasileiro de 2002 é claramente calcado no modelo italiano, prevendo alguns poucos direitos da personalidade em espécie (arts. 11 a 21). Além das manifestações legislativas, inclusive das que emanam de leis extravagantes (como, por exemplo, a Lei de Registros Públicos, o Estatuto da Criança e do Adolescente, o Estatuto do Idoso, o Estatuto da Pessoa com Deficiência), costuma-se apresentar, em sede doutrinária, relação bem mais extensa de direitos da personalidade, compondo um terreno fértil para a criação jurisprudencial de novas possibilidades, mesmo porque os tipos legais são relativamente escassos e estão longe de cobrir meticulosamente as situações da vida em que a proteção da personalidade pode ser invocada. (...) A promoção constitucional da cláusula geral de proteção da pessoa deve-se à imprescindibilidade de, diante da multiplicidade da vida real e da complexidade do comportamento humano, ir além dos parcos direitos especiais da personalidade expressamente previstos na legislação civil brasileira. O conceito de personalidade, como valor ético fundamental e como expressão da humanidade, impõe uma estrutura jurídica compreensiva, não reducionista, aberta e maleável, sem a qual se esvazia boa parte de seu conteúdo. Mesmo que abrangentes, múltiplos ou variados sejam os tipos com que se pretenda assegurar a proteção da pessoa, uma tutela limitada a direitos subjetivos legalmente estabelecidos será sempre redutora das amplas potencialidades da personalidade humana. Somente a técnica da cláusula geral tem a abertura e a

> mobilidade necessárias para enfrentar as vicissitudes, não raro inimagináveis, que surgem a cada dia na vida em sociedade, como as provocadas pela manipulação genética, pela tecnologia da informação e pela expansão das comunicações.

Mattietto observa que, na Itália, apesar do debate entre a defesa de um único direito da personalidade e a de uma série de direitos dessa natureza, o legislador optou por tipificar alguns desses direitos no Código Civil de 1942, durante o regime fascista. O autor destaca a influência do modelo italiano no Código Civil Brasileiro de 2002, que prevê alguns direitos da personalidade em espécie nos artigos 11 a 21.

Além das manifestações legislativas, observa-se que a doutrina brasileira costuma apresentar uma lista mais extensa de direitos da personalidade, criando um terreno propício para a criação jurisprudencial de novas possibilidades, dada a relativa escassez de tipos legais que cubram integralmente as situações da vida que demandam proteção da personalidade.

Argumenta-se que a promoção constitucional da cláusula geral de proteção da pessoa é necessária devido à multiplicidade da vida real e à complexidade do comportamento humano. O autor destaca que o conceito de personalidade, como valor ético fundamental e expressão da humanidade, requer uma estrutura jurídica compreensiva, aberta e maleável. A técnica da cláusula geral, segundo Mattietto, é a única capaz de lidar com as inúmeras vicissitudes, muitas vezes inimagináveis, que surgem na sociedade contemporânea, como as relacionadas à manipulação genética, tecnologia da informação e expansão das comunicações.

O trecho evidencia a complexidade na abordagem legislativa em relação aos direitos da personalidade, ressaltando a necessidade de uma proteção jurídica que vá além de uma lista limitada de direitos subjetivos legalmente estabelecidos, destacando a importância da cláusula geral como um instrumento flexível e adaptável diante das transformações sociais.

A proteção à personalidade não pode se restringir aos direitos elencados, devendo ter sua amplitude pautada no texto constitucional, com base na dignidade da pessoa humana, por ser este um dos fundamentos da República, como preceitua Doneda (2021, p. 96):

> Assim, o conjunto de situações-tipo presentes no Código Civil brasileiro sob a denominação de direitos da personalidade não devem ser lidas de forma a excluir absolutamente outras hipóteses não previstas; na verdade, muito mais importante que esse (tímido) elenco é a sua leitura à luz da cláusula geral de proteção da personalidade presente na Constituição. Assim, a chamada "positivação" dos direitos da personalidade pelo Código Civil não é o elemento fundador desses direitos, sendo sua função a de orientar a interpretação e facilitar a aplicação e a tutela nas hipóteses em que a experiência ou a natureza dos interesses possam inspirar o legislador a tratá-las com maior detalhe. A busca desse mencionado elemento "fundador" conduz à orientação axiológica constitucional, que coloca a dignidade da pessoa humana

> como fundamento da República (art. 1°, III), juntamente com os objetivos fundamentais de erradicação da pobreza e da marginalização, da redução das desigualdades sociais (art. 3°. III), e, não menos importante, a orientação do art. 5°, § 2°. de não excluir direitos e garantias, ainda que não expressos, desde que sejam decorrentes do texto constitucional.

Esta passagem aborda a questão da positivação dos direitos da personalidade no Código Civil brasileiro e a necessidade de interpretar esses à luz da cláusula geral de proteção da personalidade presente na Constituição Federal. O autor destaca que o conjunto de situações-tipo presentes no código sob a denominação de direitos da personalidade não deve ser interpretado de forma a excluir absolutamente outras hipóteses não previstas. Ressalta que, mais importante do que o elenco presentes no Código Civil, é a leitura à luz da cláusula geral constitucional de proteção da personalidade.

Doneda argumenta que a positivação dos direitos da personalidade pelo Código Civil não é o elemento fundador. Sua função é orientar a interpretação e facilitar a aplicação e a tutela, especialmente nas situações em que a experiência ou a natureza dos interesses possam inspirar o legislador a tratá-las com maior detalhe.

A busca pelo elemento instituidor conduz à orientação axiológica constitucional, destacando a dignidade da pessoa humana como fundamento da República, conforme o artigo 1°, III, da Constituição. Além disso, ressalta a importância dos objetivos essenciais da erradicação da pobreza e da marginalização, da redução das desigualdades sociais (art. 3°, III) e a orientação do artigo 5°, § 2°, que não exclui direitos e garantias não expressos, desde que decorrentes do texto constitucional.

Destaca-se a interrelação entre a legislação infraconstitucional e os princípios constitucionais, evidenciando a importância da cláusula geral de proteção da personalidade como norteadora da interpretação e aplicação dos direitos da personalidade previstos no Código Civil.

É imperioso destacar a importância da teoria dos direitos da personalidade no que tange a privacidade e a proteção de dados pessoais, vez que a mesma preza pela proteção da personalidade dialogando com a dignidade da pessoa humana e com os demais preceitos constitucionais, não se limitando a um rol taxativo imposto pelo legislador. Sendo fundamental em uma sociedade contemporânea onde a tecnologia da informação se desenvolve de forma acelerada, o que impossibilita o acompanhamento simultâneo do ordenamento jurídico. Portanto, faz-se necessário enfatizar a proteção de dados pessoais como uma política pública que foi reconhecida no ordenamento jurídico brasileiro como

Direito Fundamental.

2.1. Proteção de dados como direito e garantia fundamental

A proteção de dados é um tema de grande relevância em escala global, considerando a crescente interconexão digital e a constante coleta, processamento e compartilhamento de informações pessoais. A importância atribuída à privacidade reflete-se na ampla gama de medidas adotadas para regulamentar o tratamento das informações pessoais em diferentes contextos. Estatutos específicos, como leis de proteção de dados, são promulgados para estabelecer diretrizes claras sobre como as organizações devem lidar com as informações dos usuários. A privacidade e a proteção de dados emergem como pilares essenciais para preservar a integridade e a autonomia dos indivíduos em um mundo cada vez mais digitalizado, onde a confiança nas práticas de tratamento de dados é fundamental para o funcionamento eficiente e ético das sociedades contemporâneas, como preceitua Daniel Solove (2008, e-book, tradução nossa)

> A privacidade é uma questão de profunda importância em todo o mundo. Em quase todas as nações, numerosos estatutos, direitos constitucionais e decisões judiciais procuram proteger a privacidade. Na legislação constitucional de países ao redor do mundo, a privacidade está consagrada como um direito fundamental. (...) Além dos Estados Unidos, a grande maioria das nações protege o vazio de privacidade em suas constituições. Por exemplo, o Brasil proclama que "a privacidade, a intimidade, a vida privada, a honra e a imagem das pessoas são invioláveis"; a África do Sul declara que "todos têm direito à privacidade"; e a Coreia do Sul anuncia que "a privacidade de nenhum cidadão será violada". países reconheceram direitos constitucionais implícitos à privacidade, como o Canadá, a França, a Alemanha, o Japão e a Índia. Além disso, milhares de leis protegem a privacidade em todo o mundo. As diretrizes, diretivas e estruturas multinacionais de privacidade influenciaram a aprovação de leis de privacidade em um grande número de nações.[3]

O trecho extraído da obra *Understanding Privacy*, destaca a abrangência e a significativa importância da privacidade em escala global. Solove aponta que a questão da

---

[3] *Privacy is an issue of profound importance around the world. In nearly every nation, numerous statutes, constitutional rights, and judicial decisions cisions seek to protect privacy. In the constitutional law of countries around the globe, privacy is enshrined as a fundamental right. (...) Beyond the United States, the vast majority of nations protect privacy vacy in their constitutions. For example, Brazil proclaims that "the privacy, vacy, private life, honor and image of people are inviolable"; South Africa declares that "[e]veryone has the right to privacy"; and South Korea announces that "the privacy of no citizen shall be infringed." When privacy is not directly mentioned in constitutions, the courts of many countries have recognized implicit constitutional rights to privacy, vacy, such as Canada, France, Germany, Japan, and India. In addition, thousands of laws protect privacy around the world. Multinational privacy guidelines, directives, and frameworks have influenced fluenced the passage of privacy laws in a vast number of nations.*

privacidade é um tema central em quase todas as nações, onde uma série de dispositivos legais, como estatutos, direitos constitucionais e decisões judiciais, é empregada para salvaguardar esse direito fundamental. Destaca que a proteção da privacidade é consagrada em muitas legislações constitucionais ao redor do mundo, exemplificando ao citar dispositivos constitucionais de diferentes países, como o Brasil, a África do Sul e a Coreia do Sul, que expressam a inviolabilidade da privacidade, da vida privada, da honra e da imagem das pessoas.

A menção a países como Canadá, França, Alemanha, Japão e Índia reforça a amplitude do reconhecimento dos direitos constitucionais à privacidade, inclusive através de interpretações implícitas. O autor ressalta ainda que um grande número de leis, diretrizes e estruturas multinacionais de privacidade têm influenciado a promulgação de legislações específicas em diversas nações. Essa análise do autor salienta a complexidade e a diversidade de abordagens adotadas globalmente para proteger a privacidade, ressaltando que a discussão sobre esse direito transcende fronteiras e é moldada por uma variedade de contextos culturais, legais e políticos.

A Constituição da República Federativa do Brasil versa em seu Título II sobre os direitos e garantias fundamentais, onde no Capítulo I da referida titulação são elencados os direitos e deveres individuais e coletivos expressos no artigo 5º. O texto constitucional preceitua que as normas que definem direitos e garantias fundamentais possuem aplicabilidade imediata, bem como, deixa explícito que o rol de direitos e garantias fundamentais expressos na lei maior não constituem um rol taxativo, vez que não exclui outros direitos e garantias decorrentes do regime e dos princípios adotados por esta ou por tratados internacionais em que o Brasil seja parte.[4]

Isto posto, de acordo com José Afonso da Silva (2012, p. 177-180) é dificultoso definir um conceito sintético e certeiro para os direitos fundamentais do homem devido a sua aplicação e transformação no envolver histórico, algo que aumenta essa dificuldade são as diversas expressões utilizadas para nomeá-lo. O autor pontua as seguintes expressões: direitos naturais, direitos humanos, direitos do homem, direitos individuais, direitos públicos subjetivos, liberdades fundamentais, liberdades públicas e direitos fundamentais do homem.

[4]Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.§ 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.

Para além, o autor aponta que a expressão Direitos Fundamentais do homem seria a que melhor se adequaria ao estudo, por fazer menção a princípios que sintetizam a concepção do mundo, bem como, "informam a ideologia política de cada ordenamento jurídico, é reservada para designar, no nível do direito positivo, aquelas prerrogativas e instituições que ele concretiza em garantias de uma convivência digna, livre e igual de todas as pessoas." O autor esclarece que no que tange ao qualificativo "fundamentais" encontra-se a designação de situação jurídica sem as quais "a pessoa humana não se realiza, não convive e, às vezes, nem mesmo sobrevive; fundamentais do homem no sentido de que a todos, por igual, devem ser, não apenas formalmente reconhecidos, mas concreta e materialmente efetivados."

Cumpre destacar que o texto constitucional não apresenta uma distinção entre direitos e garantias fundamentais, neste sentido, Silva (2012, p. 188-191) relata que

> Não são nítidas porém as linhas divisórias entre direitos e garantias (...) A Constituição, de fato, não consigna regra que aparte as duas categorias, nem sequer adota terminologia precisa a respeito das garantias. Assim, é que a rubrica do Título II enuncia: Dos direitos e garantias fundamentais", mas deixa à doutrina pesquisar onde estão os direitos e onde se acham as garantias. O Capítulo I desse Título traz a rubrica: "Dos direitos e deveres individuais e coletivos", não menciona as garantias, mas boa parte dele constitui-se de garantias. Ela se vale de verbos para declarar direitos que são mais apropriados para enunciar garantias. Ou talvez melhor, diríamos, ela reconhece alguns direitos garantindo-os. Por exemplo: (...) "é garantido o direito de propriedade" (art. 5ºXXII), (...) Já noutro dispositivo está que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [...]" (art. 5º, X); aqui o direito e a garantia se integram: inviolabilidade = garantia; intimidade, vida privada, honra, imagem pessoal = direito de privacidade. (...) As garantias constitucionais em conjunto caracterizam-se como imposições, positivas ou negativas, aos órgãos do Poder Público, limitativas de sua conduta, para assegurar a observância ou, no caso de violação, a reintegração dos direitos fundamentais.

Como observa o autor, o texto constitucional não apresenta uma distinção entre o contexto de direitos e garantias fundamentais, entretanto, é possível observar que as garantias fundamentais estão expressas majoritariamente nos incisos do artigo 5º da Constituição Federal, o que é imprescindível ser observado tendo em vista a temática abordada nesta seção, o autor ainda pontua que as garantias constitucionais caracterizam-se como imposições aos órgãos do Poder Público, o que limita sua conduta com o fito de assegurar a observância dos direitos fundamentais ou ainda a reintegração destes quando violados.

Desta maneira, essa sucinta contextualização fez-se necessária tendo em vista que a proteção de dados pessoais foi reconhecida como Direito Fundamental assegurado no artigo 5º, inciso LXXIX da CRFB/1988, pela Emenda Constitucional (EC) nº 115/2022 que alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias

fundamentais, como exposto, e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Cabe uma breve análise do inciso LXXIX que versa que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". É possível perceber que este inciso apresenta uma garantia presente no termo "é assegurado", bem como apresenta explicitamente o direito fundamental à proteção dos dados pessoais. Visualiza-se que o texto introduzido pela EC nº 115/2022, abarca uma garantia e um direito fundamental. Para além, o que deu origem a referida EC foi a Proposta de Emenda à Constituição (PEC) nº 17/2019, portanto, para uma melhor compreensão desta temática, é importante proceder a análise da justificação da referida PEC.

A justificação da Pec nº 17/2019 expõe que a proteção de dados pessoais é consequência do desenvolvimento histórico da sociedade internacional, e com esta afirmativa apresenta o contexto legislativo de alguns países no que tange a privacidade e proteção de dados, apontando que este tema, com a era informacional, tem propiciado cada vez mais riscos às liberdades e garantias individuais do cidadão.

Prossegue relatando que o avanço tecnológico apresenta lado positivo e negativo, vez que oportuniza racionalização de negócios e de atividade econômica, gerando empregabilidade, prosperidade e maior qualidade de vida, entretanto, quando mal utilizada ou quando utilizada sem parâmetro moral e ético, pode causar prejuízos aos cidadãos e a sociedade, gerando concentração de mercados.

Relata que este é o motivo que levou países de todo o globo a compreenderem a importância e imprescindibilidade da regularização jurídica do tratamento de dados dos cidadãos, sendo citado como exemplificação a União Europeia que instituiu o *General Data Protection Regulation* (GDPR) que entrou em vigor em 25 de maio de 2018, gerando impacto de nível global. Menciona ainda que na América do Sul o Chile e a Argentina já contam com leis próprias de proteção de dados, assim como outros países vizinhos.

Pondera que as discussões e regulações dessa natureza têm partido da privacidade, porém já se avista uma autonomia valorativa em volta da proteção de dados pessoais devido às suas peculiaridades, ressaltando o seu merecimento quanto a tornar-se um direito constitucional assegurado. Prossegue explicando que em Portugal, a Constituição de 1976 já fazia menção à proteção aos dados pessoais, e, acesso aos recursos de informática. Traz ainda a colocação que é possível verificar algo parecido na Estônia, Polônia e atualmente no Chile que em 2018 constitucionalizou a proteção de dados pessoais.

A justificação ressalta a convicção dos proponentes da PEC nº 17/ 2019 quanto a necessidade da mudança Constitucional por ser necessário mais que uma lei ordinária versando sobre o tema, mesmo diante da importância jurídica da Lei nº 13.709/2018 (LGPD), a proposta versa sobre instituir o direito fundamental à proteção de dados pessoais e determinar a competência constitucional para legislar sobre a aludida temática.

Teve por base o fato de existirem inúmeras propostas de leis estaduais e municipais pretendendo tratar sobre o tema, até mesmo replicando o contexto da LGPD, porém isto não é racional, vez que não se deve fragmentar e pulverizar assunto de tamanha importância à sociedade, de forma que o ideal é que pertença à União a centralidade da competência legislativa, como ocorre com outros direitos fundamentais, bem como, temas gerais relevantes. Evitando que surjam no país milhares de conceitos legais estabelecendo o que é "dado pessoal", "agentes de tratamentos" e outras definições já presentes na LGPD. Os principais conceitos para a compreensão da temática em desenvolvimento serão abordadas ainda nesta seção na subseção Conceitos relevantes.

É imperioso que o país apresente uniformidade quanto a legislação de proteção e tratamento de dados pessoais, vez que é inviável as empresas e governos mundiais se adequarem às normativas específicas de cada estado ou município. A justificação ainda relata que a multiplicidade normativa pode causar problemas de compatibilidade e adequação dos dados.

Evidencia os serviços que são disponibilizados pela rede mundial de computadores, pois estes utilizam os dados pessoais de maneira cada vez mais inovadora e abrangente. Expõe que a alteração "é altamente aconselhável para a racionalização do tratamento de dados no país e sua inclusão na realidade internacional da disciplina da matéria."

A PEC nº 17/2019 tramitou pelo Congresso Nacional e a EC nº 115/2022 foi Promulgada em 11 de fevereiro de 2022, este foi um grande ganho para o ordenamento jurídico brasileiro, vez que ter a proteção de dados pessoais não apenas regulamentada em legislação infraconstitucional, mas agora com status de Direito Fundamental demonstra a importância da temática, reconhecendo que a mesma está intrinsecamente ligada à personalidade e da dignidade da pessoa humana.

Este reconhecimento fez-se importante não apenas em âmbito nacional no que tange aos titulares de dados, mas em âmbito internacional, vez que a proteção de dados pessoais é assunto de relevância mundial, e na contemporaneidade interfere nas relações de mercado entre os países, os que não atendem as exigências impostas pelos que já se encontram

avançados quanto a proteção de dados pessoais, ficam impedidos de transacionar com estes, um grande exemplo é a União Europeia que instituiu o *General Data Protection Regulation* (GDPR) e o Brasil que instituiu a LGPD.

No Brasil, por ser um país de proporções continentais, além de instituir a LGPD, foi necessário promulgar a EC nº 115/2022 não só elevando a proteção de dados pessoais ao status de Direito Fundamental, mas também fixando a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais, vez que muitos Estados e Municípios da Federação já estavam iniciando projetos legislativos com o objetivo de tratar sobre esta temática, o que causaria insegurança jurídica e conflito nas relações de mercado com empresas multinacionais.

Desta forma, a lei maior abarcou a Proteção de Dados Pessoais consagrando-a como Direito e Garantia Fundamental, ainda, limitando a competência privativa da União para legislar quanto ao tema, não dando brecha para a insegurança jurídica e possibilitando ao Brasil uma boa relação de mercado interno e externo no que tange a proteção de dados pessoais, bem como garantindo ao titular dos dados pessoais a aplicação imediata das normas que versem sobre o direito fundamental à proteção de dados pessoais, atualmente uma política pública de grande relevância no Brasil e no mundo.

Partindo desta vertente, pontua-se que os direitos e garantias fundamentais são ocasionadores de políticas públicas, vez que se concretizam por meio de prestações positivas do Estado, que, através da função estatal, conduz a efetivação de direitos dos cidadãos coordenando as ações públicas e privadas, sendo alicerçada pela Teoria dos Direitos Fundamentais. Neste sentido, Fonte (2021, p 124-125) ao dialogar sobre esta teoria, a estrutura na dignidade da pessoa humana

> O segundo ponto a considerar consiste na adoção do princípio da dignidade da pessoa humana enquanto elemento-chave da ordem constitucional que entrou em vigor em 1988. O princípio encontra-se previsto no art. 1º, III, da Constituição Federal de 1988, onde ostenta a qualidade de fundamento da República. (...). De acordo com a doutrina, trata-se do "ponto de Arquimedes no Estado constitucional", de modo que seu valor enquanto fonte própria e autônoma de obrigações e direitos não pode ser esquecido. O princípio da dignidade humana tem o importante papel de conferir unidade de sentido ao sistema de direitos fundamentais, sendo certo que estes se ancoram naquela, isto é, existem em função da necessidade de se garantir a dignidade do ser humano. O problema na conceituação da expressão "dignidade humana" leva à conclusão de que os órgãos investidos de legitimidade democrático-eleitoral devem ter papel importante neste trabalho, mas não torna inviável o reconhecimento, desde logo, de elementos essenciais ao conceito. Sendo assim, a adoção do princípio da dignidade e a necessidade de sua observância, que pode ocorrer em diversos graus, permitem o reconhecimento de dois níveis de direitos fundamentais na Constituição de 1988: (i) aqueles de imposição obrigatória,

> diretamente vinculados à materialização do seu núcleo (identificados como mínimo existencial); e (ii) os demais, consagrados normativamente pelo constituinte de 1988 e ligados, ainda que em grau menos intenso, à dignidade da pessoa humana, mas que podem se submeter à concretização realizada pelo legislador e pelo administrador público.

O trecho ressalta a importância da dignidade da pessoa humana como elemento central da ordem constitucional instituída em 1988 no Brasil. O princípio, delineado no artigo 1º, III, da Constituição Federal, é consagrado como fundamento da República, sendo descrito pela doutrina como o "ponto de Arquimedes no Estado constitucional". Nesse contexto, destaca-se a autonomia e a centralidade desse na geração de obrigações e direitos, ressaltando sua natureza como fonte própria e independente.

A dignidade da pessoa humana desempenha um papel unificador no sistema de direitos fundamentais, fornecendo uma base essencial para a compreensão e aplicação coerente desses direitos. A complexidade na conceituação do termo "dignidade humana" é reconhecida, indicando que os órgãos legitimados democraticamente têm um papel significativo na definição desse conceito, mas não impedindo o reconhecimento prévio de elementos essenciais.

A adoção deste princípio permite a identificação de dois níveis de direitos fundamentais, primeiramente, aqueles de imposição obrigatória, diretamente vinculados à materialização do núcleo essencial (identificados como mínimo existencial). Em segundo lugar, outros direitos, normativamente consagrados pelo constituinte, que, embora estejam associados, em grau menos intenso, podem ser objeto de concretização pelo legislador e pelo administrador público.

Dessa forma, a argumentação apresenta uma análise crítica e abrangente sobre a posição central da dignidade humana na ordem constitucional, destacando suas implicações na interpretação e hierarquização dos direitos fundamentais. A proteção dos dados pessoais estão abarcadas por estes e encontra fundamento na Teoria dos Direitos Fundamentais, de forma que o princípio da dignidade da pessoa humana tem importante papel de lhe conferir sentido, devendo, pois, ser observado por todos os sujeitos inerentes à relação, sendo dever do Estado prezar pelo fiel cumprimento.

Exemplificando na vertente da proteção de dados pessoais, o Executivo Federal por meio do Ministério da Gestão e da Inovação em Serviços Públicos e da Secretaria de Governo Digital, estabeleceu o Programa de Privacidade e Segurança da Informação (PPSI) no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional,

através da Portaria SGD/MGI nº 852/2023, onde destacam-se alguns conceitos: (i) controle de privacidade, sendo este o conjunto de medidas que visam implementar práticas técnicas e gerenciais para a proteção de dados pessoais em ativos de informação; (ii) proteção de dados pessoais, nos termos do inciso LXXIX do art. 5º da Constituição da República Federativa do Brasil de 1988, que constitui as ações que visam proteger direitos e liberdades fundamentais das pessoas naturais, entre eles a sua privacidade, inclusive em meios digitais; (iii) privacidade como direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, nos termos do inciso X do art. 5º da Constituição da República Federativa do Brasil de 1988, esta portaria será abordada na seção 3 deste trabalho acadêmico.

A ação do Estado no campo da política pública no que concerne à atuação dos três Poderes, é apresentada por Fonte (2021, p.86-87), quanto ao Poder Legislativo o autor menciona que "é a instituição que repercute de modo mais fiel, ainda que não perfeito, as preferências políticas de determinada sociedade". No Poder Executivo faz referência a Administração Pública destacando que é a instituição que encontra-se mais adequada para inteirar-se das normas jurídicas proferidas pelo Legislativo, assim, por questões institucionais deve prevalecer a competência da Administração Pública para concretizar as políticas públicas.

Entende que os órgãos e entidades do Executivo normalmente contam com técnicos que possuem especialização nos campos de atuação específicos, porém, relata que isto "não ocorre com o Poder Judiciário, que dispõe de juízes generalistas e peritos frequentemente nomeados ad hoc", segue alertando que deixar o Judiciário conduzir decisões políticas coletivas em caráter primário é realizar a supressão do direito à igualdade participativa característica às democracias, além de estar contribuindo para que decisões pontuais se sobreponham às decisões coletivas, o que é contrário ao princípio da separação dos poderes. Entretanto, o STF no tema 698, RE 684612 destaca que

> 1. A intervenção do Poder Judiciário em políticas públicas voltadas à realização de direitos fundamentais, em caso de ausência ou deficiência grave do serviço, não viola o princípio da separação dos poderes. 2. A decisão judicial, como regra, em lugar de determinar medidas pontuais, deve apontar as finalidades a serem alcançadas e determinar à Administração Pública que apresente um plano e/ou os meios adequados para alcançar o resultado. 3. No caso de serviços de saúde, o déficit de profissionais pode ser suprido por concurso público ou, por exemplo, pelo remanejamento de recursos humanos e pela contratação de organizações sociais (OS) e organizações da sociedade civil de interesse público (OSCIP).

O STF trata da intervenção do Poder Judiciário em políticas públicas direcionadas à concretização de direitos fundamentais, particularmente em situações em que há ausência ou falha significativa na prestação desses serviços pelo Estado. A discussão central gira em torno da possível violação ao princípio da separação dos poderes quando o Judiciário interfere nas políticas públicas.

Uma das principais conclusões do tema é que a atuação do Poder Judiciário nesse contexto não fere o princípio da separação dos poderes. Isso porque, diante da inércia ou incapacidade do Poder Executivo em assegurar direitos fundamentais, o Judiciário pode e deve intervir para garantir a sua efetivação.

No entanto, a decisão judicial não deve se limitar a determinar medidas pontuais, mas sim apontar as finalidades a serem alcançadas. É esperado que o Judiciário ordene à Administração Pública que elabore um plano ou adote os meios adequados para alcançar o resultado desejado. Essa abordagem visa garantir que a intervenção judicial seja direcionada para solucionar de maneira estrutural as deficiências identificadas nos serviços públicos, em consonância com os princípios constitucionais e respeitando as competências de cada poder.

Assim, o Tema 698 do STF estabelece parâmetros importantes para a atuação do Judiciário em questões relacionadas às políticas públicas, reforçando a sua responsabilidade na proteção e promoção dos direitos fundamentais, ao mesmo tempo em que delimita sua intervenção para preservar o equilíbrio entre os poderes e o princípio da legalidade.

Focalizando na política pública de proteção de dados pessoais, tem-se que o Poder Legislativo tendo em vista a necessidade do país quanto a regulamentação da proteção de dados pessoais, incluiu esta demanda em sua agenda política, o que deu origem a LGPD, e posteriormente a EC nº 115/2022. Entretanto, cabe à Administração Pública inteirar-se da LGPD e dar efetividade à norma fiscalizando, aplicando as sanções previstas na legislação, promovendo políticas públicas de conscientização, educativas etc. Já a intervenção judicial deve ser direcionada para solucionar de maneira estrutural as deficiências identificadas nos serviços públicos, em consonância com os princípios constitucionais e respeitando as competências de cada poder.

Tendo em vista o status de Direito Fundamental da Proteção de Dados Pessoais este trabalho acadêmico tem como alicerce a teoria geral do direito da personalidade e a teoria do direito fundamental, ambas pautadas na dignidade da pessoa humana, vez que a proteção de dados pessoais é um processo evolutivo do direito da privacidade, voltado a garantir a segurança das informações pessoais do titular dos dados.

Com base na teoria geral do direito da personalidade e na teoria do direito fundamental, seguirá sendo desenvolvida a temática da proteção da pessoa como titular dos dados, bem como, a temática política pública de proteção dos dados pessoais como direito fundamental, respectivamente, com enfoque na investigação da política pública de proteção de dados pessoais aplicada às informações pessoais de estudantes na UFRRJ, ato contínuo, cabe efetuar a análise da Legislação que embasa esta pesquisa e a importância dos Princípios que regem a Proteção de dados pessoais.

2.2. A Lei Geral de Proteção de Dados Pessoais

É imperioso atentar-se que os dados pessoais sempre existiram, vez que informações que identificam um indivíduo em todo tempo estiveram presentes nas relações sociais, bem como estes sempre foram colhidos para compor fichários com informações dos cidadãos, porém essa coleta efetuada por setores públicos ou privados era feita de forma manual, e não havia uma disciminação em tempo real, ou mesmo um compartilhamento em massa dessas informações.

Entretanto, com o desenvolvimento tecnológico essas informações deixaram o campo restrito dos antigos fichamentos manuais e passaram a ser coletadas e manuseadas com aparatos tecnológicos, o que possibilitou os mais diversos tipos de tratamento de dados pessoais. Ocorre que com esse processo evolutivo os dados pessoais passaram a ser um grande combustível econômico, fazendo com que o limite da esfera privada do titular dos dados começasse a ser violada, com a ressalva que esta violação perpassa os limites territoriais de cada País. Com a globalização os dados pessoais passaram a percorrer o mundo sem nenhum tipo de regulamentação específica, o que levou à necessidade de normatizar o tema de forma global. Neste sentido, preceituam Daniel Solove e Paul Schwartz (2021, e-book, tradução nossa)

> A informação é a força vital da sociedade atual. Cada vez mais, as nossas atividades diárias envolvem a transferência e o registo de informações. O governo recolhe grandes quantidades de informações pessoais em registos relativos ao nascimento, casamento, divórcio, propriedade, processos judiciais, veículos automotores, atividades de voto, transgressões criminais, licenciamento profissional e outras atividades de um indivíduo. As entidades do sector privado também acumulam bases de dados gigantescas de informações pessoais para fins de marketing ou para preparar históricos de crédito. Onde quer que vamos, façamos o que fizermos,

> poderíamos facilmente deixar para trás um rastro de dados que são registrados e reunidos. Estas novas tecnologias, juntamente com a utilização crescente de informações pessoais pelas empresas e pelo governo, colocam novos desafios para a proteção da privacidade.[5]

A citação extraída do livro *Consumer Privacy and Data Protection*, destaca a centralidade da informação na sociedade contemporânea, sublinhando a onipresença da transferência e registro de dados nas atividades cotidianas. Os autores evidenciam o papel proeminente do governo na coleta extensiva de informações pessoais, abrangendo uma ampla gama de domínios, desde eventos cruciais como nascimento e casamento até detalhes relacionados a processos judiciais, propriedade, veículos automotores, atividades de voto, transgressões criminais e licenciamento profissional. Adicionalmente, destacam o setor privado, que acumula grandes bases de dados para fins de marketing e elaboração de históricos de crédito, por exemplo.

Ao observar a interseção entre as novas tecnologias e a crescente utilização de informações pessoais por entidades governamentais e privadas, ressaltam os desafios emergentes para a preservação da privacidade. Esta análise crítica sugere uma reflexão sobre as implicações éticas, sociais e legais associadas à proliferação de dados pessoais. Além disso, apontam para a necessidade premente de estratégias eficazes de proteção da privacidade diante das transformações tecnológicas e das práticas disseminadas de coleta e utilização de informações pessoais. Nesse contexto, Solove e Schwartz fornecem um panorama abrangente sobre a interação complexa entre sociedade, tecnologia e privacidade, contribuindo para o entendimento acadêmico e crítico desse fenômeno contemporâneo.

Na referida obra, Solove e Schwartz também destacam que a salvaguarda da privacidade figura como um elemento fundamental para a preservação da liberdade, a consolidação da democracia e a garantia da segurança (SOLOVE; SCHWARTZ, 2021, e-book)

---

[5] *Information is the lifeblood of today's society. Increasingly, our everyday activities involve the transfer and recording of information. The government collects vast quantities of personal information in records pertaining to an individual's birth, marriage, divorce, property, court proceedings, motor vehicles, voting activities, criminal transgressions, professional licensing, and other activities. Private sector entities also amass gigantic databases of personal information for marketing purposes or to prepare credit histories. Wherever we go, whatever we do, we could easily leave behind a trail of data that is recorded and gathered together. These new technologies, coupled with the increasing use of personal information by business and government, pose new challenges for the protection of privacy.*

> Em primeiro lugar, na era da informação de hoje, a privacidade é uma questão primordial para a liberdade, a democracia e a segurança. Uma das questões centrais da privacidade da informação diz respeito ao poder das entidades comerciais e governamentais sobre a autonomia individual e a tomada de decisões. A privacidade também diz respeito ao estabelecimento de regras que possam limitar esta autonomia e tomada de decisão, permitindo necessariamente que entidades comerciais e governamentais tenham acesso a informações pessoais. Entendida de forma ampla, a privacidade da informação desempenha um papel importante na sociedade que estamos construindo na Era da Informação de hoje. Em segundo lugar, a privacidade da informação é uma questão de crescente preocupação pública. A privacidade das informações tornou-se uma prioridade na agenda legislativa do Congresso e de muitas legislaturas estaduais. Os problemas de privacidade de informações também são oportunos, aparecem frequentemente nos noticiários e são frequentemente objeto de litígio. Terceiro, existem muitas novas leis e desenvolvimentos jurídicos relativos à privacidade das informações. É uma área de crescimento no direito. O aumento dos litígios, da legislação, da regulamentação, bem como da preocupação pública com a privacidade, estão a estimular as empresas de vários sectores a abordar a questão da privacidade. Os advogados estão elaborando políticas de privacidade, litigando questões de privacidade e desenvolvendo maneiras para que empresas pontocom, corporações, hospitais, seguradoras e bancos se adaptem às regulamentações de privacidade.[6]

O trecho aborda de maneira abrangente a relevância da privacidade na sociedade da informação. Inicialmente, os autores destacam a centralidade da privacidade no contexto da liberdade, democracia e segurança na era da informação. A ênfase recai sobre a complexidade das questões relacionadas ao poder exercido por entidades comerciais e governamentais sobre a autonomia individual e a tomada de decisões, salientando a necessidade de estabelecer regras que equilibrem o acesso a informações pessoais e a proteção da autonomia individual.

Além disso, a análise apresenta a privacidade da informação como uma preocupação crescente na esfera pública, refletida na agenda legislativa do Congresso e em legislaturas estaduais dos Estados Unidos – como visto, esta questão tem espaço na agenda legislativa de

---

[6] *First, in today's Information Age, privacy is an issue of paramount significance for freedom, democracy, and security. One of the central issues of information privacy concerns the power of commercial and government entities over individual autonomy and decision making. Privacy also concerns the drawing of rules that may limit this autonomy and decision making by necessarily permitting commercial and government entities access to personal information. Understood broadly, information privacy plays an important role in the society we are constructing in today's Information Age. Second, information privacy is an issue of growing public concern. Information privacy has become a priority on the legislative agenda of Congress and many state legislatures. Information privacy problems are also timely, frequently in the news, and often the subject of litigation. Third, there are many new laws and legal developments regarding information privacy. It is a growth area in the law. Increased litigation, legislation, regulation, as well as public concern over privacy are spurring corporations in a variety of businesses to address privacy. Lawyers are drafting privacy policies, litigating privacy issues, and developing ways for dot-com companies, corporations, hospitals, insurers, and banks to conform to privacy regulations.*

muitos países. Os problemas de privacidade ganham destaque nos noticiários e se tornam frequentemente objeto de litígio, evidenciando a importância atribuída a essa questão no setor público. A terceira dimensão abordada diz respeito aos recentes desenvolvimentos legais e normativos relacionados à privacidade da informação, caracterizando-a como uma área em expansão no campo do direito.

A expansão legislativa, regulatória e a crescente conscientização pública sobre a privacidade estimulam diversas empresas em setores diversos a enfrentarem ativamente os desafios associados à privacidade. Advogados desempenham um papel crucial na elaboração de políticas de privacidade, na resolução de litígios e na adaptação das empresas às regulamentações emergentes. Este panorama abrangente delineado por Solove e Schwartz oferece uma compreensão atualizada das dinâmicas envolvidas na preservação da privacidade da informação na sociedade atual.

Devido a relevância da temática para o ordenamento jurídico brasileiro e a pressão externa que se desencadeou após a União Europeia instituir o GDPR, foi publicada no Brasil a LGPD, o que configurou um grande avanço na construção da política pública de proteção de dados pessoais no país.

2.2.1. Conceitos relevantes

A LGPD delibera a respeito do tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, tendo como objetivo proteger os direitos fundamentais de liberdade e de privacidade, bem como, o livre desenvolvimento da personalidade da pessoa natural. Desta forma, as normas gerais desta lei são de interesse nacional, de forma que a União, os Estados, o Distrito Federal e os Municípios devem observá-las.

O presente trabalho acadêmico delimita a análise da proteção de dados pessoais ao tratamento por pessoa jurídica de direito público, vez que o campo de estudo é a UFRRJ, uma autarquia federal, que tem como atividade principal desenvolver a educação superior[7] com

[7] Lei nº 9394/96 - Art. 43. A educação superior tem por finalidade:I - estimular a criação cultural e o desenvolvimento do espírito científico e do pensamento reflexivo; II - formar diplomados nas diferentes áreas de conhecimento, aptos para a inserção em setores profissionais e para a participação no desenvolvimento da sociedade brasileira, e colaborar na sua formação contínua; III - incentivar o trabalho de pesquisa e investigação científica, visando o desenvolvimento da ciência e da tecnologia e da criação e difusão da cultura, e, desse modo, desenvolver o entendimento do homem e do meio em que vive; IV - promover a divulgação de conhecimentos culturais, científicos e técnicos que constituem patrimônio da humanidade e comunicar o saber através do ensino, de publicações ou de outras formas de comunicação; V - suscitar o desejo permanente de aperfeiçoamento

base na política pública educacional do governo.[8]

Para uma análise mais precisa da aludida temática, é imperioso destacar a definição de alguns termos cruciais no que tange a pesquisa pautada na LGPD. Para que tais definições sejam efetuadas de forma precisa, valer-se-á do conceito constante artigo 5º da Lei nº 13.709/2018, cabendo ressaltar que a compreensão de cada termo é fundamental para o alcance do resultado da pesquisa. É importante enfatizar que a Proteção de Dados Pessoais contempla um estudo multidisciplinar que perpassa a esfera da Tecnologia da Informação, de inúmeras áreas do Direito, da Governança entre outros universos de contemplação, desta forma, a análise dos termos proporciona clareza à exposição.

Deste modo, um dos termos mais utilizado no corpo deste trabalho acadêmico será *dado pessoal*, sendo definido pela legislação como "informação relacionada a pessoa natural identificada ou identificável". Como já mencionado, a informação relacionada a um indivíduo é algo que sempre existiu, e dentro dessa vertente a LGPD adota um conceito aberto de dado pessoal, ou seja, a lei não restringe dados pessoais a nome, CPF, endereço ou Registro Geral, mas sim a qualquer informação que identifique ou venha a identificar uma pessoa natural, podendo esta informação ser sua aparência, seus hábitos de consumo, um apelido ou qualquer outro aspecto de sua personalidade.

Desta maneira, vislumbrando que um dado pessoal pode ser qualquer aspecto da personalidade da pessoa natural que a identifique ou a torne identificável, a lei também contemplou que o dado pessoal pode ser classificado como sensível, sendo esta distinção muito importante para o titular dos dados, vez que o *dado pessoal sensível* requer um tratamento diferenciado, revestido de maior cautela, consistindo este nos dados "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político", abarcando ainda o "dado referente à saúde ou à vida sexual, dado genético ou biométrico" quando esses dados estiverem vinculados a uma pessoa

---

cultural e profissional e possibilitar a correspondente concretização, integrando os conhecimentos que vão sendo adquiridos numa estrutura intelectual sistematizadora do conhecimento de cada geração; VI - estimular o conhecimento dos problemas do mundo presente, em particular os nacionais e regionais, prestar serviços especializados à comunidade e estabelecer com esta uma relação de reciprocidade; VII - promover a extensão, aberta à participação da população, visando à difusão das conquistas e benefícios resultantes da criação cultural e da pesquisa científica e tecnológica geradas na instituição. VIII - atuar em favor da universalização e do aprimoramento da educação básica, mediante a formação e a capacitação de profissionais, a realização de pesquisas pedagógicas e o desenvolvimento de atividades de extensão que aproximem os dois níveis escolares.

[8] Lei nº 9394/96 - Art. 8º A União, os Estados, o Distrito Federal e os Municípios organizarão, em regime de colaboração, os respectivos sistemas de ensino. § 1º Caberá à União a coordenação da política nacional de educação, articulando os diferentes níveis e sistemas e exercendo função normativa, redistributiva e supletiva em relação às demais instâncias educacionais.§ 2º Os sistemas de ensino terão liberdade de organização nos termos desta Lei.

natural.

É possível verificar que a legislação apresenta um rol taxativo quanto aos dados pessoais sensíveis, e estes estão relacionados a aspectos da personalidade do indivíduo que podem deixá-lo mais vulnerável em caso de tratamento inadequado dos dados, por este motivo, a LGPD cedeu uma seção da normativa para regulamentar sobre o tratamento dos dados sensíveis, vez que este precisa ser realizado com maior rigor e diligência, resguardando a intimidade do titular.

Para além, *banco de dados* é um termo que a compreensão é de extrema importância, deve-se atentar que os dados pessoais geralmente são armazenados, o que por sua vez forma o banco de dados, assim, este consiste no "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico". Antes da era digital as informações pessoais quando coletadas, após serem utilizadas ou durante o seu uso, também eram armazenadas, entretanto, os arquivos físicos gerados não chegavam a formar um conjunto estruturado de dados. Atualmente o armazenamento de dados formam conjuntos estruturados, como por exemplo o *Big Data*.

Desta forma, no que tange ao estudo sobre proteção de dados pessoais é imperioso destacar que toda operação efetuada com dados pessoais é denominada de *tratamento*, portanto quando há coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, há tratamento de dados pessoais.

Sublinha-se que a legislação contempla a *anonimização* como sendo a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo", ou seja, a anonimização é a utilização dos meios técnicos que trata um dado pessoal para torná-lo anonimizado. Já o *dado anonimizado* é o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

Ressalta-se ainda que os dados anonimizados não são considerados dados pessoais pela LGPD, desde que o processo de anonimização ao qual esses foram submetidos não seja revertido, pois neste caso esse tipo de dado anonimizado não será capaz de tornar uma pessoa natural identificada ou identificável, entretanto se "o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços

razoáveis, puder ser revertido", passam a ser considerados dados pessoais, conforme preceitua o artigo 12.

É fundamental compreender que, de acordo com a LGPD, o *titular* é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento", ou seja, cada indivíduo é dono dos dados que lhe identificam, é um direito que abrange a personalidade, sendo estes dados submetidos aos *agentes de tratamento*, que segundo a definição da LGPD trata-se do controlador e do operador. Neste sentido, a lei versa que o *controlador* é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", sendo o *operador* a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

Deve-se atentar que o controlador e o operador pode ser tanto uma pessoa natural, quanto uma pessoa jurídica de direito público ou privado, por conseguinte, a título exemplificativo dentro do campo de estudo que se desenvolve esta pesquisa, no contexto de uma Instituição Federal de Ensino, o controlador será a própria Instituição, no caso desta pesquisa a UFRRJ, uma pessoa jurídica de direito público.

A LGPD apresentou a *Autoridade Nacional de Proteção de Dados (ANPD)*, sendo esta o "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional". Cabe salientar que a ANPD passou a pertencer a estrutura organizacional do Ministério da Justiça e Segurança Pública em janeiro de 2023, por meio do Decreto nº 11.348/2023[9].

Portanto, é possível verificar que ao se falar de tratamento de dados pessoais, há uma cadeia de sujeitos, e para estabelecer um canal de comunicação entre estes o legislador estabeleceu a figura do *encarregado*, sendo este a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, conforme definição da LGPD.

Outro termo de grande valia para compreensão da temática abordada e que é definido pela legislação é o *consentimento*, este é um dos requisitos para o tratamento de dados pessoais e consiste na "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". O consentimento precisa ser fornecido para finalidades específicas, pois autorizações genéricas para tratar dados é nula, ressalta-se ainda que este pode ser revogado a qualquer momento,

[9] DA ESTRUTURA ORGANIZACIONAL - Art. 2º O Ministério da Justiça e Segurança Pública tem a seguinte estrutura organizacional: (...) IV - entidades vinculadas: a) Conselho Administrativo de Defesa Econômica; e b) Autoridade Nacional de Proteção de Dados.

bastando para isto uma manifestação expressa do titular dos dados.

Ainda, no que tange ao tratamento de dados, é importante compreender que *bloqueio* trata-se da “suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados”, já a *eliminação* é a “exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado”, sendo importante destacar que todo dado pessoal que já atendeu a sua finalidade deve ser eliminado.

Ainda nesta vertente do tratamento de dados pessoais, é necessário compreender que a *transferência internacional de dados* trata-se da “transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro”, de forma que o *uso compartilhado de dados* trata-se da “comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos” devendo atentar que isto ocorre “no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados".

Também é de fundamental importância compreender o significado de *relatório de impacto à proteção de dados pessoais*, que consiste na "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

Tendo em vista que o campo de pesquisa deste trabalho acadêmico é a UFRRJ, a compreensão do termo *órgão de pesquisa* é de grande relevância para o presente trabalho acadêmico, e este consiste em "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”, ainda deve-se atentar que este órgão deve incluir “em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.”

Superada a definição de alguns termos relevantes para o aprofundamento da pesquisa, cabe efetuar um breve panorama sobre a LGPD. Neste sentido, a legislação adota como seus fundamentos, sustentando nesses pontos o motivo de sua importância para o ordenamento jurídico: o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da

imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

É possível vislumbrar que a LGPD destaca nos seus fundamentos dois dos fundamentos da República Federativa do Brasil previstos no artigo 1º da CRFB/88, sendo eles a dignidade e o exercício da cidadania[10], bem como, apresenta os direitos humanos, que é um dos princípios que regem as relações internacionais da República[11]. Salienta-se, ainda, a privacidade, a inviolabilidade da intimidade, da honra e da imagem, a liberdade de expressão, de informação, de comunicação e de opinião, vez que estes são consagrados como Direitos e Garantias Fundamentais Constitucionais[12].

Vislumbra-se que a LGPD firmou sua base fundamental na Lei Maior do ordenamento jurídico brasileiro, por tratar-se de uma legislação que tem como objeto o tratamento de dados pessoais que se configuram como aspectos da personalidade do indivíduo identificado ou identificável, não teria como deixar de consagrar em seus fundamentos alguns dos fundamentos da República, o que no contexto da proteção de dados pessoais é resguardado através dos direitos dos titulares, bem como, por meio da garantia do tratamento de dados realizado de forma lícita, sendo respeitada as limitações normativas.

A normativa contemplou um dos princípios constitucionais que regem as relações internacionais, sendo ele os Direitos Humanos. De forma que é imperioso atentar-se que a LGPD tem aplicabilidade a toda operação de tratamento realizada por pessoa jurídica de direito público ou privado, abarcando o contexto do mercado nacional, bem como do mercado internacional, desde que ocorra tratamento de dados.

---

[10] CRFB/88 - Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: I - a soberania; II - a cidadania; III - a dignidade da pessoa humana; IV - os valores sociais do trabalho e da livre iniciativa; V - o pluralismo político.

[11] CRFB/88 - Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: I - independência nacional; II - prevalência dos direitos humanos; III - autodeterminação dos povos; IV - não-intervenção; V - igualdade entre os Estados; VI - defesa da paz; VII - solução pacífica dos conflitos; VIII - repúdio ao terrorismo e ao racismo; IX - cooperação entre os povos para o progresso da humanidade; X - concessão de asilo político.

[12] CRFB/88 - Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) X - 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; IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; LXXII - conceder-se-á "habeas-data": a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (...)

No que tange aos fundamentos da LGPD, cabe atenção à autodeterminação informativa, que concede autonomia ao titular quanto ao tratamento dos seus dados pessoais, ou seja, o titular dos dados passa a ter controle sobre suas próprias informações, sendo seus direitos resguardados pela normativa que lhe confere um capítulo para regulamentá-los, bem como, é possível verificar que os princípios da LGPD também corroboram em resguardar o titular dos dados. Para compreender a autodeterminação informativa, cabe citar Doneda (2021, p. 173-175)

> O direito à autodeterminação informativa orienta até hoje a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistema jurídico romano-germânico – A autodeterminação informativa é, inclusive, um dos fundamentos da disciplina da proteção de dados de acordo com a LGPD. Concebido como um direito fundamental, na esteira do direito geral de personalidade, o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações. (...) Não obstante, uma crítica baseada em seus pressupostos e no estágio atual da tecnologia, bem como da doutrina, nos sugere estarmos atentos a alguns aspectos de sua enunciação. Os pontos essenciais desta crítica são os seguintes: em relação à autodeterminação informativa, deparamo-nos com a questão acerca do que propriamente significa esta "autodeterminação". Em uma hipótese, ela conferiria ao indivíduo a oportunidade de controlar as informações que lhe digam respeito, dentro de parâmetros de ampla informação e solidariedade; já em uma leitura em chave mais liberal, a autodeterminação estaria concentrada no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais, e assim poderia até mesmo se prestar ao afastamento da matéria do âmbito dos direitos da personalidade. Outro problema é que esta leitura pode induzir à impressão de que as pessoas teriam um direito de propriedade sobre suas informações, transportando esta fenomenologia para o campo das situações patrimoniais. Tais problemas, por mais que sejam objetáveis, acabaram por constituir um embargo para uma disseminação mais ampla do direito à autodeterminação informativa.

O trecho aborda o conceito e a importância do direito à autodeterminação informativa na proteção de dados pessoais, tanto na Alemanha quanto no contexto da LGPD. Doneda destaca que esse direito, concebido como um direito fundamental, proporciona ao indivíduo o controle sobre suas informações, influenciando significativamente o desenvolvimento da disciplina da proteção de dados em países com sistemas jurídicos romano-germânicos, como o Brasil.

No entanto, também levanta críticas em relação aos pressupostos subjacentes ao direito à autodeterminação informativa, especialmente à sua interpretação e aplicação em um contexto tecnológico e jurídico em constante evolução. Um crítica diz respeito à própria definição de autodeterminação, destacando a dualidade entre uma interpretação que enfatiza o

controle das informações pelo indivíduo em um contexto de ampla informação e solidariedade, e outra que se concentra no consentimento individual para o tratamento de dados pessoais, assumindo conotações mais negociais e potencialmente afastando a proteção dentro do escopo dos direitos da personalidade.

Além disso, o autor alerta para o risco de interpretações equivocadas do direito à autodeterminação informativa, que poderiam conduzir à ideia de propriedade das informações pessoais pelo indivíduo, introduzindo conceitos patrimoniais inadequados no campo da proteção de dados. Essas críticas levantadas por Doneda apontam para desafios significativos na interpretação e aplicação do direito à autodeterminação informativa, destacando a necessidade de uma abordagem cuidadosa e contextualizada para garantir sua eficácia e coerência no contexto da proteção de dados pessoais.

Para além, é importante ater-se que a LGPD não incidirá no tratamento de dados pessoais quando este for efetuado por pessoa natural com finalidade exclusivamente particulares e não econômicas, bem como, não incide sobre tratamento realizados com finalidade exclusivamente jornalística; artística; de segurança pública; de defesa nacional; de segurança do Estado; de atividades de investigação e repressão de infrações e repressão de infrações penais; e acadêmica.

Importante ressalvar que no caso do tratamento para fins acadêmicos, aplicam-se os artigos 7º e 11 da LGPD, que elencam, respectivamente, as hipóteses em que o tratamento de dados pessoais e o tratamento de dados pessoais sensíveis podem ser realizados. Tendo em vista que o campo de pesquisa deste trabalho acadêmico é a UFRRJ, e esta será efetuada sobre a adequação do tratamento dos dados pessoais dos estudantes à luz da LGPD, será importante ater-se a questões relacionadas às atividades acadêmicas, com o objetivo de compreender quando de fato não ocorrerá a incidência da legislação.

2.2.2. Princípios

A LGPD primou por configurar em seu texto que a boa fé deverá ser observada quando realizada a atividade de tratamento de dados pessoais, desta maneira, os agentes de tratamento devem agir mediante um padrão ético de conduta, devendo observar ainda os princípios que orientam o tratamento de dados pessoais, pois estes são um norteador para o ordenamento jurídico brasileiro e para os formuladores de política pública de proteção de dados pessoais.

Destarte, os princípios que regem a LGPD encontram-se elencados no artigo 6º, e são de extrema importancia para resguardar o cumprimento da lei, cabendo enumerá-los: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. Assim, com base na investigação proposta neste trabalho acadêmico, é fundamental a compreensão destes dez princípios que a atividade de tratamento de dados pessoais deve se pautar.

A partir desta análise será possível perceber que os princípios presentes na LGPD abrangem os principais comportamentos que devem ser adotados pela sociedade para que hábitos culturais sejam modificados quanto a condutas relacionadas aos dados pessoais. Isto porque culturalmente, no Brasil, o indivíduo não possui um senso de pertencimento quanto aos seus dados pessoais, não discernindo a importância de resguardá-los.

Mesmo com a entrada em vigor da LGPD, muitos são os direitos dos titulares que permanecem sendo violados e os indivíduos que sofrem estas violações sequer tem conhecimento que há uma legislação vigente para protegê-los, e por vezes, bastaria a esses indivíduos conhecer os princípios norteadores da proteção de dados pessoais para entenderem as condutas inadequadas dos agentes de tratamento, podendo ainda coibi-las através do exercício dos seus direitos.

Nesta perspectiva, será efetuada uma análise dos princípios contidos na normativa com uma visão integrativa com a mesma e com o objeto de estudo, ou seja, serão analisados os princípios com menção a LGPD, bem como, tratando da importância dos mesmos dentro do contexto da pesquisa desenvolvida.

Por conseguinte, é importante rememorar que, este trabalho acadêmico aponta como problema a adequação da UFRRJ à política pública de proteção de dados pessoais à luz da LGPD, surgindo a seguinte questão central: quais as providências foram ou estão sendo tomadas para que ocorra a devida adequação às exigências legais e a prevenção dos riscos inerentes? Logo, tendo como ponto norteador este questionamento, bem como, ponderando que a pesquisa tem como recorte os dados pessoais dos estudantes, cabe iniciar a análise dos princípios que regem o tratamento dos dados pessoais.

Isto posto, como mencionado anteriormente, os dez princípios que regem a LGPD estão arrolados nos incisos do artigo 6º da Lei nº 13.709/2018, desta forma, o princípio abarcado pelo inciso I é o da *finalidade*, este consiste na "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

Deste modo, o tratamento de dados pessoais deverá ser bem definido e de conhecimento do titular, devendo ser eliminada a habitual prática exercida pelos controladores e operadores dos dados pessoais de utilizar os dados coletados para uma finalidade específica em outras atividades sem o consentimento do titular, a título exemplificativo, seria a UFRRJ solicitar o e-mail do estudante para comunicação de sua grade de disciplinas, porém compartilhar este e-mail com instituições parceiras para divulgação de propagandas diversas sem o consentimento do titular.

Quando a legislação aborda os requisitos para o tratamento de dados pessoais é possível verificar de forma mais consistente a importância do princípio da finalidade, desta forma, cabe pontuar que o consentimento do titular de dados deve referir-se a finalidades determinadas, pois quando autorizações genéricas são concedidas para tratar dados pessoais, estas são nulas.

Ressalta-se, porém, que é possível ocorrer mudança da finalidade que não seja compatível com o consentimento génese efetuado pelo titular para o tratamento dos dados pessoais, entretanto, o controlador deve informar previamente ao titular dos dados sobre as mudanças de finalidade, podendo este revogar o consentimento em caso de discordância quanto às alterações.

Ainda no que tange aos requisitos de tratamento de dados pessoais, a legislação menciona outras duas hipóteses em que o tratamento dos dados pessoais feito posteriormente pode ser efetuado para novas finalidades, porém, para que isto possa ocorrer devem ser observados os propósitos legítimos e específicos para este novo tratamento, bem como, a preservação do direito do titular, sendo resguardado os fundamentos e os princípios da LGPD.

A primeira hipótese é o tratamento de dados pessoais de acesso público, este precipuamente já deve considerar a finalidade, a boa-fé e o interesse público que justifiquem a disponibilização. A segunda hipótese são os dados tornados públicos pelo titular, é importante atentar-se que mesmo estes dados estando públicos, os direitos do titular são resguardados, sendo somente dispensada a exigência do consentimento.

Quando verifica-se que a finalidade do tratamento foi alcançada, ou que os dados pessoais não são mais necessários ou pertinentes para alcançar a finalidade específica esperada, ocorrerá o término do tratamento desses dados pessoais, devendo ocorrer a sua eliminação. A título de esclarecimento, o término do tratamento também poderá ocorrer com o fim do período de tratamento; com a revogação do consentimento ou ainda por determinação da ANPD.

Ato contínuo, no inciso II a LGPD trás o princípio da *adequação* que consiste na "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Há uma sintonia entre a adequação e a finalidade, vez que o controlador tem o dever de efetuar o tratamento dos dados de forma adequada às finalidades para as quais estes foram colhidos.

Nesta mesma vertente, o legislador imprimiu o princípio da *necessidade*, com previsão legal no inciso III, sendo este, segundo a lei, a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". É imperioso que o controlador e o operador detenham-se a coleta dos dados estritamente necessários para alcançar a finalidade proposta.

Os três princípios expostos alcançam uma completude, e apresentam uma primordialidade quanto a mudança das práticas de tratamento no que concerne aos dados pessoais, pode-se inferir que trata-se de uma mudança de cultura, como ressaltado anteriormente, pois os indivíduos estão habituados a não se considerarem titulares de seus próprios dados. Porém, a legislação evidencia que titular é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento", portanto, os controladores e operadores de dados pessoais devem refutar-se do hábito de tratar os dados pessoais como se fossem proprietários dessas informações.

Com foco nos princípios da finalidade, adequação e necessidade é possível verificar que a legislação impõe um limite no que tange ao tratamento dos dados pessoais, de forma que os agentes de tratamento não podem mais dispor dos dados sem que seja almejando uma finalidade específica e informada, devendo realizar a coleta somente das informações imprescindíveis para se alcançar a finalidade pretendida, mantendo o tratamento dos dados dentro do contexto informado ao titular.

A lei estabelece um conjunto de diretrizes e hipóteses que permitem o tratamento de dados pessoais, visando garantir a proteção e a segurança das informações dos cidadãos. Essas hipóteses foram delineadas com o objetivo de equilibrar os interesses dos titulares dos dados com as necessidades legítimas das organizações que os utilizam.

Primeiramente, o tratamento dos dados pessoais é permitido mediante o consentimento do titular, garantindo que a pessoa tenha controle sobre o uso de suas informações. Além disso, a legislação prevê situações em que o tratamento é necessário para o cumprimento de obrigações legais ou regulatórias por parte do controlador, bem como para

a execução de políticas públicas pela administração pública, desde que respaldadas por leis ou regulamentos.

Outras hipóteses incluem o tratamento de dados para a realização de estudos por órgãos de pesquisa, desde que seja garantida a anonimização dos dados pessoais, e para a execução de contratos ou procedimentos preliminares relacionados a contratos em que o titular seja parte. Além disso, o tratamento é permitido para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais, e para a proteção da vida, da saúde e do crédito do titular ou de terceiros.

No caso de dados pessoais sensíveis, como informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, entre outros, o tratamento só é permitido com consentimento específico e destacado do titular ou seu responsável legal. Na ausência de consentimento, o tratamento é autorizado apenas em situações excepcionais, como o cumprimento de obrigações legais, a realização de estudos por órgãos de pesquisa ou a proteção da vida e da saúde do titular ou de terceiros.

É importante ressaltar que, em todas as hipóteses de tratamento de dados pessoais, a LGPD estabelece requisitos específicos de segurança e transparência, visando garantir a privacidade e a proteção das informações dos cidadãos, conforme previsto nos artigos 9º e 10 da legislação.

O IV do artigo 6º da LGPD contempla um princípio que assegura de forma ainda mais direta um dos direitos do titular do dado, sendo este o *livre acesso*, assim, o mesmo é a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais".

Deste modo, a legislação garante que o acesso facilitado às informações sobre o tratamento de seus dados é um direito que o titular possui. Essas informações devem ser disponibilizadas de maneira clara, adequada e ostensiva para que o princípio do livre acesso seja atendido. A LGPD enumera as informações que devem ser disponibilizadas, cabendo destacá-las: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; direitos do titular.

O princípio da *qualidade dos dados* previsto no inciso V, também é garantidor de um direito do titular do dado, sendo este a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de

seu tratamento". A qualidade dos dados é um princípio que resguarda o titular dos dados, cabendo destacar que a correção de dados incompletos, inexatos ou desatualizados é um direito do titular elencado taxativamente pela legislação.

O inciso VI prossegue com mais um princípio que garante um direito do titular dos dados, sendo este o da *transparência*, assim, este é definido como a " garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Desta forma, os agentes de tratamento devem facilitar que o titular dos dados tenha acesso de forma facilitada e esclarecida sobre seus dados pessoais, sendo vedado qualquer tipo de cobrança para que estas informações sejam prestadas.

A lei resguarda que quando o consentimento é requerido ao titular, as informações devem ser apresentadas a este previamente e com transparência, de maneira clara e inequívoca, sem nenhum conteúdo enganoso ou abusivo, sob pena de ser considerado nulo. A legislação também explicita que os dados pessoais tratados por legítimo interesse do controlador, além de somente poder fundamentar-se em tratamento de dados pessoais para finalidades legítimas, com base em situações concretas, deve adotar medidas que garantam a transparência do tratamento dos dados que estão sendo baseados nesse legítimo interesse.

À vista disto, os princípios do livre acesso, qualidade dos dados e transparência formam uma tríade em resguardar de forma mais concreta os direitos dos titulares dos dados, como é possível perceber, até por suas definições, os mesmos tem a finalidade de garantir ao titular o acesso que lhe é devido as suas informações, de forma transparente e sempre sendo resguardada a qualidade dos dados.

Dentro do contexto desta pesquisa acadêmica, é fundamental que a UFRRJ proporcione aos seus estudantes acesso facilitado aos seus dados pessoais, de forma transparente e mantendo a qualidade desses dados, o que é objeto da presente investigação e será desenvolvido na seção 4 desta dissertação.

O inciso VII contextualiza que o princípio da *segurança* é a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" . Em contrapartida o princípio da *prevenção*, constante do inciso VIII, consiste na "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

Neste sentido, a legislação se preocupou em apontar orientações relativas aos princípios da segurança e da prevenção. De acordo com a estrutura e o volume das operações,

e ainda com a sensibilidade dos dados tratados, a probabilidade e a gravidade dos danos que podem ser causados aos titulares dos dados, o controlador pode implementar programa de governança em privacidade. Para tanto, é necessário que o programa demonstre o comprometimento do controlador em adotar políticas e processos internos que garantam a conformidade com as normas e boas práticas de proteção de dados pessoais. Além disso, deve abranger todos os dados pessoais sob sua responsabilidade, independentemente do método de coleta, sendo adaptado às características específicas da organização, incluindo sua estrutura, escala e sensibilidade dos dados tratados.

Ademais, o programa deve estabelecer políticas e salvaguardas adequadas com base em uma avaliação sistemática dos impactos e riscos à privacidade, visando construir uma relação de confiança com os titulares dos dados através de uma atuação transparente e oferecendo mecanismos de participação para estes. Deve também ser integrado à estrutura geral de governança da organização e contar com mecanismos de supervisão tanto internos quanto externos. Adicionalmente, é fundamental que o programa inclua planos de resposta a incidentes e medidas de remediação, e que seja atualizado regularmente com base em informações obtidas por meio de monitoramento contínuo e avaliações periódicas. Esses requisitos garantem que o programa de governança em privacidade seja eficaz e capaz de promover a proteção adequada dos dados pessoais sob responsabilidade da organização.

A LGPD também contempla no inciso IX a *não discriminação*, que consiste na "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Em sua essência, o princípio da não discriminação estabelece uma salvaguarda fundamental para proteger os titulares de dados contra práticas discriminatórias injustas ou prejudiciais que possam surgir a partir do tratamento de suas informações pessoais.

Busca garantir que as organizações e entidades responsáveis pelo tratamento de dados não utilizem essas informações para tomar decisões ou praticar ações que resultem em tratamento desigual, injusto ou prejudicial aos titulares dos dados. Isso abrange uma variedade de contextos, incluindo, mas não se limitando a, processos de seleção de emprego, concessão de crédito, acesso a serviços e benefícios, e quaisquer outras áreas em que o tratamento de dados possa influenciar a tomada de decisões que afetam os indivíduos.

Assim, o princípio da não discriminação na LGPD ressalta a importância de promover um ambiente de tratamento de dados justo, equitativo e respeitoso dos direitos individuais, reforçando os fundamentos éticos e sociais subjacentes à proteção de dados pessoais. Sua inclusão reflete o compromisso em garantir que o tratamento de dados seja realizado de forma

ética, transparente e em consonância com os princípios democráticos e os direitos fundamentais dos cidadãos.

Dentro do arcabouço normativo da LGPD o inciso X dispõe sobre o princípio da *responsabilização e prestação de contas*, que significa a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." Isto implica que os agentes de tratamento de dados devem ser capazes de comprovar, tanto interna quanto externamente, que adotaram medidas adequadas e proporcionais para garantir a proteção dos dados pessoais sob sua responsabilidade. Inclui não apenas a implementação de políticas e procedimentos, mas também a adoção de mecanismos de monitoramento, avaliação e aprimoramento contínuo das práticas de proteção de dados.

A obrigação de prestação de contas acarreta, portanto, em uma postura proativa por parte dos agentes de tratamento de dados, que devem estar aptos a demonstrar não apenas a conformidade com as normas legais e regulatórias, mas também a eficácia real das medidas adotadas na proteção dos dados pessoais. Isso envolve a documentação adequada das práticas de tratamento de dados, a realização de auditorias e avaliações periódicas, bem como a pronta resposta a incidentes e violações de segurança que possam ocorrer.

Em suma, este princípio visa promover uma cultura de transparência, responsabilidade e confiança no tratamento de dados pessoais, assegurando que os agentes de tratamento de dados assumam a responsabilidade integral pela proteção dos dados sob sua guarda e estejam prontos para prestar contas por suas ações perante as autoridades competentes e os titulares dos dados.

2.2.3. O Tratamento de Dados Pessoais pelo Poder Público

Tendo em vista que o campo de estudo deste trabalho acadêmico é a UFRRJ, uma autarquia federal, é imperioso abordar o tratamento de dados pessoais pelo poder público à luz da LGPD. Quando a legislação refere-se ao poder público está abarcando as seguintes pessoas jurídicas de direito público: os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Entretanto, buscando delimitar este tópico ao objeto da pesquisa será abordado as normas que possuem aplicabilidade direta às autarquias ou que contemplam de forma geral todo o Poder Público, não adentrando a peculiaridades de outros órgãos ou entidades públicas, como por exemplo, empresas públicas e sociedades de economia mista.

Destaca-se que a ANPD publicou em 28 de janeiro de 2022 a versão 1.0 do guia orientativo de tratamento de dados pessoais pelo Poder Público. Deste modo, o guia está inserido na competência orientativa que a lei lhe confere, cabendo citar o objetivo nas palavras da Autoridade (ANPD, 2022):

> o objetivo do Guia é auxiliar no desafio de estabelecer parâmetros objetivos, capazes de conferir segurança jurídica às operações com dados pessoais realizadas por órgãos e entidades públicas. Trata-se de assegurar a celeridade e a eficiência necessárias à execução de políticas públicas e à prestação de serviços públicos com respeito aos direitos à proteção de dados pessoais e à privacidade.

Como destacado pela ANPD, a adequação e a implementação da LGPD é um desafio para o Poder Público, porém este desafio pode ser superado se houver estratégias. Desta forma, o guia determina parâmetros objetivos com a finalidade de trazer segurança jurídica para o tratamento dos dados pessoais, o que é fundamental, vez que o objetivo da legislação não é impedir o tratamento dos dados, mas sim conferir segurança ao titular dos dados.

Os órgãos e entidades públicas necessitam dos dados pessoais para cumprirem com sua finalidade pública, é fundamental que sejam diligentes, devendo estabelecer regras de boas práticas e de governança, como será abordado na seção 3 deste trabalho acadêmico. Bem como, devem realizar o tratamento de dados pessoais na persecução do interesse público, tendo como objetivo executar as competências legais ou ainda cumprir as atribuições legais do serviço público.

O Poder Público deve ainda no exercício de suas competências informar as hipóteses em que efetuam o tratamento de dados pessoais, devendo fornecer informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas que utilizam para executar essas atividades.

Consequentemente, essas informações devem ser prestadas em veículos de fácil acesso, de preferência nos endereços eletrônicos dos órgãos ou das entidades públicas, podendo a ANPD deliberar sobre outras maneiras de publicidade das operações de tratamento. De modo que o fundamental é que o Poder Público dê transparência e publicidade a todas as informações exigidas pela LGPD.

Cabe ainda mencionar que em 26 de junho de 2023 foi publicado pela ANPD o Guia

orientativo “Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas”, destaca a autoridade que (ANPD, 2023):

> A Lei Geral de Proteção de Dados Pessoais estabelece regras específicas para o tratamento de dados pessoais que tenham finalidade acadêmica, e o Guia pretende esclarecer dúvidas sobre as hipóteses legais que autorizam o tratamento de dados pessoais e a disponibilização de acesso ou compartilhamento de dados pessoais para a realização de estudos e pesquisas, por exemplo. Além disso, o Guia traz exemplos práticos como o uso compartilhado de dados entre Secretarias de Saúde e órgãos de pesquisa, o tratamento de dados pessoais realizados por instituições de ensino, casos de uso de dados pessoais por centros de pesquisas criados pelo Ministério Público em estados da federação, entre outros. (...) O Guia vem para reforçar a necessidade de o agente de tratamento seguir padrões éticos e o princípio da boa-fé, previstos na LGPD, como um meio de realizar o tratamento de dados pessoais com finalidade acadêmica, de estudo e pesquisa pautado pela transparência, correção e lealdade, buscando sempre proteger a confiança e as expectativas do titular de dados pessoais.

Verifica-se que a autoridade enfatiza a necessidade do controlador e do operador pautarem o tratamento de dados pessoais com finalidade acadêmica em padrões éticos e no princípio da boa fé, bem como, na transparência, correção e lealdade, visando a proteção da confiança e as expectativas do titular, de forma que as orientações do referido guia é imprescindível no que tange a adequação da UFRRJ.

Para além, quando efetuar operações de tratamento de dados pessoais, o poder público deve indicar um encarregado pelo tratamento de dados pessoais. Esta indicação deve ser realizada pelo controlador, neste caso, pelo órgão ou entidade pública, que deverá divulgar publicamente, de maneira clara e objetiva, a identidade e as informações de contato deste encarregado. A legislação informa que essa divulgação pode ser realizada preferencialmente no endereço eletrônico do controlador.

Deste modo, pontua-se que o encarregado tem como atribuições: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da ANPD e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Cumpre enfatizar que a ANPD pode editar normas complementares quanto à definição e as atribuições do encarregado, abordando ainda hipóteses de dispensa de indicação de encarregado de acordo com a natureza e o porte da entidade, ou ainda de acordo com o volume de operação de tratamento de dados.

O exercício dos direitos do titular face ao Poder Público devem observar o

regulamento de legislações específicas no que tange aos prazos e procedimentos, neste sentido, a LGPD dá ênfase a Lei nº 9.507/1997 que regulamenta o Habeas Data, a Lei nº 9.784/ 1999 do Processo Administrativo, e a Lei nº 12.527/2011 sobre o Acesso à Informação. Destaca-se que se um órgão ou entidade pública negar-se a fornecer informação ou retificar dado pessoal do titular desses dados, o mesmo pode efetuar denúncia à ANPD, bem como, permanece resguardado pelo remédio constitucional do Habeas Data, previsto no artigo 5º inciso LXXII da CRFB/88.

É importante atentar-se que o Poder Público deve manter os dados pessoais em formato interoperável, ou seja, de maneira capaz de operar, funcionar ou atuar com outros dados, bem como estruturado para o uso compartilhado, visando a execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública, à disseminação e ainda o acesso das informações pelo público em geral, vez que este é um mecanismo relevante para a execução de atividades típicas dos órgãos e entidades públicas.

Ressalta-se que o Poder Público quando efetua o uso compartilhado dos dados pessoais deve estar atento as finalidades específicas de execução de políticas públicas e atribuição legal exercidas pelos órgãos e pelas entidades públicas, respeitando os princípios da finalidade; da adequação; da necessidade; do livre acesso; da qualidade dos dados; da transparência; da segurança; da prevenção; da não discriminação; da responsabilização e prestação de contas.

Cabe destacar quanto ao compartilhamento que o Poder Público não pode transferir dados pessoais constantes de bases de dados a que tenha acesso a entidades privadas, salvo no caso das exceções previstas na legislação, devendo ser informado à ANPD.

Assim, diante das exigências legais apresentadas é possível compreender que o Poder Público tem um desafio a ser enfrentado, sob pena de sofrer as sanções previstas na LGPD, pois somente não se aplica a este as pecuniárias, de forma que o mesmo pode ser sancionado administrativamente pela ANPD, após procedimento administrativo que possibilite a oportunidade da ampla defesa.

Dentre as sanções previstas pela LGPD, destacam-se algumas medidas que podem ser aplicadas em caso de infração às normas de proteção de dados. Estas incluem advertência, na qual o infrator é notificado e recebe um prazo para corrigir as irregularidades identificadas. Além disso, a infração pode ser publicizada após uma investigação adequada, destacando-se a natureza e a gravidade do ocorrido.

Outra medida que pode ser adotada é o bloqueio dos dados pessoais envolvidos na

infração até que a situação seja regularizada. Em casos mais graves, a eliminação dos dados relacionados à infração pode ser determinada. Em situações em que a gravidade da infração exige medidas mais severas, como a suspensão parcial ou total do funcionamento do banco de dados envolvido na infração por um período determinado, com possibilidade de prorrogação até que a situação seja regularizada pelo controlador. Ademais, a suspensão do exercício da atividade de tratamento de dados pode ser aplicada pelo mesmo período, com a mesma possibilidade de prorrogação.

Em casos extremos, a LGPD prevê a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados. Estas sanções visam assegurar a conformidade com as normas de proteção de dados e garantir a segurança e a privacidade dos titulares das informações, além de promover uma cultura de responsabilidade e *accountability* no tratamento de dados pessoais.

Isto posto, é imperioso resguardar a Universidade Federal Rural do Rio de Janeiro de qualquer tratamento de dados pessoais realizado de forma inadequada, e para que seja possível realizar a adequação e implementação das exigências legais, é fundamental que sejam adotadas as boas práticas e a governança no âmbito desta entidade pública de ensino, para garantir a promoção eficaz, eficiente e efetiva da análise e gestão de risco, é o que será compreendido na seção 3.

3. DA IMPLEMENTAÇÃO DAS BOAS PRÁTICAS E GOVERNANÇA

A adoção de regras de boas práticas no contexto da proteção de dados é de suma importância, especialmente em um cenário onde a gestão responsável e ética das informações pessoais tornaram-se cruciais. Estas regras constituem um conjunto de diretrizes e procedimentos que visam estabelecer padrões elevados de conduta no tratamento de dados, promovendo não apenas a conformidade legal, mas também a preservação dos direitos individuais e a construção da confiança entre as entidades e órgãos públicos e os titulares dos dados.

A implementação da política pública de proteção de dados revela-se consideravelmente mais eficaz mediante a adoção de regras de boas práticas e governança. A incorporação dessas diretrizes proporciona uma estrutura organizacional sólida, estabelecendo padrões e procedimentos que visam assegurar a integridade, confidencialidade e disponibilidade dos dados pessoais. A governança, nesse contexto, não apenas fortalece a conformidade com os requisitos legais, como os delineados na LGPD, mas também promove a criação de uma cultura organizacional voltada para a proteção e respeito aos direitos individuais.

Ao adotar regras de boas práticas e governança, os controladores e operadores se capacitam para uma gestão mais eficiente e ética do tratamento de dados pessoais. Essas regras podem abranger desde a definição de responsabilidades internas até a implementação de medidas técnicas e organizacionais que garantam a segurança e privacidade dos dados. Além disso, a governança atua como um mecanismo de autorregulação, permitindo a adaptação contínua às evoluções tecnológicas, mudanças na legislação e às dinâmicas do ambiente operacional.

A ênfase na governança em privacidade, como proposta no texto legal, reflete não apenas o comprometimento com a conformidade legal, mas também a busca por melhores práticas que vão além do simples atendimento às exigências normativas. Ao considerar a natureza, escopo, finalidade e riscos associados ao tratamento de dados pessoais, as regras de governança estabelecem um arcabouço que visa equilibrar os interesses legítimos das organizações com os direitos fundamentais dos titulares dos dados.

Dessa forma, a implementação eficaz das políticas públicas de proteção de dados torna-se intrinsecamente ligada à presença de uma governança robusta. Essa abordagem

não apenas confere maior segurança jurídica às organizações, mas também promove a confiança dos titulares dos dados e contribui para a construção de um ambiente digital mais ético e transparente.

3.1 - Das boas práticas e governança no Poder Público: a importância da implementação na política pública de proteção de dados

Governança pública é um conceito multifacetado que desempenha um papel crucial na eficácia do governo e na promoção do bem-estar social, assim, no poder público é de extrema importância para o bom funcionamento e desenvolvimento de uma sociedade democrática. Ela se refere aos processos, práticas e estruturas que são utilizados para tomar decisões, implementar políticas públicas, gerenciar recursos e promover a transparência, responsabilidade e eficácia na administração do Estado.

Deste modo, a implementação da política pública de proteção de dados é notavelmente aprimorada com a adoção de regras de boas práticas e governança. Ao incorporar essas diretrizes, estabelece-se uma estrutura organizacional sólida, definindo padrões e procedimentos para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais. Assim, é fundamental uma análise sobre governança no poder público para melhor desenvolvimento do tema, cabendo citar a visão de Leo Kissler e Francisco G. Heidemann (2006) para apresentar uma reflexão do que vem a ser governança pública:

> Após uma década de "modernização do setor público" na Alemanha, é hora de se fazer um balanço sobre a experiência. E constata-se que as administrações públicas se tornaram mais empresariais, menos onerosas e, em geral, mais eficientes; raramente, porém, mais simpáticas aos cidadãos. Em outras palavras, as fronteiras — entre os órgãos públicos e os cidadãos, entre os setores público e privado — de fato receberam novos contornos, com base na privatização e na terceirização; mas as novas bases não se revelaram favoráveis aos cidadãos. A modernização do Estado que ocorreu nos últimos 10 anos foi, principalmente, uma reforma interna inspirada na administração pública gerencial (new public management). Pautando-se por este modelo ideológico, o Estado voltado para o mercado e para a gestão na prática provocou sobretudo uma redução dos postos de trabalho na administração pública. Deve-se às condições insatisfatórias da modernização praticada até agora o surgimento e atratividade de um novo modelo: a governança pública (public governance). Até que ponto trata-se de um novo conceito para regular as relações de troca entre os setores público e privado, entre Estado, mercado e sociedade? É particularmente desafiador responder em termos científicos a essa pergunta. O entendimento que se tem sobre governança pública não é muito claro; Max Weber diria tratar-se de um conceito sociologicamente "amorfo". Não existe um conceito único de governança pública, mas antes

> uma série de diferentes pontos de partida para uma nova estruturação das relações entre o Estado e suas instituições nos níveis federal, estadual e municipal, por um lado, e as organizações privadas, com e sem fins lucrativos, bem como os atores da sociedade civil (coletivos e individuais), por outro.

O trecho apresentado destaca a experiência alemã de modernização do setor público e como isso influenciou a evolução do conceito de governança pública. Os autores mencionam que, após uma década de modernização, as administrações públicas na Alemanha se tornaram mais empresariais e eficientes, mas nem sempre mais simpáticas aos cidadãos. Isso é um indicativo de que a modernização, baseada no modelo de administração pública gerencial (*new public management*), teve êxito na eficiência, mas pode ter negligenciado aspectos relacionados à satisfação e ao envolvimento dos cidadãos.

Ressaltam a transição para a governança pública como um novo modelo regulatório que busca uma abordagem mais colaborativa e inclusiva, envolvendo não apenas o Estado e o mercado, mas também a sociedade civil. Eles reconhecem que o conceito de governança pública é multifacetado e ainda carece de uma definição clara, o que é um desafio para a sua aplicação prática.

No contexto brasileiro, pode-se fazer um paralelo com a Alemanha na experiência de modernização do setor público e a busca por uma governança pública mais eficaz. O Brasil também passou por transformações na administração pública, buscando aprimorar a eficiência e a gestão dos recursos públicos. No entanto, assim como na Alemanha, o desafio da governança pública no Brasil envolve aspectos como a transparência, a participação cidadã e a prestação de contas, de forma que o Decreto nº 9.203/2017 vem estabelecer a Política Pública de Governança da Administração Pública Federal.

3.1.1 - Do Decreto nº 9.203/2017: Princípios, *Accountability* e Diretrizes

A governança pública no Brasil pode ser vista como um esforço para superar as limitações, priorizando não apenas a eficiência, mas também a inclusão e a responsabilidade. O desafio é estabelecer um equilíbrio entre a eficiência na prestação de serviços públicos e a promoção da participação democrática, garantindo que o Estado seja capaz de atender às expectativas dos cidadãos de forma eficaz e responsável.

O *enforcement* das normas é vital para o funcionamento eficaz da sociedade e de suas instituições, conforme destacado por Almir Lima Nascimento (2022) no artigo Instrumentos Jurídicos de Governança e Implementação de Dispositivos da Legislação Brasileira. O autor salienta que a elaboração de dispositivos legais pelo legislador não se limita à sua aprovação no âmbito legislativo; é crucial considerar a simplicidade e direção no cumprimento da norma, tanto por parte dos responsáveis por sua aplicação quanto pela sociedade em geral. Nascimento enfatiza a importância de indicar claramente, no texto legal, os "degraus" que devem ser seguidos para a plena execução da norma.

O autor exemplifica a efetividade das normas por meio de dois instrumentos: a Instrução Normativa Conjunta (INC) MP-CGU nº 1, de 10 de maio de 2016, e o Decreto n° 9.203, de 22 de novembro de 2017, conhecido como Decreto de Governança. Ambos contribuem para a transformação da gestão pública no Brasil, promovendo a governança, a gestão de riscos e os controles internos. O Decreto, em particular, aborda a governança em termos de sua definição, elementos constituintes e responsabilidades na Administração Pública Federal.

Nascimento destaca a importância do gerencialismo na modernização da gestão pública, exemplificado por esses instrumentos legais. Ele menciona que a INC nº 1/2016 e o Decreto nº 9.203/2017 têm uma essência deliberativa e pedagógica, fornecendo orientação aos gestores e familiarizando os cidadãos com os conceitos modernos de gestão pública. Além disso, esses instrumentos são vistos como meios adequados para implementar dispositivos legais, contribuindo para uma administração pública mais eficiente, eficaz e efetiva. O autor ressalta que a aplicação desses instrumentos já trouxe um novo significado à implementação de normas legais, destacando a importância de ferramentas e metodologias gerenciais alinhadas à nova gestão pública.

Resumidamente, destaca-se que a Instrução Normativa Conjunta nº 1, de 10 de maio de 2016, estabelece diretrizes fundamentais no contexto da gestão pública federal, especificamente no que se refere a controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. De acordo com o disposto no artigo 1º, os órgãos e entidades que compõem o Poder Executivo federal estão obrigados a tomar medidas para sistematizar práticas relacionadas à gestão de riscos, aos controles internos e à governança. Essa iniciativa visa aprimorar e fortalecer os processos e estruturas de

gestão, garantindo maior eficácia, eficiência e transparência nas atividades desenvolvidas por essas instâncias governamentais.

A ênfase na gestão de riscos sugere a necessidade de identificar, avaliar, administrar e controlar potenciais eventos ou situações que possam impactar o alcance dos objetivos institucionais. Isso implica um comprometimento ativo em antecipar e lidar proativamente com fatores de incerteza que podem afetar o desempenho e a missão dos órgãos e entidades. A abordagem aos controles internos destaca a importância de estabelecer regras, procedimentos, diretrizes e protocolos integrados de forma eficaz. Esses controles visam assegurar a execução ordenada, ética, econômica e eficaz das operações, o cumprimento das obrigações de *accountability*, o atendimento às leis e regulamentos aplicáveis, além da salvaguarda dos recursos públicos.

Quanto à governança, a instrução normativa enfatiza a combinação de processos e estruturas implementadas pela alta administração para informar, dirigir, administrar e monitorar as atividades da organização. Isso visa alcançar os objetivos institucionais de maneira eficiente, transparente e alinhada aos interesses da sociedade. Dessa forma, a Instrução Normativa Conjunta nº 1 busca estabelecer um arcabouço normativo que promova uma cultura organizacional voltada para a excelência na gestão pública, baseada em princípios de responsabilidade, transparência, gestão de riscos e efetividade nas ações do Poder Executivo federal.

Porém, este trabalho acadêmico ater-se-á a análise dos princípios e diretrizes do Decreto nº 9.203/2017, publicado em 22 de novembro de 2017, que estabeleceu a Política de Governança da Administração Pública Federal Direta, Autárquica e Fundacional, que tem como objetivo promover a melhoria da gestão pública, aumentando a eficiência, a transparência e a responsabilidade na administração federal. Além disso, esta normativa buscou fortalecer a prestação de serviços públicos e a tomada de decisão baseada em evidências.

Esta legislação representa um esforço significativo para modernizar a gestão pública no Brasil, com foco na eficácia, na transparência e na *accountability* e define governança como o "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade".

Assim, no contexto do artigo 3º os princípios da Governança Pública representam a base para uma administração pública eficiente e ética, vez que

desempenham um papel central na orientação das práticas e políticas governamentais. Estes são os princípios, a saber: capacidade de resposta, integridade, confiabilidade, melhoria regulatória, prestação de contas, responsabilidade e transparência. Desta forma, examinar-se-á cada um desses e sua importância na governança pública.

O princípio da capacidade de resposta destaca a importância da agilidade e eficácia do governo na identificação e atendimento das necessidades da sociedade. A prontidão em fornecer serviços públicos de qualidade, tomar decisões informadas e lidar eficientemente com desafios e crises contribui diretamente para a satisfação dos cidadãos e para o alcance dos objetivos de políticas públicas. Em um contexto dinâmico, a capacidade de resposta governamental é crucial para garantir a eficiência na prestação de serviços e na adaptação a mudanças inesperadas.

O princípio da integridade destaca a necessidade de os agentes públicos atuarem com ética e probidade. Evitar conflitos de interesse, corrupção e comportamentos antiéticos é fundamental para promover a confiança da sociedade nas instituições governamentais. A integridade não apenas fortalece a legitimidade do Estado, mas também previne práticas danosas e assegura que as ações governamentais estejam alinhadas com os valores morais e éticos.

A confiabilidade, como princípio, ressalta a importância de fornecer serviços e informações governamentais de forma consistente e confiável. Essa consistência é crucial para estabelecer uma relação de confiança entre o governo e a sociedade. Garantir a precisão e a confiabilidade das ações governamentais ao longo do tempo contribui para a tomada de decisões informadas e promove a transparência, essencial para a *accountability* e avaliação do desempenho governamental.

O princípio da melhoria regulatória reconhece a importância de aprimorar a eficiência e eficácia da regulamentação governamental. Isso envolve a revisão e simplificação de regulamentos, redução de burocracia e promoção de práticas regulatórias que beneficiem a sociedade. A busca por equilíbrio entre a proteção dos interesses públicos e a facilitação da atividade econômica é essencial para garantir regulamentações proporcionais e eficientes.

A prestação de contas e responsabilidade, como princípios interligados, reforça a obrigação dos agentes públicos de prestar contas por suas ações. A divulgação de informações sobre atividades governamentais e a responsabilização perante os cidadãos

e órgãos de controle contribuem para a transparência e a legitimidade das ações governamentais.

Por fim, o princípio da transparência destaca a importância da abertura e acessibilidade das informações governamentais. Assegurar que as ações, decisões e informações do governo sejam acessíveis e claras para o público promove a *accountability*, participação cidadã e construção de uma administração pública mais eficiente e ética.

Em conjunto, esses princípios formam uma base sólida para a governança pública, orientando as práticas governamentais em direção a uma administração eficiente, ética, transparente e comprometida com o bem-estar da sociedade.

Ainda nesta vertente, quando discorre-se sobre o Decreto nº 9.203/2017 e seus princípios, é imperioso destacar a *accountability*, pois este é um termo que se refere à responsabilidade, transparência e prestação de contas de indivíduos, organizações ou instituições por suas ações e decisões. É um princípio fundamental em governança, gestão pública e em muitos outros campos. A *accountability* envolve a obrigação de prestar contas por ações ou decisões a partes interessadas, sejam elas o público em geral, partes interessadas diretas, órgãos reguladores, acionistas, entre outros. Assim destaca Fernando Filgueiras (2018, pg.88):

> Não há como precisar o momento em que o conceito de *accountability* foi utilizado pela primeira vez, mas é pertinente relacioná-lo ao surgimento dos Estados liberais e ao da moderna administração pública, tendo em vista a distinção entre a vida pública e a vida privada. O princípio da publicidade do Estado exige a criação de regras e procedimentos capazes de promover a responsabilização dos agentes públicos perante os cidadãos. *Accountability* tem origem anglo-saxã e denota uma ideia de responsabilidade política. Se traduzida para o português em um sentido literal, a melhor tradução da palavra é a ideia de prestação de contas. Dessa maneira, o conceito de *accountability* refere-se aos processos e procedimentos inerentes às modernas burocracias, tais como controle interno e externo, contabilidade pública e auditorias, mediante os quais se prestam contas ao público das políticas realizadas pelo Estado no sentido do bem comum. Contudo, mesmo em inglês, o uso da palavra *accountability* não está relacionado apenas aos processos formais de prestação de contas, mas, também, a processos políticos mais amplos, que envolvem desenhos institucionais e participação democrática na constituição de leis e de políticas públicas. Dessa forma, o termo *accountability* remete-nos, sobretudo, ao princípio da publicidade como valor democrático fundamental das burocracias públicas e do processo de formação, implementação e avaliação das políticas públicas.

O autor destaca a complexidade e a evolução do conceito de *accountability*, associando-o ao surgimento dos Estados liberais e à moderna administração pública.

Filgueiras ressalta a conexão intrínseca entre o conceito e a distinção entre a vida pública e privada, fundamentada nos princípios dos Estados liberais. O autor diz que a noção de *accountability* está enraizada na ideia de responsabilidade política, originada nos contextos anglo-saxões.

Ao explicar o termo *accountability,* Filgueiras aponta para sua tradução literal como "prestação de contas", destacando que o princípio da publicidade do Estado demanda a criação de regras e procedimentos para garantir que os agentes públicos sejam responsabilizados perante os cidadãos. A *accountability*, nesse sentido, está associada a processos e procedimentos presentes nas modernas burocracias, como controle interno e externo, contabilidade pública e auditorias, que visam prestar contas à sociedade sobre as políticas implementadas pelo Estado em prol do bem comum.

É interessante notar que, segundo o autor, a *accountability* transcende a simples prestação de contas formal, pois também está relacionada a processos políticos mais amplos. Esses processos envolvem desenhos institucionais e participação democrática na formação, implementação e avaliação de leis e políticas públicas. Dessa forma, o termo *accountability*, conforme apresentado pelo autor, está intrinsecamente ligado ao princípio da publicidade como um valor democrático fundamental das burocracias públicas e do processo mais amplo de formulação e execução de políticas públicas. A citação enfatiza a natureza abrangente e democrática do conceito, indo além das formalidades de prestação de contas para incorporar elementos fundamentais da participação cidadã e da transparência nas práticas governamentais.

Ainda nesta vertente, cabe salientar que a Instrução Normativa Conjunta nº 1/2026 traz a definição de *accountability* em seu artigo 2º, alínea I:

> Art. 2º Para fins desta Instrução Normativa, considera-se: I-*accountability*: conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas,incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;

Este artigo apresenta a definição do termo *accountability* que é caracterizado como o conjunto de procedimentos adotados por organizações públicas e pelos indivíduos que as compõem. Esses procedimentos têm o propósito de evidenciar a responsabilidade por decisões tomadas e ações implementadas. Ele destaca elementos essenciais que compõem a *accountability*, incluindo a salvaguarda de recursos públicos,

a imparcialidade e o desempenho das organizações. Isso implica que as entidades públicas e seus membros devem adotar práticas que evidenciem a responsabilidade na utilização de recursos, assegurando transparência, ética e eficiência nas decisões e ações.

A referência à salvaguarda de recursos públicos ressalta a importância de garantir que esses recursos sejam utilizados de maneira adequada e eficaz, evitando perdas, má administração e danos. Além disso, a imparcialidade destaca a necessidade de agir de forma justa e equitativa, sem favorecimentos ou discriminações, contribuindo para uma gestão pública mais transparente e confiável.

O desempenho das organizações, mencionado na citação, sugere que a *accountability* não se limita apenas à responsabilidade financeira, mas abrange a avaliação contínua do cumprimento de metas, objetivos e padrões éticos. Essa definição busca estabelecer um padrão de conduta que promova a responsabilidade e a integridade na administração pública, visando ao interesse público e ao bom uso dos recursos.

Desta maneira, pode-se dizer que *accountability* relaciona-se com a divulgação aberta e acessível de informações relevantes sobre ações, decisões e resultados. Quanto mais transparente for uma organização, mais fácil é avaliar sua conduta e tomar medidas adequadas, se necessário. Logo, as pessoas ou instituições são responsáveis por suas ações e decisões. Isso significa que podem ser chamados a prestar contas por qualquer comportamento que tenha consequências negativas ou que não esteja alinhado com normas, regulamentos ou expectativas.

Para a garantir, muitas vezes é necessária uma estrutura de controle e supervisão. Isso pode envolver órgãos reguladores, auditorias internas e externas, comitês de fiscalização e outras medidas destinadas a assegurar que as ações estejam em conformidade com as normas estabelecidas. Em casos de comportamento inadequado, as partes responsáveis podem enfrentar sanções legais, financeiras ou outras consequências, dependendo da gravidade da situação.

Assim, também está ligada à melhoria contínua, pois quando as organizações são responsáveis por suas ações, têm um incentivo para aprender com seus erros, corrigir problemas e aprimorar seus processos. Desta forma, a *accountability* desempenha um papel fundamental em várias esferas da sociedade, incluindo o setor público, o setor privado, organizações sem fins lucrativos e outros contextos. Ela é vista como um meio de promover a transparência, a confiança e a boa governança em todos

esses espaços, ajudando a garantir que as pessoas e instituições sejam responsáveis por suas ações e decisões perante a sociedade.

Para além, conforme delineadas no artigo 4º do Decreto nº 9.203/2017, as diretrizes da governança pública representam um conjunto de princípios e metas também essenciais para uma gestão pública eficiente e eficaz. Estas diretrizes estão enraizadas no propósito de melhorar a qualidade dos serviços públicos, promover a transparência, e assegurar que a administração governamental esteja alinhada com as necessidades da sociedade. Neste texto científico, explorar-se-á, a partir do próximo parágrafo, cada uma das diretrizes e sua relevância na governança pública contemporânea.

Direcionar ações para a busca de resultados para a sociedade, enfatiza a importância de que as ações governamentais sejam orientadas para a obtenção de resultados concretos que atendam às necessidades da sociedade. Isso inclui a busca por soluções inovadoras e tempestivas, mesmo em face de recursos limitados e mudanças de prioridades. Essa abordagem resulta em uma administração pública mais ágil e centrada no cidadão.

Promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, visa à melhoria da eficiência e eficácia da administração pública por meio da simplificação de processos, modernização de práticas e integração de serviços públicos, especialmente no contexto digital. Isso facilita o acesso dos cidadãos aos serviços governamentais e contribui para a desburocratização e a redução de custos.

Monitorar o desempenho e avaliar a concepção, implementação e resultados das políticas e ações prioritárias, a avaliação é fundamental para assegurar que as políticas e ações governamentais estejam alinhadas com as diretrizes estratégicas e produzam os resultados desejados. Essa diretriz promove a prestação de contas e a melhoria contínua das políticas públicas.

Articular instituições e coordenar processos para melhorar a integração entre os diferentes níveis e esferas do setor público, a coordenação entre órgãos e níveis de governo é essencial para evitar redundâncias e melhorar a eficiência. Essa diretriz visa à integração das diferentes esferas do setor público para a geração e preservação de valor público.

Fazer incorporar padrões elevados de conduta pela alta administração, enfatiza a importância de que a alta administração do governo atue como exemplo de conduta ética e profissional, orientando o comportamento dos agentes públicos e promovendo a integridade na gestão pública.

Implementar controles internos fundamentados na gestão de risco, a gestão de riscos é crucial para prevenir problemas antes que ocorram. Esta diretriz promove a prevenção de irregularidades por meio de ações estratégicas e responsabilização eficaz, em vez de confiar exclusivamente em processos sancionadores.

Avaliar propostas de criação, expansão ou aperfeiçoamento de políticas públicas, promove a avaliação cuidadosa das propostas de políticas públicas, incluindo a análise de custos e benefícios, para garantir a alocação eficiente dos recursos públicos.

Manter processo decisório orientado pelas evidências, a tomada de decisões baseada em evidências, conformidade legal, qualidade regulatória e desburocratização é essencial para garantir que as políticas públicas sejam bem fundamentadas e eficazes.

Editar e revisar atos normativos pautando-se pelas boas práticas regulatórias, busca aprimorar a qualidade das regulamentações governamentais, promovendo sua legitimidade, estabilidade e coerência. Consultas públicas são incentivadas para promover a participação da sociedade nas decisões regulatórias.

Definir formalmente as funções, competências e responsabilidades das estruturas institucionais, enfatiza a importância da clareza e da formalização das funções e responsabilidades das estruturas governamentais para evitar conflitos e garantir a eficácia da administração pública.

Promover a comunicação aberta, voluntária e transparente das atividades e resultados da organização, a comunicação transparente fortalece o acesso público à informação, promovendo a confiança e a *accountability.* Ela assegura que as atividades e resultados do governo sejam acessíveis e compreensíveis para a sociedade.

Deste modo, as diretrizes da governança pública estabelecidas no Decreto nº 9.203/2017 direcionam as ações do governo para promover o bem-estar da sociedade, melhorar a eficiência da gestão pública e fortalecer a confiança nas instituições governamentais. Ao seguir essas diretrizes, os governos podem melhorar a qualidade dos serviços públicos, otimizar o uso dos recursos e promover uma governança mais responsável e orientada para resultados.

Em síntese, o Decreto assume uma posição de destaque na governança pública brasileira ao estabelecer princípios, diretrizes e normas que guiam a atuação dos órgãos e entidades da administração pública federal. Sua importância é evidente em diversos aspectos. Como visto, ele consolida princípios essenciais da governança pública que servem como orientação para os gestores públicos, buscando promover uma administração mais eficiente, ética e transparente.

Além disso, a normativa em comento estabelece diretrizes específicas para orientar ações que visem resultados efetivos para a sociedade, incluindo a busca por soluções inovadoras diante de limitações de recursos e mudanças de prioridades, promovendo uma gestão mais orientada para o interesse público.

Destaca ainda a importância da simplificação administrativa, da modernização da gestão pública e da integração dos serviços públicos, especialmente os prestados eletronicamente, visando tornar a administração mais eficaz, acessível e alinhada com as demandas contemporâneas da sociedade.

O decreto salienta a necessidade de monitorar o desempenho e avaliar políticas e ações prioritárias para garantir o seguimento das diretrizes estratégicas. Além disso, ressalta a importância da transparência, promovendo a comunicação aberta e transparente das atividades e resultados da organização para fortalecer o acesso público à informação. Ao destacar a implementação de controles internos fundamentados na gestão de risco, busca privilegiar ações estratégicas de prevenção antes de processos sancionadores, contribuindo para uma gestão mais eficiente e prevenindo irregularidades.

Estabelece a necessidade de definir formalmente as funções, competências e responsabilidades das estruturas e dos arranjos institucionais, promovendo clareza na organização administrativa. Ressalta a importância de promover a comunicação aberta, voluntária e transparente das atividades e resultados da organização, fortalecendo o acesso público à informação.

Logo, o Decreto nº 9.203/2017 desempenha um papel crucial ao fornecer um arcabouço normativo que orienta a atuação da administração pública federal, promovendo princípios e diretrizes que visam uma gestão mais eficiente, ética e transparente, alinhada com as necessidades e expectativas da sociedade. Destacando a importância de editar e revisar atos normativos pautando-se por boas práticas

regulatórias, além da legitimidade, estabilidade e coerência do ordenamento jurídico. Foi o que buscou a LGPD ao incentivar a adoção de boas práticas e governança.

3.1.2 - Das Boas Práticas e Governança na LGPD

A LGPD demonstra um comprometimento claro com a efetividade de suas disposições ao incluir, no artigo 50, a importância da adoção de regras de boas práticas e governança. A incorporação desses elementos reflete o reconhecimento da complexidade do tratamento de dados pessoais e a compreensão de que a mera observância de normas legais não é suficiente para garantir a proteção adequada dos direitos individuais e a integridade das informações. Neste sentido cabe citar trecho do artigo a ANPD e a fiscalização da governança corporativa de proteção de dados (REYMÃO; OLIVEIRA; KOURY, 2023)

> A LGPD destinou uma seção inteira às regras de boas práticas e governança, que ocupam um lugar de destaque entre os artigos 46 a 51. Estas práticas se caracterizam como instrumentos de governança corporativa que visam estabelecer procedimentos que facilitem e viabilizem o cumprimento da legislação. Nesse sentido, a adoção destes mecanismos por parte dos agentes de tratamento de dados pessoais possui o condão de facilitar o processo e consolidá-lo. As políticas de governança propostas pela LGPD assemelham-se à modalidade de autorregulação da atividade empresarial. Entretanto, se diferenciam do modelo tradicional, posto que devem ser elaboradas e implementadas com base nas diretrizes estipuladas pela legislação, que exigem que estes programas reflitam efetivamente a estrutura, a escala e o volume das operações da empresa. Entende-se que, assim, os riscos de violação à privacidade dos indivíduos serão minimizados, com o tratamento das informações pessoais sempre pautado na segurança

As autoras destacam a relevância da seção dedicada às regras de boas práticas e governança na LGPD, ressaltando seu papel fundamental no cumprimento da legislação de proteção de dados pessoais. Ao comparar essas práticas com instrumentos de governança corporativa, ela enfatiza a importância de estabelecer procedimentos que facilitem e viabilizem a conformidade com as normas estabelecidas.

Ao adotar tais mecanismos, os agentes de tratamento de dados minimizam os riscos de violação à privacidade dos indivíduos, estabelecendo uma base sólida para o tratamento seguro e ético das informações pessoais. Essa abordagem evidencia a preocupação da LGPD não apenas com a conformidade superficial, mas também com a necessidade de adequação efetiva das práticas empresariais e governamentais à

legislação, a fim de promover uma cultura de respeito à privacidade e proteção de dados. Dessa forma, a citação realça a importância de uma governança alinhada com a legislação, contribuindo para a construção de um ambiente mais seguro e confiável no tratamento de dados pessoais.

Ao destacar a importância da adoção de regras de boas práticas, a LGPD ressalta a necessidade de diretrizes éticas e procedimentos responsáveis no tratamento de dados pessoais. Essas regras, ao abordar questões como transparência, participação ativa dos titulares dos dados e proteção dos direitos individuais, contribuem para uma abordagem mais abrangente e alinhada com princípios éticos.

A inclusão da governança como elemento essencial reforça a compreensão de que a gestão eficaz dos dados vai além do cumprimento de obrigações legais. A governança, nesse contexto, envolve a criação de estruturas organizacionais sólidas, a definição de responsabilidades claras, a implementação de medidas de segurança e a busca constante pela conformidade com as melhores práticas.

Portanto, ao enfatizar a necessidade de regras de boas práticas e governança, a LGPD reconhece a importância de uma abordagem proativa na proteção dos dados pessoais, promovendo não apenas a conformidade legal, mas também a construção de uma cultura organizacional comprometida com a ética, transparência e respeito aos direitos individuais. Essa abordagem contribui para a eficácia real da legislação, garantindo que as entidades e órgãos públicos não apenas atendam aos requisitos normativos, mas também adotem práticas que promovam a confiança e a segurança no tratamento de dados pessoais.

Assim, o Capítulo VII da LGPD aborda especificamente sobre a segurança e boas práticas no tratamento de dados pessoais, estabelecendo requisitos e diretrizes que as organizações devem seguir para garantir a segurança dos dados pessoais que coletam e processam. Isso inclui medidas técnicas e organizacionais para proteger os dados contra acessos não autorizados, vazamentos e outras ameaças à segurança. O artigo 50 da LGPD trata especificamente das boas práticas e da governança.

A governança em relação à LGPD envolve a criação de estruturas e processos internos nas organizações para garantir o cumprimento da lei, como por exemplo, a nomeação de um encarregado, a realização de avaliações de impacto, a implementação de políticas e procedimentos de proteção de dados, a criação de treinamentos para funcionários e a manutenção de registros de processamento de dados.

Esta é fundamental para assegurar que a organização esteja em conformidade com a norma, tomando medidas adequadas para proteger os dados pessoais que coleta e processa. A governança é um aspecto essencial para garantir o cumprimento da lei e a proteção dos direitos de privacidade das pessoas cujos dados são processados, organizações que lidam com dados pessoais devem implementar medidas apropriadas para cumprir os requisitos legais.

Para além, a conformidade com a LGPD traz consigo uma série de vantagens com implicações significativas no que tange à salvaguarda dos direitos humanos, dignidade e cidadania, além de outros aspectos de relevo. Cabendo delinear algumas das vantagens intrínsecas à observância dos preceitos da LGPD:

i. Proteção dos direitos humanos: a lei é concebida com o objetivo de resguardar os direitos fundamentais dos indivíduos no que diz respeito ao tratamento de seus dados pessoais. Isso abrange a proteção dos direitos à privacidade, liberdade de expressão, bem como a salvaguarda da intimidade, honra e imagem das pessoas.
ii. Respeito à privacidade: a lei confere particular ênfase à proteção da privacidade das pessoas, estabelecendo a obrigatoriedade de que as organizações coletem e processem dados pessoais de maneira transparente, informando aos titulares dos dados de que forma suas informações serão utilizadas.
iii. Liberdade de expressão: a lei não veda a liberdade de expressão, mas estabelece balizas para garantir que o tratamento de dados pessoais seja conduzido de maneira ética e respeitosa, sem infringir a privacidade alheia.
iv. Desenvolvimento econômico e tecnológico: a legislação fomenta o livre desenvolvimento econômico e tecnológico, fornecendo orientações para que as organizações processem dados pessoais de maneira responsável. Isso pode impulsionar a inovação tecnológica e o desenvolvimento de novos serviços.

Além dessas vantagens, a LGPD estabelece um sistema de sanções e penalidades para as organizações que descumprem suas disposições, promovendo, assim, a conformidade com os princípios e regras estabelecidos e, consequentemente, a proteção dos direitos individuais, desempenhando um papel de extrema relevância na

promoção da salvaguarda de dados pessoais e na garantia dos direitos humanos e da dignidade em um ambiente cada vez mais digital, neste viés é crucial a formulação de regras de boas práticas e de governança por parte dos controladores.

O artigo 50 da LGPD estabelece que os controladores e operadores, dentro de suas respectivas competências, estão autorizados a formular regras de boas práticas e governança relacionadas ao tratamento de dados pessoais, seja de maneira individual ou por meio de associações. Essas regras devem abranger diversos aspectos, tais como a organização, regime de funcionamento, procedimentos (incluindo reclamações e petições dos titulares), normas de segurança, padrões técnicos, obrigações específicas para todas as partes envolvidas no tratamento de dados, ações educativas, mecanismos internos de supervisão e mitigação de riscos, e outros aspectos pertinentes ao tratamento de dados pessoais.

No parágrafo 1º deste artigo, ressalta-se que, ao elaborar tais regras de boas práticas, os controladores e operadores devem levar em consideração a natureza, escopo, finalidade, probabilidade e gravidade dos riscos e benefícios associados ao tratamento de dados pessoais do titular.

O parágrafo 2º permite que o controlador, ao aplicar os princípios delineados nos incisos VII e VIII do artigo 6º da LGPD, e já tratados na seção 2 deste trabalho acadêmico, estabeleça um programa de governança em privacidade, desde que atendidas algumas condições. Neste sentido, deve demonstrar o comprometimento do controlador em adotar processos e políticas internas que garantam o cumprimento abrangente de normas e boas práticas relacionadas à proteção de dados pessoais, devendo ser aplicável a todos os dados pessoais sob seu controle, independente da forma como foram coletados, adaptado à estrutura e escala de suas operações, e estabelecer políticas e salvaguardas apropriadas com base em avaliações sistemáticas de impactos e riscos à privacidade.

O programa também deve buscar estabelecer uma relação de confiança com o titular, ser integrado à estrutura de governança da organização e incluir planos de resposta a incidentes e remediação, além de ser constantemente atualizado com base em informações obtidas por meio de monitoramento contínuo e avaliações periódicas. Essa efetividade deve ser demonstrada quando solicitada pela ANPD ou outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta relacionados à LGPD.

O parágrafo 3º determina que as regras de boas práticas e governança devem ser publicadas e atualizadas periodicamente, e podem ser reconhecidas e divulgadas pela autoridade nacional. Finalmente, o artigo 51 estabelece que a autoridade nacional tem a responsabilidade de incentivar a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

A conscientização dos titulares de dados pessoais, bem como dos agentes de tratamento (ou seja, as organizações que coletam, armazenam e processam esses dados), é fundamental para a eficácia da LGPD. Sem um entendimento claro dos direitos e responsabilidades relacionados à proteção de dados, a implementação da lei pode ser desafiadora, ou até mesmo tornar-se uma legislação ineficaz.

Logo, a implementação de políticas públicas voltadas para a conscientização é, portanto, crucial. Isso pode incluir campanhas de educação pública, treinamento para profissionais de privacidade de dados, orientações para empresas e entidades/órgãos governamentais, além de medidas de fiscalização e cumprimento para garantir a aderência à lei.

É importante ressaltar que a conscientização não deve ser um esforço pontual, mas contínuo, à medida que o cenário de privacidade de dados continua a evoluir. A LGPD, assim como outras regulamentações de proteção de dados em todo o mundo, é um passo importante para equilibrar o uso de dados pessoais com a proteção dos direitos individuais e a confiança do público nas instituições que coletam e processam esses dados.

3.1.3 - A ANPD e as Sanções previstas na LGPD: a importância da adoção de regras de boas práticas e governança

O artigo 55-A da Lei Geral de Proteção de Dados estabelece a criação da Autoridade Nacional de Proteção de Dados, sendo esta uma autarquia de natureza especial, vez que é uma entidade da administração pública indireta, com personalidade jurídica própria e autonomia administrativa e financeira. Sua natureza especial destaca sua importância e autonomia em relação a outros órgãos governamentais.

A ANPD possui autonomia técnica e decisória, podendo tomar decisões independentes no que diz respeito à proteção de dados pessoais. Isso ajuda a garantir

que a autoridade possa cumprir seu papel de fiscalização e regulamentação da LGPD sem influência externa indevida. Possui ainda patrimônio próprio, o que lhe confere a capacidade de gerenciar recursos financeiros para cumprir suas responsabilidades.

O Artigo 55-J da LGPD delineia as competências da Autoridade Nacional de Proteção de Dados no contexto da proteção de dados pessoais. A autoridade é incumbida de diversas responsabilidades, destacando-se:

i. Zelo pela proteção de dados pessoais: assegurar a conformidade com a legislação e garantir a proteção dos dados pessoais;
ii. Observância de segredos comerciais e industriais: preservar segredos comerciais e industriais, considerando a proteção de dados pessoais e o sigilo das informações, quando amparado por lei ou quando a quebra do sigilo violar princípios estabelecidos na lei;
iii. Elaboração de diretrizes para a política nacional: desenvolver diretrizes para a política nacional de proteção de dados pessoais e da privacidade;
iv. Fiscalização e aplicação de sanções: fiscalizar e impor sanções em casos de tratamento de dados em desacordo com a legislação, utilizando processo administrativo que garanta contraditório, ampla defesa e direito de recurso;
v. Apresentação de petições: avaliar petições de titulares contra controladores após comprovação de reclamação não solucionada pelo controlador dentro do prazo regulamentado;
vi. Promoção do conhecimento nas populações: estimular o entendimento das normas e políticas públicas sobre proteção de dados pessoais e medidas de segurança na população;
vii. Estudos sobre práticas nacionais e internacionais: realizar estudos sobre práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
viii. Estímulo à adoção de padrões: incentivar a adoção de padrões para serviços e produtos que facilitem o controle dos titulares sobre seus dados pessoais;
ix. Cooperação internacional: promover a cooperação com autoridades de proteção de dados pessoais de outros países;
x. Publicidade de operações de tratamento de dados: estabelecer formas de

publicidade das operações de tratamento de dados pessoais, respeitando segredos comerciais e industriais.

Essas competências refletem o papel da ANPD na implementação e fiscalização da proteção de dados pessoais, com destaque para a promoção da conscientização, cooperação internacional e estímulo à conformidade. O artigo também enfatiza a importância da preservação do segredo empresarial e do sigilo das informações durante o exercício dessas competências.

Assim, é fundamental destacar que o artigo 52 da lei estabelece as sanções administrativas que podem ser aplicadas pela Autoridade Nacional de Proteção de Dados em caso de infrações às normas da LGPD. É importante refletir que as sanções não devem conter somente um caráter punitivo, mas devem almejar um caráter pedagógico. Assim, cabe pontuar as sanções previstas na referida normativa que podem ser aplicadas pela ANPD:

xi. Advertência: emissão de uma advertência ao agente de tratamento de dados, indicando um prazo para que medidas corretivas sejam adotadas.

xii. Multa simples: a multa pode chegar a até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no último exercício, excluindo os tributos. No entanto, o total da multa não pode exceder R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

xiii. Multa diária: aplicação de multas diárias, observando o limite total estabelecido para a multa simples.

xiv. Publicização da infração: após a devida apuração e confirmação da infração, a ANPD pode publicizar a infração.

xv. Bloqueio de dados pessoais: a autoridade pode ordenar o bloqueio dos dados pessoais relacionados à infração até que a situação seja regularizada.

xvi. Eliminação de dados pessoais: determinação da eliminação dos dados pessoais relacionados à infração.

xvii. Suspensão parcial do funcionamento do banco de dados: suspensão parcial do funcionamento do banco de dados relacionado à infração por até 6 meses, prorrogáveis por igual período, até que a atividade de tratamento seja regularizada pelo controlador.

xviii. Suspensão do exercício da atividade de tratamento de dados: suspensão do exercício da atividade de tratamento dos dados pessoais relacionados à infração por até 6 meses, prorrogáveis por igual período.

xix. Proibição parcial ou total de atividades de tratamento de dados: proibição parcial ou totalmente do exercício de atividades relacionadas ao tratamento de dados.

Os critérios considerados para a aplicação de sanções incluem a gravidade e natureza das infrações, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência, o grau do dano, a cooperação do infrator, entre outros. As sanções podem ser aplicadas de forma gradativa, isolada ou cumulativa, dependendo das circunstâncias do caso. A aplicação das sanções deve seguir a Resolução CD/ANPD nº1/2021 que aprovou o regulamento do processo de fiscalização e do processo administrativo sancionador no âmbito da ANPD.

Cabe destacar que de acordo com o § 3º do artigo 52 da LGPD[13] as sanções administrativas pecuniárias não se aplicam às entidades e aos órgãos públicos, desta forma, a ANPD não poderá efetuar a aplicação das sanções de multa previstas nos incisos II e III do caput do referido artigo. O artigo 53 da LGPD menciona que as sanções administrativas da referida lei não substituem a aplicação de sanções administrativas, civis ou penais definidas em legislação específica. As sanções têm o objetivo de garantir a conformidade com a LGPD e promover a proteção dos dados pessoais dos indivíduos, incentivando as organizações a adotarem boas práticas e governança na implementação da política pública de proteção de dados pessoais.

Quando os agentes de tratamento optam por adotar regras de boa prática e governança no contexto do tratamento de dados, estão manifestando um compromisso sólido com a ética e a responsabilidade. Essa postura vai além da simples conformidade com as regulamentações, evidenciando uma abordagem proativa para garantir a segurança e integridade dos dados pessoais.

Em caso de um incidente fortuito, como um vazamento de dados, a presença de regras de boa prática e governança podem ser indicativas da boa fé por parte dos agentes de tratamento. Isso porque essas regras não apenas estabelecem medidas

[13] Lei nº 13709 de 2018, artigo 52, § 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

preventivas, mas também delineiam procedimentos claros para lidar com incidentes, incluindo a notificação rápida aos titulares afetados e às autoridades competentes.

Ao demonstrar boa fé mediante a adoção dessas práticas, os agentes de tratamento não apenas cumprem requisitos legais, mas também estabelecem um padrão elevado de responsabilidade e transparência. Isso contribui para a construção de confiança com os titulares de dados e reforça a reputação da entidade e do órgão público, mesmo em situações adversas, ao mostrar um compromisso genuíno com a proteção e respeito aos direitos individuais.

3.2 - Da relevância da implementação das boas práticas e governança na proteção de dados

A era digital trouxe consigo um aumento exponencial na coleta, processamento e compartilhamento de dados pessoais, tornando imperativa a discussão sobre a implementação de práticas eficazes para proteger a privacidade e os direitos dos indivíduos. Nesse contexto, a adoção de boas práticas e governança emerge como um pilar fundamental na salvaguarda da integridade e confidencialidade das informações pessoais.

A proteção de dados pessoais não é apenas uma obrigação legal, mas também um imperativo ético. A implementação de boas práticas, que incluem transparência, consentimento informado e respeito aos direitos dos titulares dos dados, reflete um compromisso ético inegociável. Ademais, a governança, ao alinhar-se com normas e regulamentações, assegura a conformidade legal, estabelecendo uma base sólida para a gestão ética de dados.

A adoção de boas práticas não se limita ao cumprimento de requisitos legais; ela se posiciona como um conjunto de vetores de proteção. Ao definir processos transparentes, promover a minimização de dados e estabelecer mecanismos eficazes de resposta a incidentes, as boas práticas atuam como barreiras contra possíveis violações, reforçando a segurança dos dados desde sua coleta até o seu descarte.

A governança, por sua vez, surge como a espinha dorsal que sustenta a implementação efetiva das boas práticas. Ela engloba a definição de responsabilidades, a criação de políticas de segurança e a condução de avaliações sistemáticas de riscos à

privacidade. Uma governança sólida não apenas estabelece diretrizes para o tratamento responsável de dados, mas também oferece flexibilidade para adaptação contínua diante de mudanças no cenário tecnológico e regulatório.

Embora a implementação de boas práticas e governança represente um avanço significativo, ela não está isenta de desafios. A complexidade crescente das operações de tratamento de dados, juntamente com a evolução constante das ameaças cibernéticas, requerem abordagens adaptativas e inovação contínua. No entanto, esses desafios também se apresentam como oportunidades para o aprimoramento constante das práticas e políticas de proteção de dados.

Em um cenário onde a proteção de dados pessoais se torna essencial para a construção de confiança e a preservação dos direitos individuais, a implementação de boas práticas e governança emerge como um imperativo. A promoção desses princípios não só fortalece a conformidade, mas também contribui para a construção de uma cultura organizacional centrada na ética e no respeito pelos direitos individuais. Assim, cabe analisar as primeiras sanções aplicadas pela ANPD como forma de incentivo a adoção de boas práticas e governança

3.2.1 - As primeiras sanções aplicadas pela ANPD: incentivo às regras de boas práticas e governança na proteção de dados

A entrada em vigor da LGPD foi um marco significativo na proteção dos dados pessoais no Brasil, conferindo à ANPD a responsabilidade de fiscalizar e aplicar sanções em caso de descumprimento da legislação. Este tópico aborda as primeiras sanções aplicadas pela autoridade e explora como essas ações desempenham um papel crucial no estímulo à adoção de regras de boas práticas e governança pelas organizações.

As sanções aplicadas pela ANPD não são apenas punitivas, mas também representam um instrumento regulatório destinado a moldar o comportamento das organizações em relação à proteção de dados. Ao analisar casos específicos de não conformidade, a autoridade oferece diretrizes claras sobre as expectativas em relação à implementação de práticas eficazes de proteção de dados.

As sanções aplicadas têm um efeito direto no estímulo à implementação de boas

práticas por parte das organizações. O cumprimento dessas práticas não apenas reduz o risco de sanções, mas também reflete um compromisso proativo com a proteção da privacidade e o respeito aos direitos dos titulares dos dados. Nesse contexto, as boas práticas não são apenas uma exigência legal, mas uma estratégia de gestão de riscos essencial.

A governança, compreendida como a estrutura organizacional que guia e supervisiona o tratamento de dados, emerge como um fator determinante na prevenção de violações e, consequentemente, evita a aplicação de sanções. Organizações que adotam práticas de governança robustas demonstram um compromisso estratégico com a conformidade contínua e a proteção dos direitos dos titulares dos dados.

Apesar de representarem um incentivo valioso, as sanções também apresentam desafios, como a necessidade de adaptação constante às mudanças regulatórias e tecnológicas. Contudo, esses desafios proporcionam oportunidades para aprimorar políticas de proteção de dados, fortalecer a cultura de conformidade e promover inovações sustentáveis no tratamento de informações pessoais.

As primeiras sanções aplicadas pela ANPD não apenas estabelecem um precedente importante na aplicação da LGPD, mas também operam como catalisadores para a adoção generalizada de regras de boas práticas e governança. Destaca-se a importância de as organizações não apenas atenderem às exigências legais, mas também internalizarem uma cultura de proteção de dados que vai além da conformidade, promovendo a confiança e a integridade no tratamento de informações pessoais em um ambiente digital dinâmico.

Assim, com o intuito de contextualizar a relevância da implementação das boas práticas e governança, destaca-se um marco importante no cenário da proteção de dados no Brasil, sublinhando a aplicação de sanções pela ANPD a uma empresa privada e a dois órgãos públicos. Esse acontecimento estabelece um precedente significativo, não apenas em termos de fiscalização, mas também como um alerta crucial para outras organizações que precisam ajustar suas práticas de tratamento de dados em conformidade com a LGPD.

Analisar essas sanções fornece insights valiosos sobre as expectativas e padrões que orientam a conformidade com a legislação de proteção de dados no Brasil. O fato de órgãos públicos terem sido alvo de sanções destaca a abrangência da legislação e sua

aplicabilidade a diversos setores, incluindo aqueles no âmbito governamental. Esse cenário reforça a importância de uma postura diligente em relação à proteção de dados, independentemente do setor de atuação.

A aplicação de penalidades pode servir como um estímulo positivo para que outros órgãos e entidades acelerem seus processos de adequação à LGPD. Isto oferece valiosas diretrizes sobre as expectativas da ANPD em relação às boas práticas de tratamento de dados e à necessidade de implementação de medidas robustas de segurança e privacidade.

A autoridade desempenha um papel fundamental na promoção da mudança de hábitos culturais relacionados à proteção de dados no Brasil, pois é uma entidade governamental criada para fiscalizar e regulamentar a LGPD. Como parte de suas responsabilidades, contribui para a conscientização da sociedade e das organizações quanto ao tratamento de dados, devendo fiscalizar o cumprimento da lei e aplicar sanções em casos de violações. Como dito, isso cria um incentivo para que as organizações cumpram a norma e adotem práticas adequadas de proteção de dados.

Neste contexto, a aplicação da primeira multa pela ANPD constitui um marco significativo na implementação efetiva da política pública de proteção de dados pessoais. A multa foi aplicada a empresa Telekall Inforservice por meio do Processo Administrativo Sancionador nº 00261.000489/2022-62 com base no Relatório de Instrução nº 1/2023/CGF/ANPD. Desta forma, a ANPD tomou as medidas apropriadas e aplicou as sanções cabíveis à Telekall Infoservice de acordo com a LGPD e o Regulamento de Fiscalização, incluindo a imposição de multa e advertência, de acordo com o despacho da CGF/ANPD publicado no Diário Oficial da União de 06 de julho de 2023 (BRASIL,2023):

> O COORDENADOR-GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD, no uso de suas atribuições legais e regulamentares, com fundamento no art. 17, inciso I, do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, examinando os autos do processo em epígrafe, instaurado em face da TELEKALL INFOSERVICE, inscrita no CNPF/MF sob o nº 11.193.228/0001-24, micro empresa, em razão dos indícios de infração à Lei Geral de Proteção de Dados Pessoais (LGPD); e CONSIDERANDO o teor do Relatório de Instrução nº 1/2023/CGF/ANPD (4232669), cujas razões acolho e integro à presente decisão, inclusive como motivação, com fulcro no §1º do art. 50 da Lei nº 9.784/1999 c/c o art. 55 e seguintes do Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021;, decide: 1. Aplicar à empresa TELEKALL INFOSERVICE as sanções de: 1.1.

> ADVERTÊNCIA, sem imposição de medidas corretivas, por infração ao art. 41 da LGPD; e 1.2. MULTA SIMPLES, nos valores de R$ 7.200,00 (sete mil e duzentos reais) por infração ao art. 7º da LGPD e de R$ 7.200,00 (sete mil e duzentos reais) por infração ao art. 5º do Regulamento de Fiscalização, totalizando R$ 14.400,00 (catorze mil e quatrocentos reais). 1.2.1. Caso o autuado resolva, de acordo com o disposto no art. 18 do Regulamento de Fiscalização, renunciar expressamente ao direito de recorrer da decisão de primeira instância, fará jus a um fator de redução de 25% (vinte e cinco por cento) no valor da multa aplicada, desde que faça o recolhimento no prazo para pagamento definido no caput do art. 17 do Regulamento de Fiscalização, 20 (vinte) dias úteis, totalizando nestas circunstâncias o montante de R$ 10.800,00 (dez mil e oitocentos reais). 2. Pela intimação do autuado para cumprimento da sanção e/ou apresentação de recurso, em até 10 (dez) dias úteis, em consonância com o art. 44 da Lei nº 9.784/99 c/c o art. 58 do Regulamento de Fiscalização. Advirto o autuado que a multa deverá ser paga no prazo de até 20 (vinte) dias úteis, contados a partir da ciência oficial da decisão de aplicação da sanção, nos termos do art. 55, §2º, II, do Regulamento de Fiscalização. 3. Aguarde-se o trânsito em julgado. Após, em caso de não cumprimento desta decisão, encaminhe-se este Processo Administrativo Sancionador para a Procuradoria Federal Especializada - PFE da ANPD para a execução da multa cominada, sob pena de inscrição do autuado no Cadastro Informativo de Créditos não Quitados do Setor Público Federal (Cadin) e na Dívida Ativa da União, nos termos do art. 56 c/c art. 67 do Regulamento de Fiscalização.

A CGF/ANPD concluiu que a empresa infringiu o artigo 7º da LGPD, que estabelece as hipóteses legais para o tratamento de dados pessoais. A empresa foi considerada em infração por não ter respaldo legal para suas atividades de tratamento de dados pessoais. Outra infração cometida foi ao artigo 41 da LGPD, que determina que o controlador deve indicar um encarregado pelo tratamento de dados pessoais. Esta foi considerada em infração por não ter indicado o encarregado conforme exigido pela lei.

Também ocorreu infração ao artigo 5º do Regulamento de Fiscalização da ANPD, que estabelece os deveres dos agentes regulados, incluindo a obrigação de fornecer informações e documentação quando requisitados pela ANPD. Foi considerada em infração por não ter respondido adequadamente às solicitações da autoridade. Como resultado dessas infrações, a empresa foi sujeita a sanções.

Para a infração ao art. 7º da LGPD e ao art. 5º do Regulamento de Fiscalização, foram aplicadas multas simples. O valor da multa foi limitado a 2% (dois por cento) do faturamento bruto da empresa, pois se trata de uma microempresa, resultando em uma multa total de R$ 14.400,00 (quatorze mil e quatrocentos reais) – R$ 7.200,00 (sete mil e duzentos reais) para cada infração. Quanto à infração ao art. 41 da LGPD, foi aplicada uma sanção de advertência. É importante ressaltar que o valor das multas e sanções pode variar dependendo das circunstâncias específicas de cada caso, e a ANPD pode levar em consideração diversos fatores ao determinar as penalidades.

Após a aplicação da referida multa a uma pessoa jurídica de direito privado, a autoridade já sancionou dois órgãos públicos, sendo eles o Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo - IAMSPE por meio do processo administrativo sancionador nº 00261.001969/2022-41 e a Secretaria de Estado da Saúde de Santa Catarina - SES-SC por meio do processo administrativo sancionador nº 00261.001886/2022-51.

A ANPD divulgou, no DOU de 06 de outubro de 2023, a conclusão do processo sancionador contra o Instituto de Assistência ao Servidor Público Estadual de São Paulo:

> O COORDENADOR-GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD, no uso de suas atribuições legais e regulamentares, com fundamento no art. 17, inciso I, do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, examinando os autos do processo em epígrafe, instaurado em face do INSTITUTO DE ASSISTÊNCIA AO SERVIDOR PÚBLICO ESTADUAL DE SÃO PAULO - IAMSPE, inscrito no CNPJ/MF sob o nº 60.747.318/0001-62, em razão dos indícios de infração à Lei Geral de Proteção de Dados Pessoais (LGPD); e CONSIDERANDO o teor do Relatório de Instrução nº 2/2023/CGF/ANPD (SUPER nº 4286376), cujas razões acolho e integro à presente decisão, inclusive como motivação, com fulcro no §1º do art. 50 da Lei nº 9.784/1999 c/c o art. 55 e seguintes do Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021;, decide: 1. Aplicar ao IAMSPE as sanções de: 2. ADVERTÊNCIA, por infração ao art. 48 da LGPD, com imposição da seguinte medida corretiva, nos termos do art. 55, §2º, I do Regulamento de Fiscalização, para impor ao IAMSPE a obrigação de: 2.1. Ajustar, no prazo de 10 (dez) dias úteis da data de intimação, o COMUNICADO já existente no sítio do IAMSPE, conforme a redação abaixo: Lei Geral de Proteção de Dados Pessoais - Comunicação de Incidente de Segurança: O Iamspe comunica que tomou conhecimento da ocorrência de incidente de segurança que pode ter comprometido a privacidade dos dados da organização por conta de um acesso não autorizado em dados cadastrais indicados por um usuário externo no início do ano de 2022. Dentre os dados que poderiam ter sido afetados, estariam dados pessoais cadastrais, salário e de residência de nossa base de cientes, o que poderia acarretar o risco de exposição por um determinado período de tempo até nossas correções, ressaltando-se aqui que não identificamos nem fomos comunicados de extração ocorrida. Informamos que o Instituto, imediatamente, realizou ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema de cadastro dos seus contribuintes e dependentes. Por conta destas ações, o Instituto comunicou à Autoridade respectiva somente após a realização dos ajustes necessários. Após comunicação de incidente de segurança à Autoridade Nacional de Proteção de Dados e aos usuários em geral, informamos que estabelecemos um cronograma de ações para melhoria de nossos controles apresentados à ANPD. Dúvidas, solicitações e reclamações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no telefone: (11) 4573-9352, e-mail: lgpd@iamspe.sp.gov.br. Estamos disponíveis para atendimento de segunda-feira a sexta-feira, das 9h às 17h. Política de Privacidade do Iamspe: http://www.iamspe.sp.gov.br/politica-de-privacidade/. 2.1.1. O IAMSPE

> deverá juntar aos autos, no prazo de 10 (dez) dias úteis da data de intimação, comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 1 (uma) captura de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura. 2.2. O comunicado acima deve permanecer disponível por 90 (noventa) dias corridos, contados a partir da data de cumprimento do ajuste no Comunicado, nos termos do item 2.1 acima. 2.2.1. O IAMSPE deverá juntar aos autos comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 9 (nove) capturas de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura, sendo que cada captura deve ser feita no intervalo mínimo de 9 (nove) dias entre cada uma. 2.2.2. A comprovação de cumprimento da medida corretiva deverá ser juntada aos autos em até 5 (cinco) dias úteis do final de cada período de 30 (trinta) dias. 3. ADVERTÊNCIA, por infração ao art. 49 da LGPD, com imposição da seguinte medida corretiva, nos termos do art. 55, §2º, I do Regulamento de Fiscalização, para impor ao IAMSPE a obrigação de: 3.1. Informar à ANPD, neste mesmo processo, o resultado dos programas e objetivos desenvolvidos e implementados, conforme disposto no Anexo V (Plano de três meses e seis meses) das Alegações Finais (SUPER nº 4280896), especificamente quanto aos itens 3, 4, 5, 12, 15 e 17. 3.1.1. Em relação aos itens 3, 4 e 5, o IAMSPE deverá, em até 10 (dez) dias úteis da data da intimação: a) informar o andamento e apresentar à ANPD o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual se comprovará seu cumprimento à ANPD; ou b) em caso de já estarem cumpridos, trazer aos autos comprovação do cumprimento. 3.1.2. Em relação aos itens 12, 15, 17, o IAMSPE deverá apresentar à ANPD, em até 10 (dez) dias úteis da data da intimação, o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual se comprovará seu cumprimento à ANPD. 4. Pela intimação do autuado para cumprimento das sanções e medidas corretivas e/ou apresentação de recurso, em até 10 (dez) dias úteis, em consonância com o art. 56 da Lei nº 9.784/99 c/c o art. 58 do Regulamento de Fiscalização. 5. Aguarde-se o trânsito em julgado. Após, em caso de não cumprimento desta decisão, encaminhe-se este Processo Administrativo Sancionador para a Procuradoria Federal Especializada - PFE da ANPD para a execução das medidas corretivas.

A autoridade impôs ao IAMSPE advertências por violações específicas à LGPD, acompanhadas de medidas corretivas direcionadas. A primeira advertência refere-se ao artigo 48 da LGPD, envolvendo a obrigação de ajustar um comunicado no site do IAMSPE, informando sobre um incidente de segurança e as ações tomadas para mitigar o impacto. A segunda advertência refere-se ao artigo 49 da lei, exigindo que o IAMSPE informe à ANPD os resultados de programas implementados.

O instituto tem um período específico para ajustar o comunicado em seu site, seguido da obrigação de fornecer comprovação fotográfica dessa implementação. Além disso, deve apresentar cronogramas para o cumprimento das medidas corretivas, demonstrando seu compromisso com a conformidade à LGPD.

O despacho conclui enfatizando a necessidade de cumprimento das decisões da

ANPD, destacando que a não conformidade pode resultar na execução das medidas corretivas pela Procuradoria Federal Especializada. A análise destaca a firmeza da autoridade na aplicação das normas de proteção de dados, sublinhando a importância da conformidade contínua para organizações sujeitas à LGPD.

Em 18 de outubro de 2023 a ANPD emitiu sanções contra a Secretaria de Estado da Saúde de Santa Catarina:

> O COORDENADOR-GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD, no uso de suas atribuições legais e regulamentares, com fundamento no art. 17, inciso I, do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, examinando os autos do processo em epígrafe, instaurado em face da SECRETARIA DE ESTADO DA SAÚDE DE SANTA CATARINA - SES/SC, inscrito no CNPJ/MF sob o nº 82.951.245/0001-69, em razão dos indícios de infração à Lei Geral de Proteção de Dados Pessoais (LGPD); e
>
> CONSIDERANDO o teor do Relatório 4/2023 de Instrução (SEI nº 4478157), cujas razões acolho e integro à presente decisão, inclusive como motivação, com fulcro no §1º do art. 50 da Lei nº 9.784/1999 c/c o art. 55 e seguintes do Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021;, decide: 1. Aplicar à SES/SC as sanções de: 2. ADVERTÊNCIA, por infração ao art. 38 da LGPD, sem a imposição de medida corretiva. 3. ADVERTÊNCIA, por infração ao art. 48 da LGPD, com imposição da seguinte medida corretiva, nos termos do art. 55, §2º, I do Regulamento de Fiscalização, para impor à SES/SC a obrigação de: 3.1. Manter o CIS ao titular geral indicado por esta CGF na primeira página do https://listadeespera.saude.sc.gov.br/#/home, página inicial do sítio, por mais 90 (noventa) dias a contar da data da publicação da decisão neste PAS, considerando que após a publicação dessa decisão é possível que os titulares tomem ciência do incidente em questão e busquem mais informações junto à SES/SC. 3.1.1. A SES/SC deverá juntar aos autos comprovação de que a medida corretiva descrita foi cumprida por meio da apresentação de, pelo menos, 9 (nove) capturas de tela do sítio da SES/SC contendo o comunicado e com visualização clara da data da captura sendo que cada captura deve ser feita no intervalo mínimo de 9 (nove) dias entre cada uma. A comprovação de cumprimento da medida corretiva deverá ser juntada aos autos em até 5 (cinco) dias úteis do final de cada período de 30 (trinta) dias. 3.2. Enviar CIS ao titular de maneira individualizada para os titulares identificados por meio da extração de informação do arquivo vazado e veiculado no site "RAID FORUMS". A viabilidade desta medida decorre de ter sido indicada pelo próprio autuado na proposta de TAC enviada à esta CGF, conforme Termo Proposta TAC (SEI nº 3666469) e corroborado em Parecer encarregado de dados (SEI nº 4470740), diante da possibilidade de uso da ferramenta Notifica-BR. 3.2.1. A SES/SC deverá juntar aos autos, no prazo de 20 (vinte) dias úteis da data de intimação, comprovação de que a medida corretiva descrita foi cumprida por meio da apresentação de uma planilha com a lista completa de todos os titulares identificados que foram individualmente comunicados contendo (i) o nome completo do titular; (ii) e informação de contato utilizada para a comunicação individual (o número de telefone, se por meio telefônico; o e-mail, se por correio eletrônico etc.), a fim de que seja possível que a CGF valide, por amostra, a comunicação feita ao titular. 4. ADVERTÊNCIA, por infração ao art. 49 da LGPD, sem a imposição de medida corretiva. 5. ADVERTÊNCIA, por infração ao art. 5º do Regulamento de Fiscalização, sem a imposição de medida corretiva. 6. Pela

> intimação do autuado para cumprimento das sanções e medidas corretivas e/ou apresentação de recurso, em até 10 (dez) dias úteis, em consonância com o art. 56 da Lei nº 9.784/99 c/c o art. 58 do Regulamento de Fiscalização. 7. Aguarde-se o trânsito em julgado. Após, em caso de não cumprimento desta decisão, encaminhe-se este Processo Administrativo Sancionador para a Procuradoria Federal Especializada - PFE da ANPD para a execução das medidas corretivas.

Foram identificadas quatro infrações à LGPD e ao Regulamento de Fiscalização, sendo três delas consideradas graves. A Coordenação-Geral de Fiscalização concluiu que a SES-SC negligenciou a segurança dos sistemas que tratam dados pessoais de cidadãos atendidos pelo sistema de saúde estadual, infringindo o art. 49 da LGPD.

Além disso, a Secretaria não comunicou de maneira clara, adequada e tempestiva um incidente de segurança, afetando cerca de 300 mil titulares de dados, resultando em uma infração ao art. 48 da lei. A ANPD também sancionou a SES-SC por não apresentar o Relatório de Impacto de Proteção de Dados Pessoais (RIPD), conforme o art. 38 da LGPD, e por não fornecer outras informações requisitadas pela autoridade, violando o Regulamento de Fiscalização. Assim, a ANPD aplicou quatro sanções de advertência, uma para cada infração, e determinou medidas corretivas, incluindo a manutenção de um comunicado de incidente de segurança no site por 90 dias e a informação direta aos titulares afetados.

Julga-se importante estabelecer um comparativo entre as sanções impostas pela ANPD à Telekall, SES/SC e IAMSPE:

Telekall Infoservice: (i) Advertência: Por infração ao artigo 41 da LGPD, sem imposição de medidas corretivas; (ii) Multa Simples: R$ 7.200,00 (sete mil e duzentos reais) por infração ao artigo 7º da LGPD; R$ 7.200,00 (sete mil e duzentos reais) por infração ao artigo 5º do Regulamento de Fiscalização; totalizando R$ 14.400,00 (quatorze mil e quatrocentos reais), tendo como fator de redução da multa a opção de renunciar ao direito de recorrer para obter desconto de 25% (vinte e cinco por cento), resultando em multa de R$ 10.800,00 (dez mil e oitocentos reais); (iii) Intimação do Autuado: cumprir a sanção e/ou apresentar recurso em até 10 dias úteis. Prazo de 20 dias úteis para o pagamento da multa após a ciência oficial.

Secretaria de Estado da Saúde de Santa Catarina (SES/SC): (i) Advertência: por infração ao artigo 38 da LGPD, sem imposição de medidas corretivas; (ii) Advertência: por infração ao artigo 48 da LGPD, imposição de medidas corretivas relacionadas à manutenção de comunicado por 90 dias, envio individualizado do Comunicado de

Incidente de Segurança (CIS) aos titulares identificados; (iii) Advertência: por infração ao artigo 49 da LGPD, sem imposição de medidas corretivas.

Instituto de Assistência ao Servidor Público Estadual de São Paulo (IAMSPE): (i) Advertência: por infração ao artigo 48 da LGPD, imposição de medidas corretivas relacionadas à divulgação de incidente de segurança no site, manutenção do comunicado por 90 dias, envio individualizado do CIS aos titulares identificados; (ii) Advertência: por infração ao artigo 49 da LGPD, imposição de medidas corretivas para informar a ANPD o resultado dos programas e objetivos desenvolvidos e implementados.

É importante destacar que os dois órgãos públicos sancionados pela ANPD violaram os artigos 48 e 49 da LGPD, estabelecendo assim um precedente para que outros órgãos públicos realizem ajustes em conformidade com a legislação. Observando ainda a importância do Relatório de Impacto de Proteção de Dados Pessoais, previsto no artigo 38 da LGPD, que estabelece que a autoridade nacional tem o poder de exigir que o controlador elabore um relatório de impacto à proteção de dados pessoais, inclusive dados sensíveis, relacionado às suas operações de tratamento de dados. Isso deve ser feito de acordo com as diretrizes estabelecidas em regulamento, e respeitando os segredos comerciais e industriais.

O parágrafo único do referido artigo esclarece que o relatório deve conter, no mínimo, informações como a descrição dos tipos de dados coletados, a metodologia empregada na coleta e na garantia da segurança das informações, bem como a análise do controlador em relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados durante o processo de tratamento de dados. Essa exigência visa garantir a transparência, a segurança e a conformidade das práticas do controlador em relação à proteção de dados pessoais, incluindo dados sensíveis.

O artigo 48 da LGPD estabelece a obrigatoriedade do controlador em comunicar à autoridade nacional e ao titular sobre incidentes de segurança que possam resultar em risco ou dano relevante aos titulares. Este comunicado deve ocorrer em prazo razoável, conforme determinado pela autoridade nacional, e deve incluir informações essenciais, tais como a descrição da natureza dos dados pessoais afetados, detalhes sobre os titulares envolvidos, indicação das medidas técnicas e de segurança adotadas para a proteção dos dados, considerando segredos comerciais e industriais, bem como a exposição dos riscos associados ao incidente. Adicionalmente, o comunicado deve

esclarecer os motivos de eventual demora na comunicação e apresentar as medidas adotadas ou a serem tomadas para reverter ou mitigar os efeitos do prejuízo.

No parágrafo 2º, destaca-se a prerrogativa da autoridade nacional em avaliar a gravidade do incidente e, se necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências específicas. Tais providências podem incluir a ampla divulgação do incidente em meios de comunicação e a implementação de medidas para reverter ou mitigar os efeitos do incidente.

Ainda, no parágrafo 3º, salienta-se a importância da autoridade nacional avaliar a gravidade do incidente, considerando a eventual comprovação de que foram adotadas medidas técnicas adequadas para tornar os dados pessoais afetados ininteligíveis para terceiros não autorizados, dentro dos limites técnicos do serviço.

Por sua vez, o artigo 49 da LGPD estabelece requisitos para os sistemas utilizados no tratamento de dados pessoais. Tais sistemas devem ser estruturados de forma a atender aos requisitos de segurança, padrões de boas práticas, governança e princípios gerais estabelecidos na lei, bem como às demais normas regulamentares aplicáveis.

A legislação visa garantir a proteção efetiva dos dados pessoais, desde a comunicação de incidentes de segurança até a definição de padrões para os sistemas que realizam o tratamento dessas informações, reforçando a importância da conformidade e governança no contexto da proteção de dados. Este arcabouço legal contribui para o avanço da segurança da informação e a preservação da privacidade dos titulares de dados.

É fundamental que as entidades e órgãos públicos compreendam a natureza sensível dos dados pessoais e assumam a responsabilidade de tratá-los com o devido respeito e cuidado. Isso não apenas ajuda a evitar problemas legais, mas também constrói a confiança dos usuários. Portanto, a conscientização sobre a importância dos dados pessoais e a conformidade com as regulamentações de privacidade são essenciais na era digital. Neste sentido, a ANPD deve ao aplicar as sanções previstas na LGPD buscar associar ao caráter pedagógico, para que os agentes de tratamento sejam estimulados a se adequarem à normativa.

No entanto, é crucial destacar que as penalidades pecuniárias não são passíveis de aplicação às entidades e órgãos públicos, o que pode resultar em uma falta de

estímulo para a devida conformidade. Diante desse cenário, torna-se imperativo investir na promoção de uma mudança cultural, levando em consideração o caráter pedagógico da penalidade. Essa abordagem busca contribuir para uma transformação na cultura relacionada ao tratamento de dados pessoais por parte das entidades e órgãos públicos. Isso se faz necessário, pois os agentes de tratamento muitas vezes estão habituados a lidar com dados pessoais sem as devidas garantias de segurança.

Logo, para que haja uma efetiva implementação da política pública de proteção de dados, as entidades e órgãos públicos devem incluir a implementação de medidas de segurança, regras de boas práticas e governança para proteger os dados pessoais contra acessos não autorizados, vazamentos e violações. Cultivando uma cultura de conformidade com a LGPD, isso envolve treinamento de funcionários, implementação de políticas de privacidade e a nomeação de um Encarregado de Proteção de Dados quando necessário.

A cultura de proteção de dados deve ser dinâmica e orientada para o aprimoramento contínuo. As organizações devem estar dispostas a ajustar suas práticas à medida que as ameaças à privacidade evoluem e as regulamentações mudam. Logo, a mudança de hábitos culturais é essencial para a implementação eficaz da proteção de dados, pois garante que tanto os indivíduos quanto as organizações estejam alinhados com os princípios de privacidade e cumpram as obrigações legais. Essa mudança cultural é um componente-chave para o sucesso da LGPD e de outras regulamentações de proteção de dados em todo o mundo.

Neste viés, a adoção de regras de boas práticas no contexto da proteção de dados é de suma importância, especialmente em um cenário onde a gestão responsável e ética das informações pessoais tornaram-se cruciais. Esta implementação é fundamental por diversos motivos: (i) refletem as exigências legais e regulatórias, ao adotá-las, as organizações se alinham aos requisitos legais, evitando sanções e penalidades decorrentes de não conformidade; (ii) quando bem elaboradas têm como foco central a proteção dos direitos dos titulares dos dados; (iii) contribui para a construção de confiança entre as organizações e os titulares dos dados; (iv) reforça a imagem da entidade e do órgão público comprometidos com a segurança e privacidade dos dados de seus usuários; (v) incluem medidas preventivas e reativas para lidar com potenciais violações de dados; (vi) refletem um comprometimento ético com o tratamento responsável dos dados; (vii) podem estimular a inovação sustentável, incentivando a

busca por soluções tecnológicas que respeitem a privacidade desde a concepção (*privacy by design*) e a incorporação de princípios éticos em processos de desenvolvimento.

Em resumo, a adoção de regras de boas práticas não só atende a exigências legais, mas também promove uma cultura organizacional centrada na ética, transparência e respeito pelos direitos individuais. Esse compromisso não apenas protege a organização de possíveis implicações legais, mas também contribui para a construção de relacionamentos duradouros com os titulares dos dados.

3.2.2 - Do encarregado e do relatório de impacto de proteção de dados pessoais como boa prática.

A proteção de dados pessoais tornou-se uma temática central no contexto contemporâneo, impulsionada pelo avanço tecnológico e pela crescente digitalização das informações. Nesse cenário, a LGPD surge como um marco regulatório no Brasil, estabelecendo princípios e diretrizes para o tratamento adequado dessas informações sensíveis. Dois elementos cruciais nesse contexto são o papel do Encarregado e a elaboração do Relatório de Impacto de Proteção de Dados (RIPD).

O Encarregado, conforme estipulado pelo artigo 41 da LGPD, é um agente designado pelo controlador de dados para atuar como ponto de contato entre a organização, os titulares dos dados e a ANPD. Essa figura desempenha um papel estratégico ao fomentar uma cultura de proteção de dados na organização. Ao receber solicitações dos titulares e da autoridade nacional, o Encarregado adota providências e orienta funcionários sobre as práticas a serem seguidas em relação à proteção de dados pessoais. Sua atuação contribui para o cumprimento das normas legais e a promoção da transparência na gestão de informações.

Já o Relatório de Impacto de Proteção de Dados, conhecido como RIPD, configura-se como uma ferramenta proativa e preventiva. Embora a LGPD não exija explicitamente a elaboração do RIPD, sua construção representa uma boa prática recomendada em diversos setores. Esse relatório visa identificar e mitigar potenciais riscos à privacidade dos titulares durante o tratamento de dados pessoais. Ele contempla uma análise aprofundada dos impactos das operações de tratamento, proporcionando

uma visão clara dos procedimentos adotados pela organização para proteger as informações sob sua responsabilidade.

A relação entre o Encarregado e o RIPD destaca-se como uma abordagem sinérgica na conformidade com a LGPD. O Encarregado, ao estar ciente das operações e práticas internas, pode desempenhar um papel fundamental na condução ou supervisão da elaboração do RIPD. Sua expertise contribui para uma análise mais abrangente e criteriosa, assegurando que todos os aspectos relevantes sejam considerados no processo.

Dessa forma, a designação de um Encarregado e a elaboração do RIPD não apenas atendem aos requisitos legais, mas também refletem um compromisso ético e responsável por parte das organizações. Além de mitigar riscos legais e financeiros, essas práticas fortalecem a confiança dos titulares, melhoram a reputação da instituição e demonstram um alinhamento proativo com os princípios de proteção de dados pessoais. Em um cenário dinâmico e desafiador, investir na integração efetiva desses elementos é essencial para promover a governança da informação e a sustentabilidade das operações no universo digital.

3.2.2.1 - Do encarregado

A ANPD publicou a primeira versão do *guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado* em maio de 2021 e a segunda versão em abril de 2022, este foi elaborado com o propósito de oferecer diretrizes esclarecedoras sobre os conceitos e as responsabilidades dos agentes envolvidos no tratamento de dados pessoais, especialmente o controlador, o operador e o encarregado.

O guia busca preencher lacunas interpretativas da LGPD, proporcionando orientações não vinculantes sobre quem pode exercer essas funções, definições legais, regimes de responsabilidade, casos práticos e perguntas frequentes. Ele serve como um recurso informativo para organizações, tanto públicas quanto privadas, na aplicação prática dos princípios estabelecidos pela lei, contribuindo para uma compreensão mais clara e consistente das responsabilidades relacionadas ao tratamento de dados pessoais.

Assim, a ANPD (2022, pg.22-24) em seu guia orientativo, informa que

conforme estabelecido no artigo 41 da LGPD, o controlador de dados é obrigado a designar um encarregado para o tratamento de dados pessoais. O encarregado desempenha um papel crucial ao fomentar e disseminar a cultura de proteção de dados na organização, lidando com solicitações de titulares e da autoridade nacional, além de orientar funcionários sobre práticas relacionadas à proteção de dados.

A LGPD não especifica as circunstâncias em que uma organização deve indicar um encarregado, sendo assumido que, como regra geral, toda organização deve designar alguém para esse papel. Entretanto, em conformidade com o § 3º do art. 41, a ANPD publicou a Resolução CD/ANPD nº 2/2022, que estabelece o Regulamento de Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte, permitindo a dispensa da necessidade de indicação do encarregado.

A legislação não faz distinção entre instituições públicas ou privadas, reforçando a importância de ambas cumprirem a obrigação de indicar um encarregado. A LGPD também não especifica se o encarregado deve ser pessoa física ou jurídica, ou se deve ser um funcionário interno ou um agente externo. Boas práticas internacionais sugerem que o encarregado pode ser tanto um funcionário interno quanto um agente externo, sendo recomendável a indicação formal por meio de contrato de prestação de serviços ou ato administrativo.

É relevante que o encarregado tenha liberdade em suas atribuições, e suas qualificações profissionais devem ser determinadas pelo controlador, considerando conhecimentos de proteção de dados e segurança da informação que atendam às necessidades da organização. A LGPD não impede o apoio ao encarregado por uma equipe de proteção de dados, sendo importante que ele tenha recursos adequados, incluindo recursos humanos, financeiros, tempo e infraestrutura.

Embora a legislação não proíba um mesmo encarregado de atuar em nome de diferentes organizações, é essencial garantir sua eficiência ao atender às demandas de cada entidade. A responsabilidade pelas atividades de tratamento de dados pessoais permanece com o controlador ou operador de dados, conforme estabelecido pelo art. 42 da LGPD.

O guia ainda informa que as atribuições do encarregado, conforme estipulado pelo §2º do art. 41, incluem a aceitação de reclamações e comunicações dos titulares, prestação de esclarecimentos e adoção de providências, recebimento de comunicações

da autoridade nacional e tomada de providências, orientação de funcionários e contratados sobre práticas relacionadas à proteção de dados pessoais, além da execução de outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

É crucial que os detalhes de contato do encarregado estejam facilmente acessíveis, conforme o § 1º do art. 41 da LGPD, divulgados de maneira clara e objetiva, preferencialmente no site do controlador. Em consonância com o § 3º do art. 41, a ANPD poderá estabelecer normas complementares sobre a definição e atribuições do encarregado. Importante ressaltar que, no momento, não há exigência legal ou regulamentar para a comunicação ou registro da identidade e informações de contato do encarregado perante a ANPD, podendo essa questão ser regulamentada pela Autoridade em normativo futuro.

Salienta-se que em 20/11/2020 foi publicada no DOU a instrução normativa SGD/ME nº 117, de 19 de novembro de 2020, que é anterior ao guia orientativo. Esta dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

Esta estipula que a autoridade máxima de órgãos e entidades da administração pública federal deve designar um encarregado, conforme estabelecido nos dispositivos legais contidos no inciso III do artigo 23 e no artigo 41 da LGPD. Este encarregado deve possuir conhecimentos multidisciplinares essenciais para a função, preferencialmente nas áreas de privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público. Além disso, é determinado que o encarregado não deve estar vinculado às unidades de Tecnologia da Informação ou ocupar cargos de gestão de sistemas de informação dentro da estrutura do órgão ou entidade.

Também estabelece que os órgãos que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) têm a responsabilidade de adequar políticas e diretrizes de Tecnologia da Informação, adaptar sistemas, serviços e infraestrutura de TI, além de prestar informações e suporte técnico ao encarregado.

Reafirma que a identidade e informações de contato do encarregado devem ser divulgadas publicamente, de maneira clara e objetiva, no site institucional do órgão ou

entidade, conforme previsto no parágrafo 1º do artigo 41 da LGPD.

Enfatiza que a autoridade máxima do órgão ou entidade deve garantir ao encarregado acesso direto à alta administração, apoio imediato das unidades administrativas para atender solicitações de informações e contínuo aprimoramento relacionado aos temas de privacidade e proteção de dados pessoais.

Logo, a nomeação de um encarregado não apenas satisfaz os requisitos legais, mas também representa um compromisso ético e responsável por parte das organizações. Essa prática fortalece a confiança dos titulares, aprimora a reputação da instituição e evidencia um comprometimento proativo com os princípios de proteção de dados pessoais. Em um contexto dinâmico e desafiador, isto é fundamental para promover regras de boa prática e governança institucional.

3.2.2.2 - Do relarório de impacto de proteção de dados

O Relatório de Impacto à Proteção de Dados Pessoais figura como um instrumento essencial no contexto da LGPD, proporcionando uma análise criteriosa e sistemática dos possíveis impactos das operações de tratamento de dados pessoais sobre a privacidade dos titulares. Destaca-se que, no cenário atual, o processo de regulamentação desse tema encontra-se em fase de desenvolvimento, como delineado na Agenda Regulatória para o biênio 2023/2024, aprovada pela Portaria nº 35, de 4 de novembro de 2022.

Nesse contexto, é imprescindível salientar que, em virtude desse processo regulatório em andamento, a ANPD pode estabelecer obrigações adicionais e ajustar parâmetros concernentes aos RIPDs no futuro. Tal prerrogativa reflete a dinâmica evolutiva do campo da proteção de dados e a necessidade de adaptação às transformações tecnológicas e sociais, garantindo que as normativas estejam alinhadas com as demandas contemporâneas.

Assim, a implementação e aprimoramento do RIPD constituem-se como uma jornada dinâmica, sujeita a evoluções normativas que visam fortalecer os mecanismos de proteção à privacidade. Essa perspectiva ressalta a importância de uma abordagem proativa por parte das organizações, antecipando-se às futuras exigências da ANPD e demonstrando um comprometimento contínuo com a conformidade e a salvaguarda dos

dados pessoais.

O controlador, conforme estabelecido nos artigos 5º, inciso XVII, e 38 da LGPD, é o agente responsável pela elaboração do RIPD. A ANPD recomenda a elaboração desse relatório em contextos nos quais as operações de tratamento de dados pessoais possam apresentar elevado risco aos princípios gerais de proteção de dados, às liberdades civis e direitos fundamentais dos titulares, conforme avaliação a ser realizada pelo próprio agente de tratamento.

A LGPD delineia situações específicas em que a elaboração do RIPD pode ser exigida pela ANPD, incluindo operações de tratamento relacionadas à segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais, tratamentos fundamentados em interesses legítimos, operações de entidades do Poder Público, e operações de controladores em geral, especialmente aquelas que envolvem dados pessoais sensíveis.

O momento ideal para a elaboração do RIPD é antes do início do tratamento dos dados pessoais para a finalidade desejada. Isso permite ao controlador antecipar e avaliar os possíveis riscos associados ao tratamento, identificando a probabilidade de sua ocorrência e adotando medidas apropriadas para mitigar esses riscos. Caso não seja possível elaborar o RIPD antes do início do tratamento, a recomendação é que seja elaborado assim que for identificado um tratamento que possa gerar alto risco, respeitando sempre as diretrizes da ANPD.

A gestão de riscos relacionados à privacidade, um aspecto crucial na elaboração do RIPD, deve seguir diretrizes gerais e considerar aspectos como objetivos estratégicos, estrutura organizacional, requisitos legais da LGPD, e demais normativos aplicáveis. O processo de gestão de risco pode ser conduzido por diferentes metodologias, e a escolha da metodologia é de responsabilidade do controlador.

O RIPD deve conter, no mínimo, a descrição dos tipos de dados pessoais tratados, a metodologia utilizada para o tratamento e garantia da segurança das informações, e a análise do controlador em relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados. Embora a divulgação do RIPD não seja obrigatória, permitir o acesso público pode ser uma prática recomendável, demonstrando transparência e responsabilidade do controlador. No entanto, em relação a entidades e órgãos públicos, a publicação do RIPD pode ser exigida pela ANPD ou

realizada pelo próprio controlador, respeitando a legislação pertinente.

O controlador pode optar por elaborar um RIPD único para operações similares ou distintos para projetos/processos que envolvam diferentes finalidades ou riscos. A elaboração do relatório é recomendada sempre que o tratamento possa gerar alto risco, conforme critérios específicos da lei. A gestão de riscos e a avaliação do nível de risco devem considerar possíveis consequências sobre os titulares dos dados pessoais, levando em conta aspectos como a perda de confidencialidade, integridade ou disponibilidade de dados, reversão da anonimização, violação de liberdades e direitos, entre outros.

Enquanto não houver regulamentação específica sobre o RIPD, os controladores podem adotar como parâmetro o conceito de tratamento de alto risco definido no Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte. Este conceito considera critérios gerais, como "larga escala" ou "afetar significativamente interesses e direitos fundamentais dos titulares", e critérios específicos, como "uso de tecnologias emergentes ou inovadoras" e "utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos".

A elaboração do relatório é uma prática essencial na conformidade com a legislação, permitindo que o controlador esteja ciente e possa mitigar os riscos associados ao tratamento de dados pessoais, fortalecendo a proteção da privacidade e dos direitos dos titulares.

O encaminhamento do relatório à ANPD não é determinado pela LGPD como uma regra geral. No entanto, a legislação estabelece que, durante o exercício efetivo de suas funções de fiscalização e em situações específicas previstas na lei, a autoridade pode requisitar do controlador o envio do RIPD. Isso inclui a possibilidade de solicitar cópias de documentos, sejam eles físicos ou digitais, juntamente com dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais.

Dessa forma, o controlador está obrigado a encaminhar o relatório somente quando solicitado pela autoridade, ficando sujeito a medidas de fiscalização em caso de descumprimento desta requisição. Esse processo tem como objetivo proporcionar à ANPD uma visão abrangente das práticas de tratamento de dados adotadas pelo controlador, permitindo a avaliação da conformidade com os princípios e diretrizes estabelecidos pela lei.

O controlador pode consultar a ANPD em caso de dúvidas sobre as salvaguardas e medidas a serem adotadas para mitigar os riscos identificados. No entanto, esta não fornece respostas individuais a consultas jurídicas em tese ou que demandem a emissão de parecer específico sobre condições hipotéticas ou concretas. Embora a autoridade não emita manifestações sobre as salvaguardas em casos específicos, o controlador pode enviar dúvidas. Essas demandas são avaliadas e consolidadas para possíveis considerações no processo de elaboração de regulamentos ou orientações futuras.

No processo de elaboração do RIPD, é recomendável que o encarregado seja consultado, alinhando-se com as atribuições legais definidas na LGPD. Além disso, o controlador pode consultar outros membros da organização, operadores, o público externo e especialistas para enriquecer o processo de elaboração do relatório, considerando diferentes perspectivas.

Embora não haja uma exigência específica de registro de opiniões divergentes, essa prática pode ser considerada positiva em termos de transparência e responsabilização. Os controladores têm flexibilidade para determinar as estruturas e formatos de seus relatórios, contribuindo para a integridade do processo e evidenciando o compromisso do controlador com a consideração de diferentes perspectivas.

Após a elaboração do RIPD, o controlador deve analisar a viabilidade de dar continuidade aos processos de tratamento de dados pessoais. Recomenda-se a revisão contínua deste, especialmente diante de eventos que possam implicar mudanças nos riscos identificados. Isso assegura que o relatório permaneça atualizado e relevante ao ambiente operacional do controlador, fortalecendo a postura proativa em relação à proteção de dados pessoais.

É imperioso destacar os dados e informações o que a ANPD (2023) pontua que devem constar no RIPD:

> É recomendável que o RIPD reúna os seguintes dados e informações: a) Identificação dos agentes de tratamento e do encarregado; b) Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos; c) Justificativa da necessidade de elaboração do relatório (por exemplo: alto risco, solicitação da ANPD, gestão de riscos e prevenção, outros); d) Projeto/Processo que justifica a elaboração do RIPD; e) Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD; f) Tratamento de dados; i. Descrição do tratamento (desde a coleta até a eliminação); ii. Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa); iii. Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratados, de forma completa); iv. Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes,

> autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços); v. Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver; vi. Volume de dados pessoais tratados e número de titulares envolvidos no tratamento; vii. Fonte de coleta; viii. Finalidade do tratamento (Justifique a finalidade de tratamento para cada dado); ix. Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver); x. Política de armazenamento (descrever os prazos de retenção e métodos de descarte); g) Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento; h) Análise de princípios da LGPD; i) Riscos identificados ao titular; j) Resultado apurado com base na metodologia utilizada pelo agente de tratamento: descrição do risco e do impacto para os titulares, probabilidade, impacto, risco total; k) Medidas, salvaguardas e mecanismos de mitigação de risco: risco; tratamento do risco (descrever as medidas adotadas para mitigação do risco); risco após o tratamento, risco residual. l) Comentários e aprovações.

A estrutura proposta está alinhada de maneira eficaz com os princípios e diretrizes estabelecidos pela lei. Cada componente desse guia abrangente reflete uma abordagem detalhada no tratamento de dados pessoais, demonstrando um compromisso claro com a transparência, responsabilidade e avaliação de riscos.

A identificação dos agentes de tratamento e do encarregado é fundamental para estabelecer clareza sobre as responsabilidades e envolvimento de cada parte no processo de tratamento de dados, cumprindo com os princípios de *accountability*. A consideração de consultas e pareceres de outras partes interessadas destaca a importância da colaboração e da coleta de perspectivas diversas, promovendo uma abordagem inclusiva na elaboração.

A justificativa da necessidade de formulação do relatório oferece contexto essencial, indicando motivações como alto risco, solicitação da ANPD, gestão de riscos ou outros fatores relevantes. Os elementos relacionados a projeto/processo e sistemas de informação conectam o RIPD ao contexto operacional mais amplo, ajudando a entender as nuances do tratamento de dados dentro de projetos e sistemas específicos.

O detalhamento do tratamento de dados, incluindo dados pessoais e sensíveis, categorias de titulares, volume de dados e fonte de coleta, é essencial para uma avaliação abrangente e alinhamento com os princípios de finalidade, necessidade e proporcionalidade. A análise da hipótese legal e princípios da LGPD garante que o tratamento de dados esteja em conformidade com a legislação e princípios éticos.

A identificação de riscos, incluindo descrição, probabilidade, impacto e avaliação total do risco, oferece uma visão detalhada dos desafios potenciais associados ao tratamento de dados. A descrição das medidas adotadas, tratamento de riscos e

avaliação do risco residual destaca a ênfase na mitigação efetiva de riscos e na proteção dos titulares.

A inclusão da seção de comentários e aprovações assegura a transparência e responsabilidade, destacando a importância de revisões críticas e aprovações formais. Em resumo, a estrutura delineada para o RIPD não apenas atende às exigências da LGPD, mas também estabelece uma base sólida para uma cultura organizacional de proteção de dados. Ela incentiva a reflexão profunda sobre as práticas de tratamento de dados, promovendo a conformidade contínua e o aprimoramento das medidas de proteção à privacidade.

Assim, o relatório é um documento crucial no âmbito da lei, compreendendo a descrição pormenorizada dos processos de tratamento de dados pessoais suscetíveis a gerar riscos elevados para a salvaguarda dos princípios fundamentais de proteção previstos na legislação e para as liberdades civis e direitos fundamentais dos titulares de dados. Por isso, este relatório deve contemplar não apenas a exposição dos tipos de dados coletados e as metodologias de tratamento, mas também as análises e reflexões do controlador sobre as medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Ao refletir sobre o exposto nesta seção, surge a imperativa necessidade de direcionar a atenção para as adequações indispensáveis à implementação efetiva da política pública de proteção de dados na UFRRJ. Na próxima seção desta dissertação, serão analisadas as estratégias e ações práticas que visam a implementação da LGPD, promovendo não apenas a conformidade com a legislação vigente, mas também o fortalecimento da cultura de proteção de dados na UFRRJ. A investigação aqui realizada representa o ponto de partida para a construção de uma base sólida que assegurará a integridade e a segurança dos dados pessoais na universidade.

4. ADEQUAÇÕES NECESSÁRIAS PARA IMPLEMENTAÇÃO DA POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS NA UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

A implementação da Política Pública de Proteção de Dados representa um desafio significativo para instituições de ensino superior, sendo essencial para garantir a integridade e a privacidade das informações. Este estudo foca nas adaptações necessárias para efetivar essa política na UFRRJ, reconhecendo a complexidade inerente à gestão de dados em um ambiente acadêmico.

A proteção de dados na educação superior tornou-se uma prioridade diante do crescente uso de tecnologias e sistemas que envolvem informações sensíveis de estudantes, docentes e corpo técnico, é importante salientar que esta dissertação focaliza o recorte de pesquisa nos dados pessoais dos estudantes. A implementação de uma política específica é crucial para alinhar a UFRRJ com a LGPD, e assegurar a conformidade legal.

A UFRRJ, como instituição multifacetada, enfrenta desafios específicos na proteção de dados. Isso inclui a diversidade de dados tratados, desde registros acadêmicos até informações de pesquisa. A necessidade de conciliar a transparência acadêmica com a proteção da privacidade cria um cenário complexo que exige adequações específicas em seus processos internos.

A implementação da Política Pública de Proteção de Dados na UFRRJ é um passo crucial para garantir a segurança e privacidade dos dados tratados pela instituição. A adequação visa enfrentar os desafios específicos da universidade, criando um ambiente que concilie eficazmente a transparência acadêmica com a proteção da privacidade individual.

O escopo desta pesquisa concentra-se nos dados pessoais dos estudantes, reconhecendo a sensibilidade dessas informações e a necessidade de abordagem diferenciada no contexto da proteção de dados. Ao analisar de forma específica esse segmento, pretende-se identificar desafios, melhores práticas e eventuais lacunas que merecem atenção especial por parte da instituição.

Portanto, esta dissertação busca contribuir para um entendimento mais aprofundado das questões relacionadas à proteção de dados na educação superior, com

foco específico nos dados pessoais dos estudantes da UFRRJ. Ao fazê-lo, pretende-se não apenas atender às exigências legais, mas também promover um ambiente seguro e ético para o tratamento dessas informações sensíveis no âmbito acadêmico.

A LGPD estabelece, no contexto da universidade, por ser uma autarquia federal de ensino, diretrizes específicas para o tratamento de dados. As principais hipóteses encontram-se nos incisos III e IV do artigo 7º, bem como no inciso II, alíneas b e c do artigo 11 da referida legislação, este último aplicável no caso de dados sensíveis.

O artigo 7º, incisos III e IV, destaca as situações em que a administração pública, como a UFRRJ, pode legitimamente realizar o tratamento de dados. O inciso III autoriza o tratamento e compartilhamento de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, desde que observadas as disposições do Capítulo IV da lei. Já o inciso IV respalda o tratamento para a realização de estudos por órgão de pesquisa, com a ressalva de garantir, sempre que possível, a anonimização dos dados pessoais.

No que tange ao tratamento de dados sem o fornecimento de consentimento do titular, o artigo 11 da LGPD, em seu inciso II, oferece as alíneas b e c como situações em que tal tratamento é indispensável. A alínea b autoriza o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos. Por sua vez, a alínea c respalda a realização de estudos por órgão de pesquisa, com a condição de garantir, sempre que possível, a anonimização dos dados pessoais sensíveis.

Dessa forma, é imperativo que a UFRRJ, ao proceder com o tratamento de dados, esteja em estrita conformidade com as disposições legais da LGPD, especialmente observando as condições específicas delineadas nos artigos mencionados. Essa análise proporciona uma compreensão das bases legais que respaldam as atividades de tratamento de dados na instituição, reforçando a importância da conformidade e do respeito aos princípios estabelecidos pela legislação de proteção de dados pessoais.

No guia orientativo para tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas, a ANPD (2023, pg.20) destaca que

> O tratamento de dados pessoais realizado por instituições de ensino para fins administrativos ou comerciais, ainda que possua algum vínculo indireto com

> ações acadêmicas, deve respeitar integralmente a LGPD. É o caso da coleta de dados pessoais de estudantes para matrículas, estágios, processos seletivos, registros de presença e notas de avaliação ou, ainda, do tratamento de dados pessoais de funcionários e de docentes pelo setor de recursos humanos dessas instituições. Outro exemplo que pode ser mencionado é o tratamento de dados pessoais feito por essas instituições para fins de exibição de anúncios publicitários, o qual deve observar integralmente a LGPD, haja vista a sua natureza de atividade comercial.

Pode-se perceber que a coleta de dados para atividades como matrículas, estágios, controle de presença e avaliação acadêmica não se enquadram nas exceções destinadas às atividades acadêmicas estipuladas na LGPD. É crucial salientar que o foco primordial desta pesquisa recai precisamente sobre a coleta de dados dos estudantes para fins administrativos.

Diante desse contexto, a hipótese de tratamento e compartilhamento de dados que se mostra mais pertinente para embasar as práticas da universidade é aquela referente à execução de políticas públicas. Conforme estabelecido pela normativa, essa hipótese autoriza a administração pública, como a UFRRJ, a realizar o tratamento de dados necessários à execução de políticas públicas previstas em leis, regulamentos, contratos, convênios ou instrumentos congêneres.

Ao adotar essa perspectiva, a pesquisa concentra-se na análise crítica e contextualizada da hipótese legal que melhor se coaduna com a natureza das atividades administrativas da instituição, proporcionando uma base sólida para a definição de diretrizes alinhadas com as normativas. Essa abordagem estratégica contribui para uma interpretação assertiva da legislação, analisando as práticas da universidade em conformidade com os princípios fundamentais da proteção de dados pessoais.

Nesta vertente, a UFRRJ executa política pública educacional, com previsão constitucional[14]. A universidade desempenha um papel crucial na execução de uma política pública educacional, alinhada com os preceitos constitucionais previstos na Carta Magna de 1988. Conforme o Artigo 205 da Constituição Federal, a educação é reconhecida como um direito de todos e um dever do Estado e da família, buscando promover e incentivar o pleno desenvolvimento da pessoa, sua preparação para o

[14] CRFB/88 - Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho. Art. 207. As universidades gozam de autonomia didático-científica, administrativa e de gestão financeira e patrimonial, e obedecerão ao princípio de indissociabilidade entre ensino, pesquisa e extensão.§ 1º É facultado às universidades admitir professores, técnicos e cientistas estrangeiros, na forma da lei. § 2º O disposto neste artigo aplica-se às instituições de pesquisa científica e tecnológica.

exercício da cidadania e sua qualificação para o trabalho.

Destaca-se ainda o princípio da autonomia das universidades, conforme estabelecido no Artigo 207 da CRFB/88, que confere às instituições de ensino superior autonomia didático-científica, administrativa e de gestão financeira e patrimonial. Essa autonomia assegura a capacidade de estabelecer suas diretrizes acadêmicas, administrativas e financeiras, respeitando o princípio da indissociabilidade entre ensino, pesquisa e extensão.

É relevante observar que a legislação educacional brasileira, representada pela Lei nº 9.394/96, conhecida como a Lei de Diretrizes e Bases da Educação Nacional (LDB), consolida as bases da educação no país, estabelecendo as diretrizes gerais para a educação, inclusive no âmbito universitário, e reconhece a indissociabilidade entre ensino, pesquisa e extensão como um princípio orientador das instituições de ensino superior.

Portanto, ao considerar o arcabouço legal que respalda a atuação da UFRRJ, percebe-se que a execução de políticas públicas no campo educacional está intrinsecamente alinhada com sua missão institucional, enfatizando o cumprimento dos propósitos constitucionais e legais que norteiam o sistema educacional brasileiro. Essa compreensão embasa a hipótese de tratamento e compartilhamento de dados para a execução de políticas públicas, respaldando as práticas administrativas da instituição no contexto da LGPD.

Assim, salienta-se que esta seção aborda uma investigação de campo fornecendo um panorama sucinto da instituição em estudo, destacando o cenário atual em relação à adequação e implementação à LGPD, bem como delineia estratégias de ação para alcançar a conformidade. No entanto, antes de adentrar nos detalhes deste estudo, é de suma importância apresentar o desenho metodológico adotado para conduzir a pesquisa.

4.1 - Desenho metodológico: integrando abordagens quantitativas e qualitativas

Este tópico delineia a abordagem metodológica empregada na investigação realizada na UFRRJ durante o período de 2023 a 2024. O estudo adotou uma perspectiva teórico-empírica, transversal e descritiva, fundamentada na interseção entre teoria e prática para oferecer uma compreensão abrangente do fenômeno em análise. A

opção pelo caráter descritivo da pesquisa se justifica pela sua natureza exploratória, buscando identificar e descrever os processos e práticas relacionados à proteção de dados dos discentes da universidade sob análise.

Epistemologicamente, a pesquisa se enquadra no paradigma qualitativo, embora também tenha incorporado elementos quantitativos em sua análise. Segundo Demo (2017, p. 5,6)

> "todo fenômeno qualitativo é dotado também e naturalmente de faces quantitativas e vice-versa. Parto do ponto de vista de que entre quantidade e qualidade não existe dicotomia, pois são faces diferenciadas do mesmo fenômeno. (...) Assim, toda pesquisa qualitativa só tem a ganhar se cuidar também de suas ilações quantitativas, ou melhor dizendo, se souber aliar-se favoravelmente a métodos quantitativos.

A citação enfatiza a interconexão entre os aspectos qualitativos e quantitativos na pesquisa. O Autor argumenta que, embora tradicionalmente vistos como distintos, quantidade e qualidade são na verdade dimensões complementares de um mesmo fenômeno, isso sugere que ambas as abordagens podem locupletar mutuamente uma pesquisa. Ao afirmar que toda pesquisa qualitativa se beneficia ao incorporar elementos quantitativos, Demo destaca a importância da complementaridade entre métodos qualitativos e quantitativos, o que pode enriquecer a compreensão e a análise do fenômeno estudado.

Assim, neste estudo, a utilização de métodos mistos, que incluem tanto técnicas qualitativas quanto quantitativas, é considerada essencial para uma investigação completa e robusta sobre a proteção de dados dos estudantes na UFRRJ. Essa abordagem permite explorar tanto as nuances e percepções qualitativas dos participantes quanto os dados objetivos e mensuráveis, fornecendo uma visão abrangente e fundamentada do fenômeno em análise. Assim destaca John W. Creswell e J. David Creswell (2021, e-book)

> Abordagem de métodos mistos – perspectiva pragmática, coleta sequencial de dados quantitativos e qualitativos. O pesquisador baseia a investigação no pressuposto de que a coleta de diversos tipos de dados proporciona um entendimento mais completo de um problema de pesquisa do que um tipo de dados isoladamente. O estudo começa com um levantamento geral de informações para generalizar os resultados para uma população e, em uma segunda fase, concentra-se em entrevistas qualitativas abertas visando a coletar os detalhes do ponto de vista dos participantes para ajudar a explicar a investigação quantitativa inicial.

O trecho destaca a abordagem de métodos mistos, baseada em uma perspectiva pragmática, que envolve a coleta sequencial de dados quantitativos e qualitativos. Os pesquisadores partem do pressuposto de que a combinação de diferentes tipos de dados oferece uma compreensão mais abrangente de um problema de pesquisa do que apenas um tipo de dados isoladamente.

Nessa abordagem, o estudo inicia com uma coleta geral de informações, geralmente por meio de um levantamento, para generalizar os resultados para uma população maior. Em seguida, na segunda fase, o foco é nas entrevistas qualitativas abertas, que visam capturar os detalhes e nuances do ponto de vista dos participantes. Essas entrevistas ajudam a explicar e aprofundar os resultados obtidos na fase quantitativa inicial, proporcionando uma compreensão mais completa e rica do fenômeno em estudo.

Nesta dissertação, para alcançar os objetivos propostos, foram utilizados métodos mistos, incluindo a aplicação de questionários e entrevistas. De acordo com Demo (2017, p 30-31)

> O questionário fechado será aplicado uma vez só, não permite conversa paralela, insiste em condições aleatórias e acéticas. A entrevista aberta poderá ser repetida até se ter a sensação de que o problema foi bem abordado. (...) A informação qualitativa é, assim, comunicativamente trabalhada e retrabalhada, para que duas condições sejam satisfeitas: do ponto de vista do entrevistado, ter a confiança de que se expressou como queria; do ponto de vista do entrevistador, ter a confiança de que obteve o que procurava ou de que realizou a proposta. Nem sempre se encontra o que se busca, mas é possível pelo menos armar as condições mais favoráveis para tanto, também para evitar "inventar" o dado que se quer, colocando na boca do entrevistado o que o analista quer ouvir.

Demo ressalta as diferenças entre o questionário fechado e a entrevista aberta, enfatizando as vantagens desta última em proporcionar uma interação mais rica e flexível entre o entrevistador e o entrevistado. Enquanto o questionário fechado é limitado por sua natureza estruturada e não permite uma discussão mais aprofundada, a entrevista aberta oferece a oportunidade de repetição e exploração mais detalhada do problema em questão.

O autor destaca a importância da comunicação eficaz na obtenção de informações qualitativas, ressaltando que tanto o entrevistador quanto o entrevistado

devem sentir-se confiantes de que suas necessidades foram atendidas durante o processo. Além disso, ele adverte contra a manipulação dos dados, destacando a importância de criar condições favoráveis para a obtenção de informações autênticas, em vez de forçar respostas que se encaixem nas expectativas do analista. Importante destacar o que preceitua Marco Costa e Fátima Costa (2019, e-book)

> A entrevista é o principal instrumento usado para coletar dados em pesquisas com abordagem qualitativa. A palavra “entrevista” é derivada do francês “entrevue”, que significa o ato de ver um ao outro, e do latim “intervedere”, significando ver entre si. (...) Entrevista Não Estruturada ou Aberta – É aquela em que não existe um roteiro fechado, apenas uma pauta. As perguntas são abertas e é desenvolvida no contexto de uma conversação. Ela é flexível tanto para o entrevistador, quanto para o entrevistado. (...) Questionário é uma palavra derivada do latim “quaestionarius”, que significa ação de buscar, interrogar. O questionário é uma das técnicas mais utilizadas, tanto em estudos com abordagem qualitativa, quanto naqueles com abordagem quantitativa. É um instrumento de coleta de dados, aplicado quando se quer atingir um grande número de indivíduos. (...) A grande vantagem do questionário, como instrumento de coleta de dados, é a sua capacidade de atingir um grande número de pessoas.

Os autores destacam a importância da entrevista como principal instrumento de coleta de dados em pesquisas qualitativas. Eles explicam que a palavra "entrevista" tem origem no francês e no latim, significando o ato de ver um ao outro, enfatizando a natureza interativa desse método. A entrevista não estruturada ou aberta é descrita como aquela em que não há um roteiro fechado, permitindo uma conversa mais flexível e contextualizada entre o entrevistador e o entrevistado, formato este adotado nesta dissertação.

Quanto ao questionário, os autores explicam sua utilidade tanto em estudos qualitativos quanto quantitativos, destacando sua capacidade de alcançar um grande número de respondentes. A principal vantagem do questionário é sua eficácia em atingir uma ampla amostra da população-alvo.

Nesta pesquisa, os questionários permitiram a coleta de dados quantitativos sobre as percepções e conhecimentos dos estudantes em relação à proteção de dados, enquanto as entrevistas proporcionaram percepções qualitativas mais profundas da gestão e de servidores, permitindo uma compreensão abrangente das práticas e desafios enfrentados pela universidade.

A combinação desses métodos possibilitou uma abordagem ampla da questão em estudo, contribuindo para uma análise mais completa e fundamentada. Os resultados

obtidos foram então analisados e interpretados à luz da revisão teórica realizada previamente, permitindo a elaboração de conclusões embasadas e recomendações relevantes para aprimorar a proteção de dados na UFRRJ.

4.2 - Panorama conciso da Universidade Federal Rural do Rio de Janeiro

A presente dissertação tem como objeto de estudo a UFRRJ, e, nesse contexto, torna-se imperativo a elaboração de um panorama conciso sobre esta instituição de ensino superior. Assim, para uma análise mais precisa, foi utilizado o Relatório de Gestão 2022 (UFRRJ,2022), que relata que esta é uma instituição pública e gratuita de ensino, pesquisa e extensão localizada no município de Seropédica, na Baixada Fluminense, com campus adicionais em Nova Iguaçu, Três Rios e Campos dos Goytacazes. Seu principal propósito é promover o desenvolvimento científico, tecnológico, artístico e cultural no país, contribuindo para a formação de profissionais autônomos e capacitados para atuar nos diversos campos do conhecimento.

O relatório informa que a UFRRJ desempenha um papel crucial na disseminação do conhecimento, formando e diplomando indivíduos em diferentes níveis e áreas. Além disso, busca estimular o pensamento crítico e reflexivo, impulsionando o desenvolvimento local, regional e nacional. A instituição, autarquia de regime especial vinculada ao Ministério da Educação (MEC), tem origens que remontam a 1910, com a criação da Escola Superior de Agricultura e Medicina Veterinária (ESAMV).

Prossegue destacando que ao longo dos anos, a UFRRJ passou por transformações significativas, tornando-se uma universidade em 1943, com diversas reorganizações subsequentes. Em 1967, foi transferida para o MEC, assumindo a denominação atual. A instituição possui uma ampla gama de cursos e áreas de estudo, adaptando-se às demandas dos municípios onde está presente.

O Programa de Apoio a Planos de Reestruturação e Expansão das Universidades Federais (REUNI), implementado em 2007, marcou um momento importante em sua história, resultando na criação de novos cursos e campus, como os de Nova Iguaçu e Três Rios. Além disso, a UFRRJ incorporou o campus de Campos dos Goytacazes em 1991, dedicado especialmente a atividades de pesquisa na área sucroalcooleira.

Atualmente, a universidade é composta por 12 Institutos, 50 departamentos

acadêmicos, 38 coordenações de graduação, 34 coordenações de pós-graduação e um Colégio Técnico de Ensino Básico, Técnico e Tecnológico. Seu compromisso com a pesquisa e o ensino é evidenciado por sua estrutura acadêmica diversificada, abrangendo diferentes campos de estudo. Para uma compreensão mais ampla, é pertinente apresentar a linha do tempo que percorre desde a criação da ESAMV até os dias atuais.

Figura 1 - Linha do tempo: UFRRJ - Da ESAMV à Atualidade

Fonte: Relatório de gestão 2022 (UFRRJ, 2022)

Com base nos dados fornecidos na figura 1, verifica-se que a UFRRJ conta com uma comunidade estudantil extensa. Nesse contexto, torna-se imprescindível a conformidade com a LGPD para assegurar o tratamento seguro das informações pessoais desses estudantes. Para iniciar a análise quanto à adequação à lei, primeiramente foi averiguado o site institucional, com o intuito de verificar se a autarquia federal de ensino já disponibiliza as informações de contato do encarregado de dados, bem como, se há outras informações quanto a LGPD para a comunidade acadêmica.

Neste sentido, o site institucional da UFRRJ é uma ferramenta de extrema importância, sendo uma vitrine virtual que fornece informações relevantes sobre a instituição para o público, incluindo estudantes, docentes, colaboradores e a comunidade em geral. Nesse contexto, a disponibilidade de informações claras e acessíveis sobre o encarregado de dados, conforme estabelecido pela LGPD, é crucial para demonstrar o comprometimento da universidade com a transparência e a

conformidade legal no tratamento de dados pessoais.

A seção dedicada ao encarregado de dados no site institucional deve conter dados essenciais, como o nome completo do encarregado, suas formas de contato, como endereço de e-mail e telefone, além de esclarecimentos sobre a função desempenhada por essa figura na proteção dos dados pessoais dos estudantes. Essas informações devem ser apresentadas de maneira clara, direta e de fácil acesso, possibilitando que os usuários do site, especialmente os titulares dos dados, possam contatá-lo quando necessário.

A página dedicada ao encarregado no site institucional pode incluir informações sobre os direitos dos titulares de dados, orientações sobre como realizar solicitações relacionadas à privacidade, e esclarecimentos sobre como a instituição de ensino está comprometida em garantir a segurança e a privacidade das informações pessoais dos estudantes.

Dessa forma, a presença de informações sobre o encarregado no site institucional não apenas atende aos requisitos legais estabelecidos pela LGPD, mas também fortalece a cultura de transparência da instituição, proporcionando confiança aos membros da comunidade acadêmica e reforçando o compromisso da UFRRJ com a proteção de dados pessoais. Neste sentido a lei preceitua que:

> Art. 5º Para os fins desta Lei, considera-se: (...) VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (...) Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: (...) III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei. (...) Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e

> o porte da entidade ou o volume de operações de tratamento de dados.

Os artigos citados da LGPD destacam a figura do encarregado, desempenhando um papel crucial na operacionalização e conformidade do tratamento de dados pessoais. Este, conforme definido no artigo 5º, é a pessoa indicada pelo controlador e operador para servir como um elo de comunicação entre o controlador, os titulares dos dados e a ANPD.

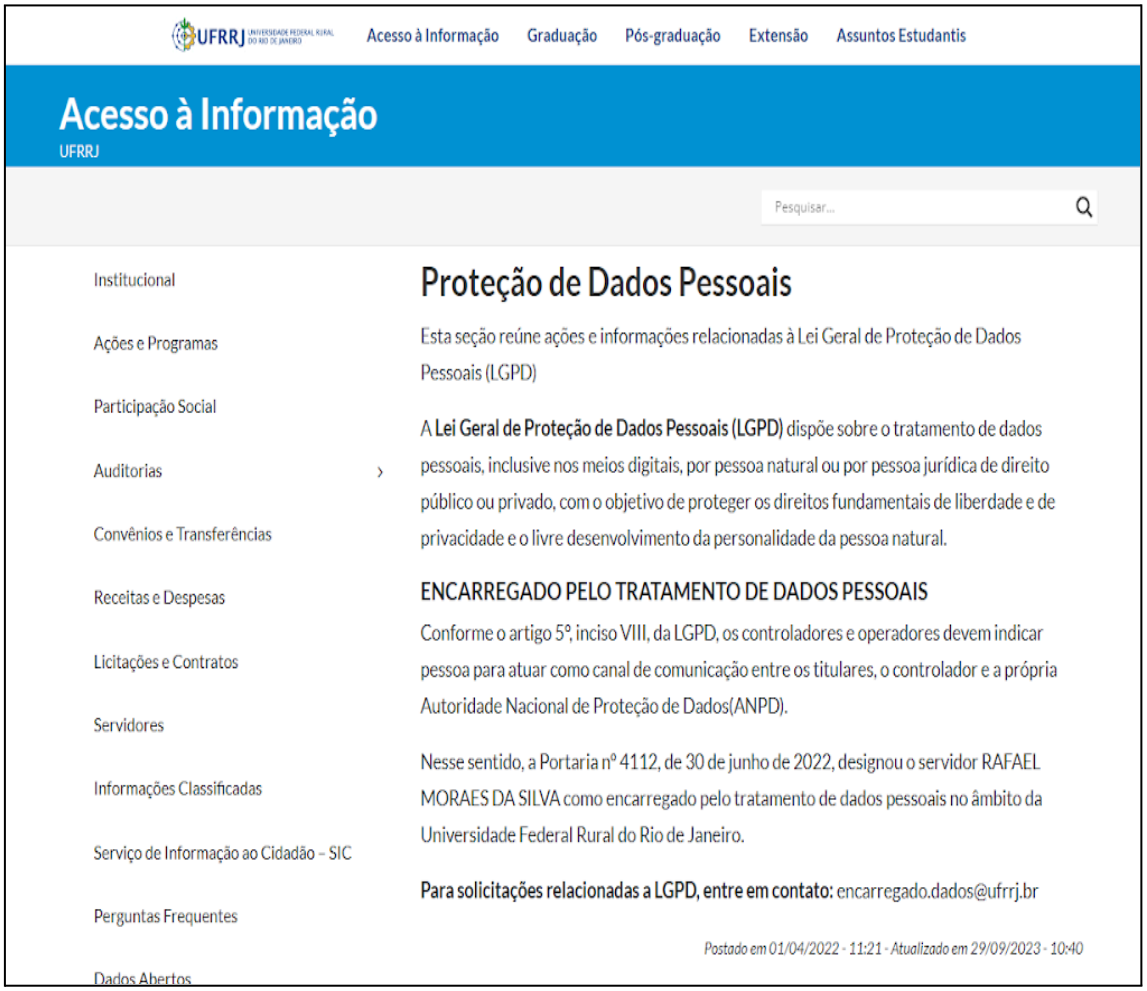
O artigo 41 da LGPD reforça a obrigatoriedade de indicação de um encarregado pelo controlador, estabelecendo claramente suas responsabilidades e atividades. Essa indicação não apenas fortalece a transparência no tratamento de dados pessoais, mas também assegura que os titulares dos dados tenham um ponto de contato para esclarecimentos, reclamações e comunicações.

A divulgação pública da identidade e informações de contato do encarregado, conforme exigido pelo parágrafo 1º do artigo 41, reforça a transparência e a acessibilidade desse profissional, promovendo a confiança dos titulares dos dados. Além disso, o parágrafo 2º enumera as atividades do encarregado, indo desde a recepção de reclamações até a orientação dos funcionários da entidade sobre práticas relacionadas à proteção de dados pessoais.

A flexibilidade concedida à Autoridade Nacional, conforme expresso no parágrafo 3º, permite a adaptação das normas relacionadas à definição e atribuições do encarregado com base na natureza e porte da entidade ou no volume de operações de tratamento de dados. Isso reconhece a diversidade de contextos nos quais a LGPD é aplicada, permitindo uma abordagem proporcional às necessidades específicas de cada organização.

Em síntese, a LGPD enfatiza a importância do encarregado como um agente central na proteção de dados pessoais, promovendo a transparência, responsabilidade e comunicação eficaz na cadeia do tratamento de dados, e assim sendo, a UFRRJ já se adequou a exigência legal de nomear um encarregado de dados e de apresentar em seu site as informações sobre este, o que pode ser verificado na figura 2.

Figura 2: Proteção de Dados Pessoais UFRRJ



Fonte: Acesso à Informação (UFRRJ, 2023)

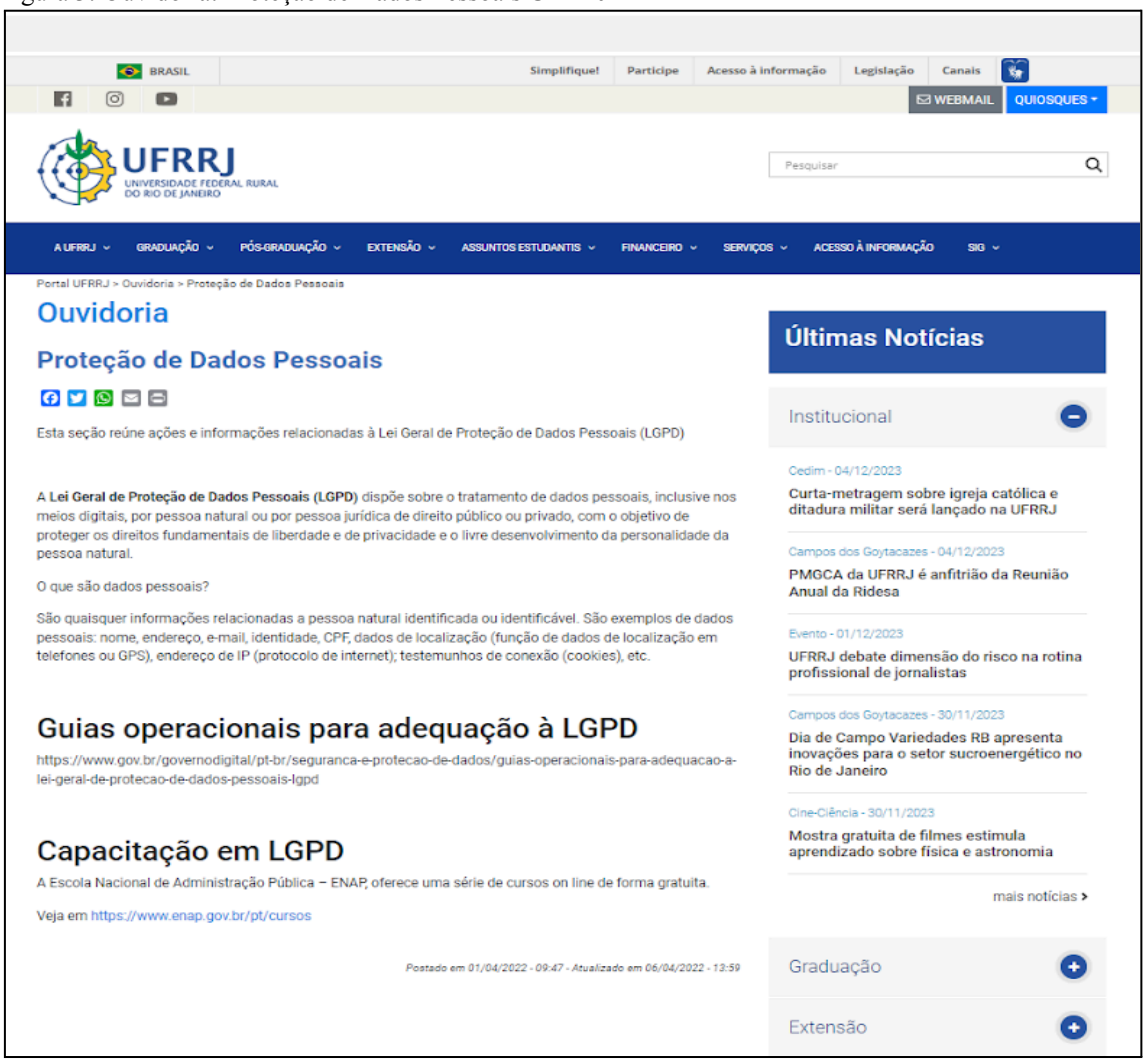
A constatação proporcionada pela Figura 2 revela que o servidor Rafael Moraes da Silva é o encarregado pela proteção de dados pessoais na UFRRJ. Essa designação foi formalizada por meio da Portaria nº 4112, datada de 30 de julho de 2022. Isto evidencia o compromisso da universidade em atender às diretrizes da LGPD. A escolha de um servidor para ocupar esse papel destaca a importância de um profissional capacitado e envolvido com a instituição para liderar iniciativas sobre proteção de dados.

O e-mail disponibilizado, encarregado.dados@ufrrj.br, proporciona um canal direto para contato com o encarregado, garantindo uma comunicação acessível aos titulares dos dados e demais partes interessadas. Essa transparência no fornecimento de informações de contato é uma prática fundamental para promover a comunicação efetiva entre os envolvidos e para atender às expectativas de transparência estabelecidas pela LGPD.

Portanto, a UFRRJ, ao apresentar de maneira explícita e acessível a identidade

do encarregado, sua designação oficial e as informações de contato, demonstra uma abordagem comprometida e transparente em relação à proteção de dados pessoais, cumprindo assim um dos requisitos legais e promovendo a confiança dos titulares de dados na instituição. Ato contínuo cabe destacar a figura 3 sobre o site da Ouvidoria da UFRRJ.

Figura 3: Ouvidoria: Proteção de Dados Pessoais UFRRJ



Fonte: Ouvidoria (UFRRJ, 2022)

É possível constatar pela figura 3 que no site da Ouvidoria da UFRRJ, estão disponíveis informações referentes à LGPD e à definição de dados pessoais. O site também disponibiliza um link para acessar os guias operacionais destinados à adequação à LGPD, hospedados no Gov.br, bem como um link para acessar a Capacitação em LGPD oferecida pela Escola Nacional de Administração Pública (ENAP). Contudo, é importante avaliar se essas iniciativas são suficientes para garantir

a conformidade total com a legislação e promover a conscientização adequada entre os envolvidos.

4.3 - O cenário atual da Universidade quanto à adequação e implementação da lei

Este tópico contempla a descrição do estudo de campo conduzido na UFRRJ, no qual os dados colhidos durante a pesquisa empírica serão apresentados. A análise será baseada nos questionários preenchidos pelos estudantes e nas informações obtidas por meio de entrevistas com o encarregado de dados e setores estratégicos responsáveis pela salvaguarda dos dados pessoais dos estudantes na instituição. A abordagem do estudo compreenderá uma avaliação do atual panorama da UFRRJ, visando proporcionar uma compreensão abrangente do cenário institucional no que concerne à proteção de dados.

Inicialmente, uma análise minuciosa foi conduzida no site institucional, com foco na avaliação da conformidade quanto às informações relacionadas ao encarregado. Essa análise buscou verificar se o site fornece de maneira clara e acessível todas as informações pertinentes sobre este, conforme preconizado pela LGPD.

Dessa maneira, a investigação compreende tanto a percepção dos estudantes por meio dos questionários, quanto a visão interna da instituição obtida por meio de entrevistas, proporcionando uma abordagem abrangente e multifacetada no exame da proteção de dados na UFRRJ. Essa análise será instrumental para identificar áreas de conformidade e eventuais lacunas que requerem atenção para assegurar a integridade e privacidade dos dados pessoais dos estudantes.

4.3.1 - Análise do questionário aplicado aos Estudantes: o titular de dados e o conhecimento da LGPD

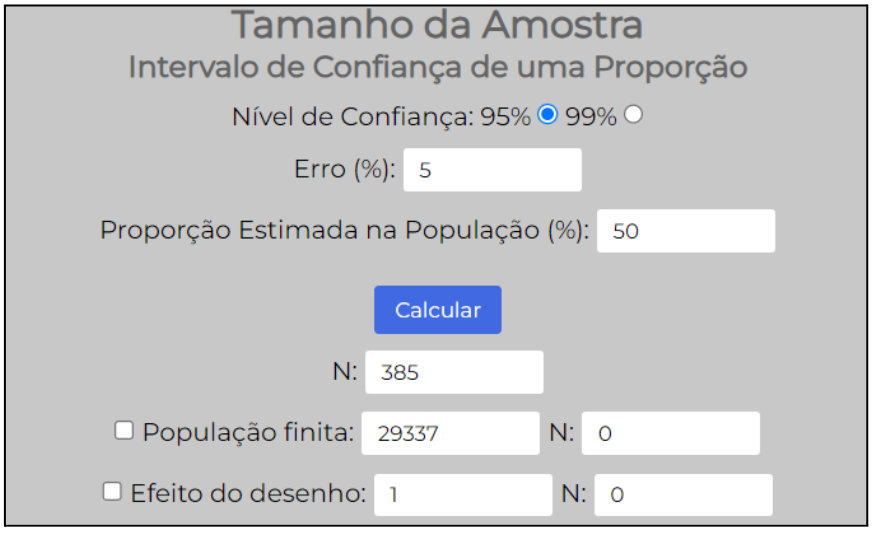
Tendo em vista a delimitação do tema, qual seja, proteção dos dados pessoais dos estudantes da UFRRJ, fez-se necessário verificar qual o conhecimento dos titulares dos dados sobre o tratamento de suas informações pessoais pela instituição. Com o intuito de efetuar a aludida investigação a pesquisadora elaborou um questionário, o mesmo foi aplicado aos estudantes da entidade de ensino através de Qr-code distribuído aos estudantes pela pesquisadora no campus de Seropédica, bem como, foram utilizados

grupos de WhatsApp cujo os membros são majoritariamente alunos da UFRRJ, nestes grupos foi disponibilizado o link para preenchimento do formulário.

De acordo com o catálogo institucional da UFRRJ/2021[15], o número de estudantes é 29.337 (vinte e nove mil, trezentos e trinta e sete), sendo 27.300 (vinte e sete mil e trezentos) da graduação e 2.037 (dois mil e trinta e sete) da pós-graduação, com 56 (cinquenta e seis) cursos de graduação, 2 (dois) cursos de graduação a distância, 29 (vinte e nove) cursos de mestrado acadêmico, 8 (oito) cursos de mestrado profissional e 17 (dezessete) cursos de doutorado.

Para obter a amostragem correta foi utilizada a calculadora amostral da USP, o cálculo empregado foi o Intervalo de Confiança de uma Proporção[16], tendo 95% (noventa e cinco por cento) como nível de confiança, 5% (cinco por cento) de erro, 50% (cinquenta por cento) de proporção estimada na população e 29.337 (vinte e nove mil, trezentos e trinta e sete) de população finita, assim o resultado para a amostragem foi de 385 (trezentos e oitenta e cinco) estudantes, conforme demonstrado na figura 4, foram obtidas 532 (quinhentas e trinta e duas) respostas ao formulário aplicado.

Figura 4: Calculadora amostral/USP



Fonte: Cálculo Amostral (USP, 2023)

[15] Em contato com a Coordenadoria de Comunicação Social (CCS) foi informado que a nova edição do catálogo institucional ainda está em fase de elaboração.

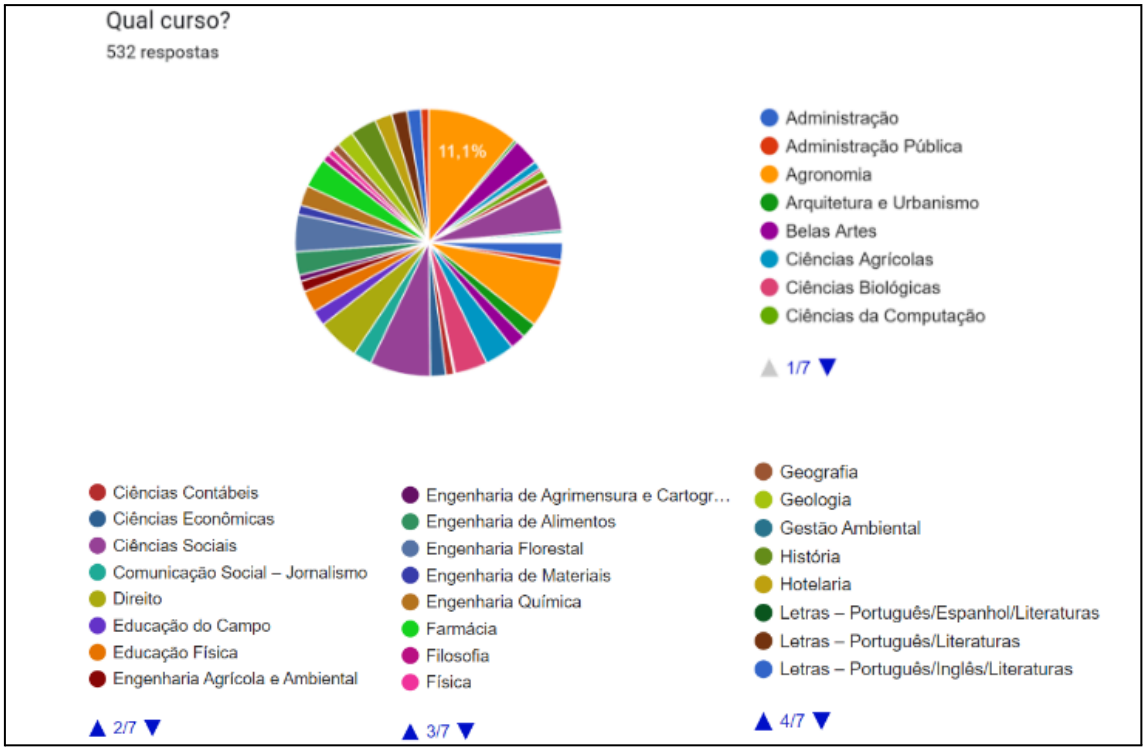
[16] USP: Para calcular o tamanho da amostra são necessárias as seguintes informações:
- Erro (%): margem de erro máximo que o pesquisador admite na sua pesquisa.
- Proporção esperada (%): a proporção (prevalência) que o pesquisador estima que vai encontrar na população com a caraterística sendo estudada. Essa estimativa pode vir da literatura, de um projeto piloto, ou adotar 50% que é a maior variabilidade possível, pois assim o tamanho da amostra calculado atenderá para qualquer que seja a prevalência encontrada.

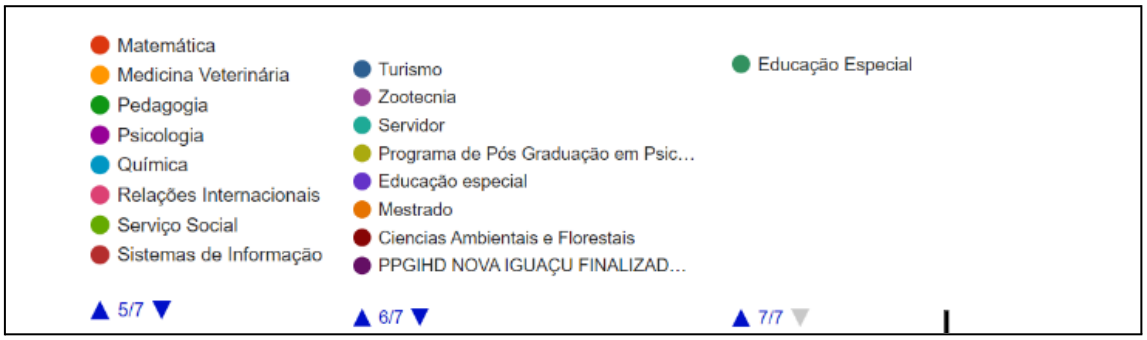
O questionário informava que o intuito era analisar se os estudantes da UFRRJ possuem conhecimento sobre a importância da proteção de seus dados pessoais, destacava ainda que o preenchimento era anônimo e as respostas seriam utilizadas exclusivamente para fins acadêmicos, solicitando uma resposta, pessoal e sincera.

Este continha 9 (nove) perguntas, quais sejam: (i) Você é estudante da Universidade Federal Rural do Rio de Janeiro?; (ii) Qual campus?; (iii) Qual curso?; (iv) Qual o grau acadêmico?; (v)Você conhece a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais?; (vi) Você tem conhecimento de quais são os seus dados pessoais que a UFRRJ possui?; (vii) Você sabe quais são os setores da UFRRJ que podem acessar seus dados pessoais?; (viii) Você sabe quem é o encarregado pelo tratamento de dados da UFRRJ?; (ix) Você sabe como entrar em contato com o encarregado pelo tratamento de dados da UFRRJ?

A primeira pergunta tem o intuito de garantir que o questionário fosse respondido pelos estudantes da instituição. Já as dois, três e quatro é para garantir a abrangência da pesquisa, verificando se a mesma atingiu todos os campus, diversos cursos e grau acadêmico dos estudantes. E nestes aspectos, tendo em vista que a universidade possui 112 cursos entre graduação e pós-graduação, o questionário foi bem sucedido, como é possível verificar na figura 5, sendo este o gráfico da terceira questão.

Figura 5: Questionário - 3ª Pergunta

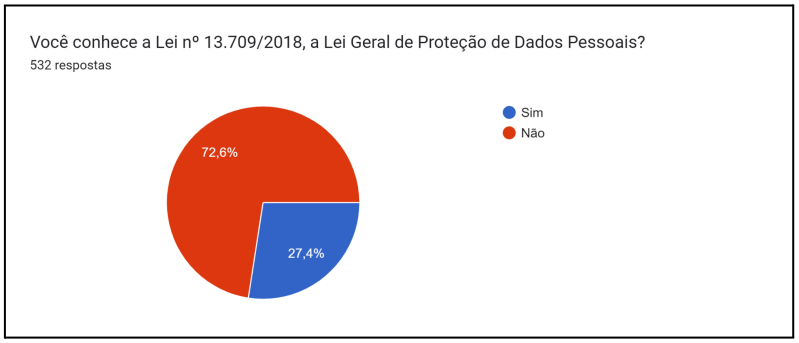




Fonte: Elaborado pela pesquisadora

Da quinta à nona pergunta a ênfase foi na temática da pesquisa. A quinta pergunta busca analisar se os alunos conhecem a LGPD, das 532 (quinhentas e trinta e duas) respostas, 72,6% (setenta e dois inteiros e seis décimos por cento) não conhecem, e 27,4% (vinte e sete inteiros e quatro décimos por cento) conhecem, como é possível verificar na figura 6, o que comprova que a maioria dos estudantes como titulares de dados desconhecem a legislação que lhe conferem direitos quanto ao tratamento de seus dados pessoais.

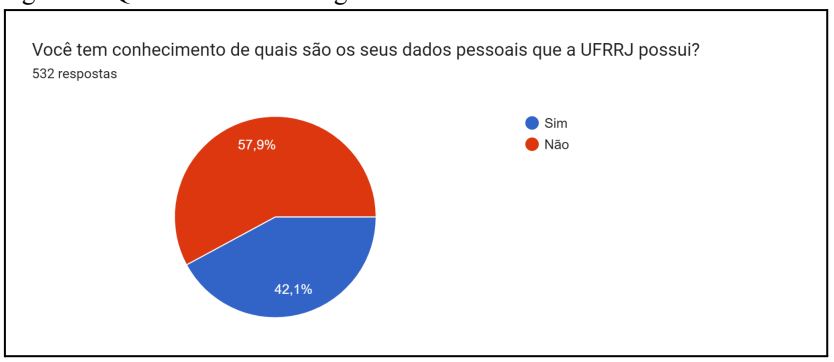
Figura 6: Questionário - 5ª Pergunta



Fonte: Elaborado pela pesquisadora

Foi também questionado se os estudantes têm conhecimento de quais são os seus dados pessoais que a UFRRJ possui, como é possível verificar na figura 7, 57,9% (cinquenta e sete inteiros e nove décimos por cento) tem conhecimento e 42,1% (quarenta e dois inteiros e um décimo por cento) não tem conhecimento.

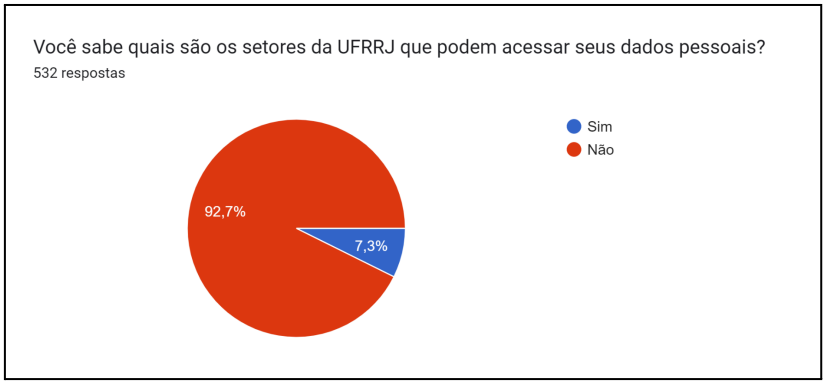
Figura 7 - Questionário - 6ª Pergunta



Fonte: Elaborado pela pesquisadora

Após questionar se os estudantes conheciam a legislação, foi crucial saber se os mesmos tinham conhecimento sobre alguns direitos básicos dos titulares de dados. A sétima pergunta indaga se sabem quais os setores da UFRRJ podem acessar seus dados, 92,7% (noventa e dois inteiros e sete décimos por cento) informaram que não e 7,3% (sete inteiros e três décimos por cento) informaram que sim. É o que demonstra a figura 8.

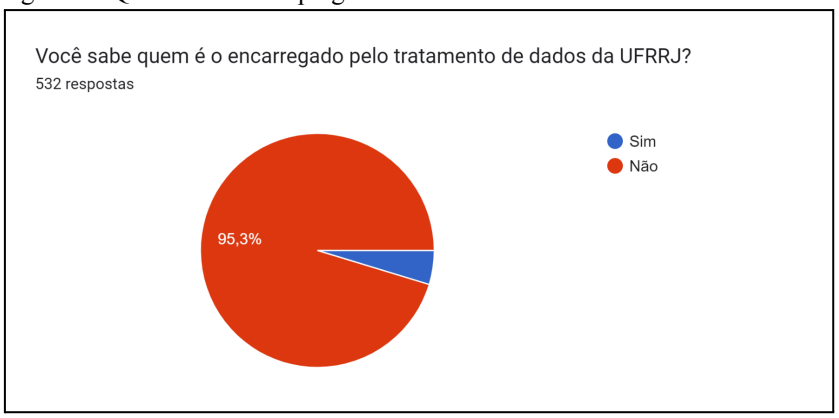
Figura 8 - Questionário - 7ª Pergunta



Fonte: Elaborado pela pesquisadora

Neste mesmo sentido, a 8ª pergunta questiona se os estudantes sabem quem é o encarregado pelo tratamento de dados da instituição, e na mesma vertente das respostas anteriores, há desconhecimento por parte da maioria dos estudantes, 95,3% (noventa e cinco inteiros e três décimos por cento) não sabe quem é o encarregado e 4,7% (quatro inteiros e sete décimos por cento) sabe quem é o encarregado.

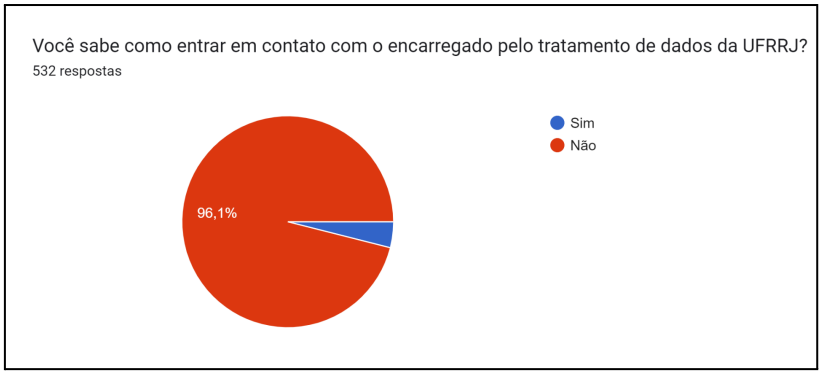
Figura 9 - Questionário - 8ª pergunta



Fonte: Elaborado pela pesquisadora

A 9º pergunta foi realizada com o intuito de verificar se os estudantes saberiam como entrar em contato com o encarregado, vez que o contato deve estar disponibilizado no site institucional de acordo com o artigo 41, §1º da LGPD, porém, 96,1% (noventa e seis inteiros e um décimo por cento) não sabem como entrar em contato com o encarregado e 3,9% (três inteiros e nove décimos por cento) sabem como entrar em contato.

Figura 10 - Questionário - 9ª pergunta



Fonte: Elaborado pela pesquisadora

Pela amostragem é possível verificar que os estudantes não conhecem a LGPD. Efetuando uma análise das respostas fica nítido que os alunos que conhecem a legislação acabam desconhecendo quais são os seus dados pessoais tratados pela instituição, entretanto, tais dados são fornecidos pelo próprio aluno no momento da matrícula ou na execução de alguma atividade, o que demonstra a necessidade da mudança cultural quanto ao fornecimento dos dados pessoais, vez que o titular de dados, deveria ter ciência de quais dados tem fornecido aos controladores, pois muitas

vezes estes não são compartilhados entre empresas/órgãos públicos, mas são fornecidos pelo próprio titular.

Ocorre que também foi possível verificar em um primeiro momento, de acordo com análise das respostas, que a UFRRJ não efetua divulgação a respeito da LGPD entre os seus estudantes, de forma que consta no site a informação sobre o encarregado de dados, mas esta não alcança os titulares. Bem como, não há informação sobre quais setores podem ter acesso aos dados tratados pela instituição.

Durante a aplicação do formulário alguns estudantes fizeram considerações à pesquisadora informando que antes de responder a pesquisa desconheciam totalmente o tema. Outros discentes manifestaram a intenção de adquirir mais conhecimento sobre os seus dados pessoais. Logo, a avaliação da investigação foi positiva, uma vez que logrou êxito em verificar se os estudantes da UFRRJ têm conhecimento sobre a legislação e a importância dos seus dados pessoais.

4.3.2 - Investigando o contexto institucional: uma abordagem estratégica

No intuito de aprofundar a compreensão do contexto da UFRRJ durante o processo de adequação à LGPD, foram conduzidas entrevistas e aplicação de questionário a gestores e servidores de setores estratégicos da instituição. Este enfoque metodológico foi adotado visando obter insights valiosos diretamente daqueles que desempenham papéis cruciais na gestão e implementação das medidas relacionadas à proteção de dados na universidade.

A iniciativa de entrevistar gestores e servidores de setores estratégicos reflete a importância atribuída à compreensão das práticas, desafios e estratégias adotadas durante o processo de adaptação à LGPD na UFRRJ. Dessa forma, busca-se não apenas identificar as medidas técnicas implementadas, mas também compreender as nuances organizacionais e os aspectos práticos da conformidade com a legislação de proteção de dados.

As entrevistas e a aplicação do questionário foram estruturadas de maneira a abranger temas relevantes, como as políticas internas adotadas, os procedimentos de coleta e tratamento de dados, a conscientização dos colaboradores e os desafios enfrentados. A análise das respostas obtidas nas entrevistas contribuirá para uma visão abrangente do panorama da UFRRJ em relação à conformidade com a lei, destacando

ações eficazes, pontos de aprimoramento e, por conseguinte, promovendo um entendimento mais completo das práticas de proteção de dados na instituição.

No estágio inicial desta pesquisa, foram abordados dois profissionais de relevância estratégica na UFRRJ. Thais Alves Gallo Andrade, ocupante do cargo de Pró-reitora Adjunta da Pró-Reitoria de Planejamento, Avaliação e Desenvolvimento Institucional (PROPLADI) que respondeu ao questionário. E foi conduzida entrevista com Rafael Moraes da Silva, designado como encarregado de dados da instituição, conforme estabelecido pela Portaria nº 4112/2022.

A escolha baseou-se na importância de suas funções e responsabilidades dentro da universidade. Como Pró-reitora Adjunta, Thais Alves Gallo Andrade desempenha um papel crucial na formulação de estratégias institucionais, enquanto Rafael Moraes da Silva, na posição de encarregado de dados, é diretamente responsável por coordenar as atividades relacionadas à proteção e tratamento adequado dos dados em conformidade com as diretrizes estabelecidas pela LGPD.

O estudo de campo foi delineado com o propósito de obter uma perspectiva detalhada sobre a abordagem da UFRRJ em relação à lei. Ao explorar as experiências e visões desses profissionais, almeja-se compreender não apenas os aspectos técnicos, mas também as estratégias organizacionais e os desafios enfrentados durante o processo de adaptação à legislação de proteção de dados. As informações colhidas contribuirão significativamente para uma análise abrangente do panorama da instituição em relação à normativa.

Num estágio subsequente da pesquisa, foram realizadas entrevistas com uma equipe composta por profissionais-chave da UFRRJ no que tange ao desenvolvimento deste trabalho. O Coordenador da Coordenadoria de Tecnologia da Informação e Comunicação (COTIC) foi um dos entrevistados, juntamente com a servidora atualmente responsável pela segurança da informação, também lotada na COTIC. Adicionalmente, foram ouvidos a servidora encarregada pelo Núcleo de Governança de Integridade (NGI) e um servidor lotado na Pró-Reitoria de Graduação. Vale destacar que, diferentemente do primeiro grupo de entrevistados, os nomes dos servidores deste segundo bloco não serão divulgados, por opção da pesquisadora em manter o anonimato.

A escolha desses entrevistados reflete a intenção de abranger diferentes

perspectivas e áreas-chave relacionadas à gestão de dados, segurança da informação e governança de integridade na UFRRJ. O Coordenador da COTIC e a servidora responsável pela segurança da informação proporcionaram insights sobre as práticas e desafios específicos no âmbito tecnológico e de proteção de dados na instituição. A servidora encarregada pelo NGI contribuiu com informações relacionadas à governança e integridade, enquanto a conversa com o servidor da Pró-Reitoria de Graduação permitiu uma visão mais ampla da forma de coleta dos dados dos estudantes.

A opção por não divulgar os nomes dos servidores visa garantir a confidencialidade e privacidade. Essas entrevistas constituem uma parte crucial da pesquisa, fornecendo uma visão abrangente das abordagens, desafios e práticas adotadas pela UFRRJ no contexto da adequação à legislação.

4.3.2.1 - Questionário aplicado a Pró-reitora Adjunta da PROPLADI

Segue abaixo as perguntas e respostas do questionário aplicado à Thais Alves Gallo Andrade, Pró-reitora Adjunta da Propladi e desenvolvido pela pesquisadora. Vale ressaltar que, em razão da agenda da Pró-reitora, não foi viável realizar a entrevista. Devido à relevância para os propósitos da pesquisa, optou-se pela aplicação do formulário. O objetivo foi captar a percepção da alta gestão acerca da importância da LGPD:

i. **Pesquisadora:** Qual a importância da Propladi na estrutura da UFRRJ?

   Pró-reitora Adjunta: É responsável por pensar a Universidade e propor melhorias na sua estrutura, além de ser responsável por obras, TI, planejamento estratégico institucional e orçamento.

ii. **Pesquisadora:** A Propladi é a Pró-reitoria responsável pelo tratamento de dados na instituição, desta forma, como está a adequação à Lei Geral de Proteção de Dados?

   Pró-reitora Adjunta: No PDI 2023-2024 inserimos como um dos objetivos. Igualmente, está sendo realizado planejamento para sua implantação e implementação.

iii. **Pesquisadora:** Qual o plano de ação para a adequação à LGPD?

   Pró-reitora Adjunta: Estamos finalizando o Plano de Ação para o

Planejamento para sua implantação e implementação em janeiro de 2024.

iv. **Pesquisadora:** A Propladi já efetuou algum curso de capacitação dos servidores quanto ao tratamento de dados à luz da LGPD?

Pró-reitora Adjunta: Não.

v. **Pesquisadora:** Se sim, quais foram os cursos de capacitação?

Pró-reitora Adjunta: Ainda não há respostas para esta pergunta.

vi. **Pesquisadora:** Se não, há pretensão de realizar esta capacitação?

Pró-reitora Adjunta: Sim

vii. **Pesquisadora:** Na pesquisa realizada entre os estudantes, a maioria desconhece a LGPD, não sabem quem é o encarregado de dados e como entrar em contato com o mesmo. A Propladi já efetuou alguma campanha de conscientização para os titulares de dados na instituição?

Pró-reitora Adjunta: Não

viii. **Pesquisadora:** Se sim, quais campanhas de conscientização?

Pró-reitora Adjunta: Ainda não há respostas para esta pergunta.

ix. **Pesquisadora:** Se não, há pretensão de realizar tal conscientização?

Pró-reitora Adjunta: Sim.

x. **Pesquisadora:** A UFRRJ já implementou ou pretende implementar regras de boa prática e governança de acordo com a LGPD?

Pró-reitora Adjunta: Sim.

xi. **Pesquisadora:** Quais os maiores desafios para a adequação da UFRRJ a LGPD?

Pró-reitora Adjunta: Tempo, qualificação, dinheiro e mão de obra.

xii. **Pesquisadora:** A UFRRJ já implementou os princípios e diretrizes de governança de acordo com o decreto n^{0} 9203/2017?

Pró-reitora Adjunta: Não.

xiii. **Pesquisadora:** Se sim, quais são as regras implementadas?

Pró-reitora Adjunta: Ainda não há respostas para esta pergunta.

xiv. **Pesquisadora:** Quais os maiores desafios para a implementação das regras de governança?

Pró-reitora Adjunta: Criar a política de governança e definir princípios e diretrizes.

As respostas formuladas pela Pró-reitora Adjunta da Propladi proporcionam uma visão importante sobre a posição e as ações da UFRRJ em relação à LGPD e a governança institucional. Destacam-se alguns pontos-chave que merecem análise.

A Pró-reitora Adjunta enfatiza o papel amplo da Propladi na UFRRJ, descrevendo suas responsabilidades abrangentes, que incluem a gestão de obras, Tecnologia da Informação, planejamento estratégico institucional e orçamento. Essa amplitude de atribuições coloca a Propladi em uma posição estratégica para influenciar e implementar práticas relacionadas à LGPD.

Em relação à adequação à LGPD, a Pró-reitora Adjunta destaca a inclusão desse tema no Plano de Desenvolvimento Institucional (PDI) 2023-2024, indicando um reconhecimento formal da importância dessa legislação para a instituição. O planejamento para a implantação e implementação da LGPD está em andamento, com um plano de ação previsto para janeiro de 2024.

No entanto, alguns desafios são evidenciados, como a falta de capacitação dos servidores sobre o tratamento de dados à luz da LGPD. Embora haja a intenção de realizar essa capacitação, a ausência de cursos até o momento indica uma lacuna que precisa ser abordada para garantir uma implementação eficaz.

A conscientização dos estudantes sobre a LGPD também é uma preocupação, conforme revelado pela pesquisa aplicada aos estudantes. A falta de campanhas de conscientização até o momento é reconhecida, mas a intenção de promover essas iniciativas demonstra um comprometimento futuro.

Quanto à implementação de regras de boa prática e governança de acordo com o Decreto n^{0} 9203/2017, a resposta sugere que essa etapa ainda não foi alcançada, mas existe a intenção de estabelecer políticas e definir princípios e diretrizes.

Finalmente, os maiores desafios para a adequação à LGPD e a implementação das regras de governança são apontados como tempo, qualificação, recursos financeiros e mão de obra. Esses desafios destacam a complexidade da tarefa e a necessidade de abordagens estratégicas e recursos adequados.

Em resumo, as respostas revelam que há intenção de adequar a UFRRJ às exigências estabelecidas pela LGPD, bem como, há pretensão da implementação de boas práticas e governança, entretanto, destaca desafios que exigirão esforços coordenados e estratégias que deverão ser adotadas. Assim, diante deste contexto, para melhor compreensão do cenário apresentado, foi realizada entrevista com o encarregado

de dados da instituição. Salienta-se que consta no site institucional a nomeação do encarregado e a divulgação do contato, o que constitui uma boa prática já realizada pela instituição de ensino.

4.3.2.2 - Entrevista com o Encarregado de Dados da UFRRJ

A entrevista com o Encarregado de Dados da UFRRJ, Rafael Moraes da Silva, designado pela Portaria nº 4112/2022, foi efetuada através de sala de reunião virtual, onde estavam presentes o encarregado e a pesquisadora, na ocasião a entrevista foi gravada e revelou-se extremamente produtiva e esclarecedora. Durante o diálogo, foram abordados diversos aspectos relacionados à implementação da política pública de proteção de dados na universidade.

Rafael tem formação multidisciplinar, sendo advogado especialista em privacidade e proteção de dados e bacharel em sistema da informação. Trouxe percepções valiosas sobre as práticas atuais da instituição no que diz respeito ao tratamento de dados pessoais. Sua experiência e conhecimento aprofundado sobre as diretrizes da LGPD contribuíram significativamente para o entendimento do panorama atual e para a identificação de áreas que demandam atenção especial.

A entrevista não apenas ofereceu uma visão abrangente dos desafios enfrentados pela universidade no processo de conformidade com a LGPD, mas também destacou as iniciativas positivas que já estão em andamento. As informações compartilhadas pelo encarregado de dados serão cruciais para a próxima fase da análise, na qual serão delineadas e detalhadas as adequações necessárias para fortalecer a proteção de dados na instituição.

O comprometimento e a expertise do encarregado são elementos fundamentais para o sucesso da implementação da política de proteção de dados. A partir dos esclarecimentos obtidos na entrevista, será possível formular estratégias eficazes que estejam alinhadas não apenas com as exigências legais, mas também com os princípios éticos e as melhores práticas no tratamento de dados pessoais.

A primeira pergunta da entrevista foi sobre o que o encarregado poderia dizer quanto a implementação da proteção de dados na UFRRJ, o mesmo iniciou sua fala destacando o “desafio gigantesco por ser órgão público”, em seguida passou a

apresentar a Framework[17] do Programa de Privacidade e Segurança da Informação (PPSI) instituído pela Secretaria de Governo Digital por meio da Portaria SGD/MGI nº 852, de 28 de março de 2023.

Cabe esclarecer que a portaria informa que o estabelecimento do Framework do PPSI, conforme o Artigo 7º, engloba a criação de um conjunto de controles, metodologias e ferramentas de suporte, sendo estes considerados controles internos de gestão, de acordo com a Instrução Normativa Conjunta CGU/MPOG nº 1, de 10 de maio de 2016. Os elementos e ferramentas desse framework serão disponibilizados no portal institucional da Secretaria de Governo Digital, e revisões podem ser implementadas pela mesma secretaria, seguindo as diretrizes estabelecidas pela legislação vigente.

Os controles do framework devem respeitar a LGPD, a Política Nacional de Segurança da Informação, os normativos emitidos pela ANPD e pelo Gabinete de Segurança Institucional, além das recomendações dos órgãos federais de controle interno e externo. A adoção desse framework pelos órgãos e entidades é obrigatória, sendo de responsabilidade da Estrutura de Governança de cada um, conforme o Artigo 8º.

O processo de implementação do framework, como detalhado no Artigo 9º, envolve etapas como autoavaliação, análise de lacunas, planejamento e implementação. A decisão de não adotar medidas obrigatórias precisa ser devidamente justificada com base em análise de riscos. A Secretaria de Governo Digital terá um papel ativo na promoção de diagnósticos periódicos, acompanhando e apoiando o planejamento e a implementação do framework. Além disso, poderá elaborar e revisar padrões, processos, procedimentos, guias operacionais e ferramentas de apoio para aprimorar o framework de privacidade e segurança da informação, conforme estabelecido no Artigo 12.

Cabe citar na íntegra o artigo 9º da Portaria SGD/MGI nº 852/2023 que informa as etapas para a implementação do framework

> Art. 9º Considera-se como etapas para a implementação do framework pelos

[17] Framework é um conceito que engloba estratégias e iniciativas direcionadas para resolver um determinado tipo de problema. No entanto, sua abrangência vai além do âmbito de Tecnologia da Informação (TI) ou software. Dessa maneira, as empresas utilizam esse recurso como uma maneira de aprimorar seus resultados por meio de abordagens predefinidas.

> órgãos e entidades pertencentes ao SISP: I - autoavaliação: execução de avaliação pelo próprio órgão, considerando o modelo de avaliação de maturidade e capacidade disponibilizado por meio do framework; II - análise de lacunas: a partir da autoavaliação, esta etapa consiste na identificação de oportunidades quanto à necessidade de implementação de medidas ou de melhoria contínua das medidas já implementadas para aumento da capacidade e maturidade do órgão ou entidade; III - planejamento: após identificadas as oportunidades de melhorias identificadas na etapa anterior, o órgão deve realizar planejamento que especifique o prazo e as necessidades de recursos para implementação, considerando aspectos orçamentários e de recursos humanos do próprio órgão ou entidade; e IV - implementação: esta etapa consiste na implementação das medidas ou na melhoria contínua de medidas já implementadas para aumento da capacidade e maturidade do órgão.

Destaca-se que o encarregado da UFRRJ informou que a instituição já realizou a fase de autoavaliação utilizando o modelo de avaliação de maturidade e capacidade disponibilizado pela secretaria do governo digital no endereço eletrônico https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/framework. A fase da análise de lacunas também já foi executada. O encarregado no momento da entrevista mostrou a planilha que consta a autoavaliação e a identificação de oportunidades quanto à necessidade de implementação de medidas, vez que a pesquisadora é servidora pública federal do órgão sob análise, entretanto, os dados não podem ser compartilhados neste trabalho acadêmico devido ao sigilo das informações institucional, por questão de segurança dos dados.

Essa abordagem demonstra o comprometimento da instituição em seguir as diretrizes estabelecidas pelo framework de privacidade e segurança da informação, evidenciando um esforço na busca pela conformidade e proteção efetiva dos dados pessoais.

A fase do planejamento está em andamento, ressalta-se que a entidade de ensino por meio do encarregado e de servidores do TI estão desenvolvendo um sistema para inventariar os dados onde constará, por exemplo: (i) documento utilizado na coleta; (ii) tipo de dado pessoal; (iii) classificação (criança e adolescente/ dado pessoal /dado pessoal sensível); (iv) titular; (v) finalidade da coleta; (vi) meio da coleta.

Além dos pontos anteriormente abordados, é importante ressaltar que o sistema de inventário de dados incluirá outros tópicos relevantes. Atualmente, aguarda-se a indicação de um setor modelo pela Pró-Reitoria de Planejamento, Avaliação e Desenvolvimento Institucional (PROPLADI) para participar da fase de teste e implementação do sistema.

Os dirigentes da instituição terão acesso ao sistema para preencher as informações requeridas no inventário de dados. Isso possibilitará à instituição ter um controle abrangente sobre todos os dados pessoais que estão sendo tratados, contribuindo assim para a transparência e conformidade com as diretrizes da política de proteção de dados. Essa iniciativa fortalecerá a capacidade da instituição em gerenciar e proteger de maneira eficaz as informações pessoais sob sua responsabilidade.

Ao ser questionado sobre a existência de um Relatório de Impacto à Proteção de Dados (RIPD), o encarregado indicou que o inventário de dados desempenhará um papel crucial nesse contexto, uma vez que permitirá a identificação e análise dos riscos relacionados à proteção de dados.

Quando questionado sobre a previsão de treinamento para os servidores em relação à proteção dos dados pessoais conforme a LGPD, o encarregado informou que há uma programação para iniciar em 2024. Apesar da intenção inicial de realizar o treinamento no final do ano de 2023, não houve alocação de orçamento para essa finalidade. O responsável pela condução desse treinamento será o próprio encarregado em conjunto com a Coordenação de Desenvolvimento de Pessoas (CODEP), vinculada à Pró-reitoria de Gestão de Pessoas (PROGEP).

Foi esclarecido que o plano de treinamento tem como objetivo a transferência de conhecimento, envolvendo a participação de pessoas estratégicas de cada setor. A ideia é que esses indivíduos capacitados durante o treinamento atuem como multiplicadores, compartilhando o conhecimento adquirido em seus respectivos setores de trabalho. Essa abordagem visa proporcionar agilidade na capacitação dos servidores da instituição em relação às práticas de proteção de dados.

Ao ser indagado se o e-mail disponibilizado no site institucional para contato com o encarregado tem recebido demandas, este informou que somente demandas internas de dúvidas dos servidores quando a execução de algumas tarefas que envolvam proteção de dados. No entanto, esclareceu que até o momento não recebeu nenhuma demanda dos titulares de dados. Ele ressaltou que nenhum estudante encaminhou qualquer solicitação por meio desse canal de contato.

Foi questionado se o mesmo julga importante a conscientização dos alunos quanto a importância dos dados pessoais, vez que o formulário demonstrou que estes não têm conhecimento sobre a LGPD, que desconhecem o encarregado de dados e como se comunicar com ele. A resposta foi que é fundamental esta conscientização, mas que a

mesma não deveria ser realizada somente pela instituição, mas também pelo Governo Federal através da ANPD.

O Encarregado de Dados também mencionou que, após diversas solicitações, conseguiu realizar uma palestra de conscientização destinada à alta gestão, abrangendo a Reitoria e as Pró-reitorias. Vale ressaltar que a UFRRJ conta com sete Pró-reitorias: Gestão de Pessoas (Progep); Assuntos Estudantis (Proaes); Assuntos Financeiros (Proaf); Extensão (Proext); Graduação (Prograd); Pesquisa e Pós-Graduação (Proppg); Planejamento, Avaliação e Desenvolvimento Institucional (Propladi).

Na resposta à questão sobre a existência de um setor de governança na UFRRJ, o encarregado informou que, atualmente, a instituição não possui tal estrutura. Ainda ressaltou que a responsabilidade pela proteção de dados não recai exclusivamente sobre a Coordenadoria de Tecnologia da Informação e Comunicação (COTIC), como erroneamente muitos podem pensar. Ele destacou que a eficácia da proteção de dados na instituição depende do comprometimento de todos, especialmente da alta gestão.

A entrevista realizada com o Encarregado de Dados revelou-se produtiva e esclarecedora, evidenciando uma atuação efetiva desse profissional na instituição, orientada para a adaptação às diretrizes da LGPD. O início do processo de inventário na universidade se configura como um passo crucial, uma vez que fornecerá dados essenciais para a análise dos riscos relacionados ao tratamento de informações pessoais.

A conscientização da alta gestão emerge como um fator determinante nesse contexto, uma vez que a compreensão e o engajamento das lideranças são fundamentais para o sucesso na implementação da normativa de proteção de dados. Ademais, a capacitação dos servidores assume papel relevante, constituindo-se como um elemento-chave para a efetiva aplicação das práticas estabelecidas pela LGPD. Dessa forma, a conjugação desses esforços convergirá para a construção de um ambiente organizacional mais alinhado com os preceitos legais e as melhores práticas em proteção de dados.

4.3.2.3 - Entrevista com o Coordenador da Coordenadoria de Tecnologia da Informação e Comunicação

Para compreender melhor a estrutura organizacional da Coordenadoria de Tecnologia da Informação e Comunicação (COTIC), foi realizada entrevista com o

Coordenador do setor, como visto, este departamento integra a Propladi. A mesma ocorreu no campus da UFRRJ em Seropédica, onde estavam presentes o coordenador e a pesquisadora, a mesma foi gravada. A pesquisadora informou sobre a temática da pesquisa ressaltando a importância da tecnologia da informação na implementação da política pública de proteção de dados pessoais e questionou se há adoção de práticas de governança por parte da entidade.

Em resposta ao questionamento, o coordenador informou que na estrutura da COTIC existe o Núcleo de governança da tecnologia da informação e comunicação, porém destacou que formalmente não há ninguém alocado, e que quando ele assumiu a coordenação já era assim. Informou que a quantidade de Analistas não é adequada para o quantitativo de pessoas da comunidade acadêmica que beira em torno de 30 mil pessoas entre servidores e estudantes, então, na prática a governança da tecnologia da informação acaba sendo efetuada na medida do possível pelo próprio coordenador aos poucos, destacou que também depende do que a cultura da instituição permite que seja executado.

Geralmente as práticas de governança desempenhadas pela coordenação da COTIC ocorrem quando há algum memorando circular determinando uma ação pontual. Foi questionado se há um treinamento da equipe referente às práticas de governança. O coordenador respondeu que não, que isso parte mais do interesse de cada pessoa. Salientou ainda que tem diferença entre gestores, pois tem gestores que acham essa questão da governança “horrível”, devido a formalização das regras, o que esbarra na questão cultural.

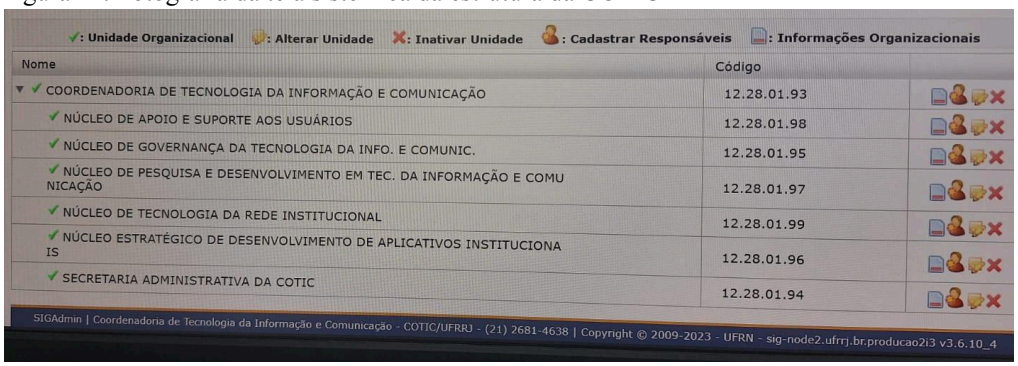
O entrevistado ressaltou que, em algumas situações, ao consultar a literatura, identifica formas mais organizadas e eficientes de implementar governança. Contudo, ele reconhece a necessidade de avaliar cuidadosamente como essas abordagens serão recebidas no contexto institucional, ponderando se é vantajoso investir esforços para insistir nesses métodos ou se seria mais adequado adaptá-los, ou até mesmo reconsiderar sua implementação.

Ele observa que, ao tentar estabelecer práticas de governança em um ambiente de setor público com servidores que desfrutam de estabilidade no emprego, é comum que alguns indivíduos ajam desconsiderando as regras, confiantes de que não enfrentarão consequências significativas. Nesse contexto, a pesquisadora também

abordou a questão da não eficácia dos Processos Administrativos Disciplinares, destacando que, frequentemente, os gestores deixam de instaurá-los.

Apresentou, ainda, em tela sistêmica a disposição atual do setor, permitindo que a mesma fosse fotografada com o objetivo de integrar este trabalho acadêmico como é possível visualizar na figura 11

Figura 11: Fotografia da tela sistêmica da estrutura da COTIC



Fonte: fotografia efetuada pela pesquisadora

Através da análise da figura 11, torna-se evidente que a COTIC é constituída por seis setores. No entanto, o coordenador esclareceu que nem todos esses setores operam efetivamente, devido à ausência de servidores atribuídos por falta de pessoal. Isso ocorre pela inexistência de códigos de vagas disponíveis.

Assim, o entrevistado esclareceu que os núcleos que estão com servidores alocados são o Núcleo de apoio e suporte aos usuários e Núcleo de tecnologia da rede institucional. Já o Núcleo de governança da tecnologia da informação e comunicação, o Núcleo de pesquisa e desenvolvimento em tecnologia da informação e comunicação, o Núcleo estratégico de desenvolvimento de aplicativos institucionais e a Secretaria administrativa da COTIC não possuem servidores alocados.

O coordenador informou que o setor de segurança da informação está localizado no Núcleo de Tecnologia da Rede Institucional, desempenhando um papel crucial na proteção de dados. O setor de segurança da informação tem grande relevância na implementação de medidas proativas para prevenir incidentes de segurança, gerenciar riscos e garantir a conformidade com regulamentações, como a LGPD, assim, foi realizada entrevista com a servidora responsável por este setor.

Desta forma, a entrevista conduzida com o Coordenador da COTIC revelou-se uma fonte de informações relevantes para a pesquisa em andamento. Evidenciou-se de maneira clara a dificuldade enfrentada pela coordenadoria em estabelecer um padrão de excelência devido à escassez de mão de obra, ocasionada pela ausência de códigos de vagas, para aumentar o quantitativo de códigos depende da liberação do MEC. A estrutura organizacional da coordenadoria é robusta, contudo, a carência de servidores para atender a todos os núcleos compromete a efetividade das operações.

É digno de nota que a ausência de um servidor alocado no núcleo de governança resulta na execução dessa função pelo próprio coordenador, especialmente quando solicitado por órgãos externos. Essa prática, embora evidencie um comprometimento da liderança, também ressalta as limitações operacionais devido à insuficiência de recursos humanos especializados.

Essas questões, quando analisadas à luz da proteção de dados, apresentam-se como potenciais pontos de vulnerabilidade. A falta de recursos humanos adequados pode impactar diretamente a capacidade da coordenadoria em garantir a segurança e integridade dos dados. Assim, torna-se imperativo considerar medidas que visem otimizar a alocação de recursos e fortalecer as práticas de governança, a fim de mitigar possíveis riscos e assegurar a conformidade com a normativa vigente em proteção de dados.

4.3.2.4 Entrevista com a servidora responsável pela segurança da informação

A entrevista com a servidora responsável pela segurança da informação foi realizada no campus da UFRRJ em Seropédica, estando presentes a servidora responsável e a pesquisadora, na ocasião a entrevista foi gravada. A pesquisadora informou sobre a temática da pesquisa ressaltando a importância da segurança da informação na implementação da política pública de proteção de dados pessoais e questionou sobre como encontra-se a segurança da informação na instituição.

A servidora mencionou que a segurança da informação encontra-se em processo de estruturação e destacou que, em virtude do programa Governo Digital, o Executivo

Federal está impondo aos órgãos federais a necessidade de se adequarem significativamente no que diz respeito à segurança da informação.

Informou ainda que em um *webinar*[18] realizado pela Secretaria do Governo Digital foram definidas algumas metas para a adequação das instituições do executivo federal. Durante o evento, foi apresentado um *framework* que serve como suporte nesse processo de adaptação, destacou que em março de 2023 foi publicada a Portaria SGD/MGI nº 852/2023 que dispõe sobre o PPSI. Sublinhou ainda que essa adequação é referente a segurança da informação e controle da privacidade, e que por este motivo o trabalho é realizado em conjunto com o encarregado de dados da instituição[19]

Observa-se que o setor de segurança da informação tem estabelecido uma colaboração com o encarregado de dados da instituição, com o propósito de assegurar o cumprimento das diretrizes estabelecidas pelo Governo Federal em relação à segurança da informação e ao controle da privacidade. Essa sinergia de esforços configura-se como um substancial avanço para a universidade em seu processo de adaptação à LGPD.

---

[18] O webinar é um seminário online, apresentado em tempo real ou disponibilizado em formato gravado, direcionado a um público específico. Sua origem está associada ao termo *web based seminar*, que literalmente significa um seminário conduzido via internet.

[19] Portaria SGD/MGI nº 852/2023 - Art. 6º Compõem a Estrutura de Governança do PPSI em cada órgão e entidade da administração pública federal direta, autárquica e fundacional: I - o Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019, responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução; II - o Gestor de Segurança da Informação, dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação; III - o Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis; e IV - o Responsável pela Unidade Controle Interno, atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017. §1º Os agentes públicos listados nos incisos I e II do caput, juntamente com os proprietários de ativos, gestores do negócio ou de políticas públicas, compõem a primeira linha de defesa quando se tratar de controles de privacidade e segurança da informação. §2º O Encarregado pelo Tratamento de Dados Pessoais desempenha o papel de apoiar as partes citadas no parágrafo anterior com orientações acerca das diretrizes que envolvam privacidade e proteção de dados pessoais nos termos do art. 41 da LGPD. §3º A Secretaria de Governo Digital, por meio da Diretoria de Privacidade e Segurança da Informação, atuará no apoio ao diagnóstico, no acompanhamento e na prestação de apoio técnico em relação às ações do PPSI no âmbito dos órgãos e entidades, em articulação com a respectiva Estrutura de Governança, considerando o responsável pela unidade de controle interno como ponto focal para intermédio das ações.

A entrevista conduzida com a servidora encarregada pela segurança da informação emergiu como um componente de grande relevância para os propósitos desta pesquisa. A atividade colaborativa entre o setor de segurança da informação e o encarregado de dados reflete um comprometimento institucional em garantir a integridade e proteção dos dados.

4.3.2.5 - Entrevista com a servidora responsável pelo Núcleo de Governança de Integridade

Inicialmente, cumpre destacar que conforme estabelecido pelo artigo 3º, inciso II do Decreto nº 9203/2017, a integridade figura como um dos princípios da governança no contexto da administração pública federal. Esse preceito ressalta a importância atribuída à manutenção e preservação da integridade nas atividades e processos governamentais. Nesse cenário, a integridade não apenas denota a coerência e consistência das ações administrativas, mas também enfatiza a necessidade de garantir que tais ações estejam alinhadas aos padrões éticos e legais.

A governança na esfera pública, ao abraçar o princípio da integridade, busca assegurar a lisura, transparência e responsabilidade nas práticas administrativas, promovendo, assim, a confiança da sociedade nas instituições governamentais. A integridade, enquanto um princípio da governança, demanda uma atuação diligente na prevenção de desvios éticos e na promoção de uma gestão pública íntegra e alinhada aos interesses coletivos.

Como foi possível verificar em entrevista com a Pró-reitora da PROPLADI, a UFRRJ ainda não possui uma governança totalmente instituída na entidade de ensino, entretanto, foi possível verificar que há um Núcleo de Governança de Integridade. Desta forma, a servidora responsável pelo núcleo foi entrevistada no campus da UFRRJ em Seropédica, onde estavam presentes a servidora e a pesquisadora, na ocasião a entrevista foi gravada. A pesquisadora informou sobre a temática da pesquisa ressaltando a importância da governança na implementação da política pública de proteção de dados pessoais e questionou se a instituição já tem o núcleo de integridade estruturado.

Em resposta a servidora destacou que a governança é composta de alguns mecanismos de liderança, estratégia e controle para poder direcionar e monitorar a gestão, a governança não é gestão, vez que a mesma indica e a gestão faz. Já a

integridade é um princípio de governança e dentro da governança há vários princípios, de forma que a integridade é um deles. Não se atinge a governança sem a integridade, destacou que tem outros princípios que são necessários a adoção pela instituição para se alcançar a governança, como por exemplo a transparência, a prestação de contas, melhoria regulatória, confiabilidade, e a integridade é um desses princípios.

A entrevistada informou que a integridade hoje na UFRRJ não se preocupa com os dados pessoais, está em uma fase embrionária, embora devesse estar mais avançada. Não é uma unidade separada, e neste momento não se atenta a questões da LGPD, mas a servidora entende que esta é uma função da integridade, uma vez que a legislação abarca direitos humanos e preservação dos direitos fundamentais.

A servidora salientou que a integridade hoje está mudando, ela não se resume mais a *compliance*, ou seja, no sentido de ter que aderir às normas formais, entretanto, como saber se uma organização é íntegra? Ela não pode contratar com empresas que têm trabalho escravo, que desrespeita os direitos das minorias, que não tem equidade de gênero, por exemplo, isto está dentro da integridade agora, transformou-se em algo que transcende a anticorrupção, em contraste com a perspectiva mantida desde o ano de 2017. Agora para uma empresa ser íntegra ela tem que abarcar causas sociais, como as mencionadas, e nesta vertente, a LGPD está ligada às questões que diz respeito aos direitos humanos e aos direitos fundamentais, logo tem que ser abarcada pela integridade, hoje não funciona desta forma, mas há uma expectativa de que em algum momento próximo consiga-se.

Perguntou-se se a instituição tem se preocupado com outros princípios de governança além da integridade. Em resposta, informou que tem um comitê de gerenciamento de risco, mas que não sabe como funciona. Inclusive o comitê, na opinião da servidora, deveria ser interligado com a integridade, porque juntos eles poderiam fortalecer a governança na UFRRJ. Quanto aos outros critérios de governança, desconhece que tenha alguma prática nesse sentido.

A pesquisadora ressaltou que então há práticas de governança na instituição, porém não são interligadas. A servidora destacou que não são interligadas e que ela só tem conhecimento do comitê de gerenciamento de risco, que faz o mapeamento do risco, com o intuito de fortalecer as práticas de governança na universidade, mas não sabe como funciona. Informou que na UFRRJ a governança se confunde um pouco com a gestão, o que não deveria ocorrer, destacando que essa é uma discussão muito forte

nos grupos de pesquisa, no sentido das pessoas compreenderem que governança e gestão não se confundem. “Você não faz a gestão sem a governança, mas você faz a governança sem uma boa gestão. Porque a governança vai falar que a gestão tem que trilhar determinado caminho, agora quem vai executar é a gestão.”

Foi indagado se caso tivesse algo mais estruturado referente a governança na UFRRJ, este setor deveria estar ligado a qual parte da estrutura institucional. Foi respondido pela servidora que deveria ser ligado à Reitoria. O ideal seria a integridade vir de um núcleo de governança e a governança funcionaria muito bem como uma controladoria, esta não se confunde com corregedoria. “A controladoria seria um mecanismo de governança que ramificaria em integridade, corregedoria, ouvidoria, sendo a controladoria uma governança estruturada, para não ficar solto, tendo uma pessoa preocupada em reunir todos esses mecanismos para melhora da condução das políticas, pois se não tiver centralizado na mão de alguém fica pulverizado como está agora, tem a integridade aqui, a ouvidoria ali, e os setores não dialogam. Até a questão da LGPD poderia estar ligada a controladoria.”

Questionada se a UFRRJ está atendendo as práticas de governança, respondeu que na sua visão duas práticas são pouco para dizer que a UFRRJ atende a governança. A Integridade foi criada quando a Controladoria Geral da União (CGU) impôs, vez que o decreto de governança é de 2017 e em 2018 a CGU publicou uma portaria, alterada em 2019, obrigando as instituições públicas do executivo federal a criarem a integridade, então a princípio foi *proform*, desde então foi elaborado um planejamento monitorando a questão do conflito de interesse, mas tudo muito embrionário, a servidora pontua que deveria ser criado um núcleo lotando mais servidores para atuarem nesta demanda, vez que atualmente só há ela lotada no núcleo de integridade.

A entrevistada informou que com a mudança de governo, no ano de 2023 tudo que estava programado no planejamento da CGU quanto a integridade, permaneceu inerte,vez que ocorreu mudança de todos os cargos, portanto agora os processos estão se alinhando. Destaca sua participação em uma conferência realizada em dezembro de 2023, considerando este evento como um ponto de partida para iniciar as atividades em 2024, período que se aproxima com diversas demandas a serem enfrentadas.

A pesquisadora observou que há uma percepção de que a CGU enfatiza a governança no contexto da integridade, levantando a questão se não deveria ocorrer o inverso. Em resposta a servidora informou que eles cobram a integridade dentro da

governança. “Como a governança é um chapéu e tem várias coisas, eles pegaram uma das coisas e estão cobrando isso”, A entrevistada indica que, caso houvesse uma ênfase na cobrança da governança, a situação tenderia a se agravar, “porque não iria ter nada, pois seriam vários outros chapeuzinhos, e desse chapéu abrem outros, vez que da integridade se tem o PAD, a ética, o conflito de interesse, o nepotismo, a integridade também não é pequena.”

Logo, a entrevista destaca a necessidade de fortalecimento da governança na UFRRJ, evidenciando que as práticas existentes ainda não estão devidamente interligadas. A servidora ressalta a importância de uma governança estruturada, centralizada na Reitoria, que abranja diferentes aspectos, incluindo a possibilidade da proteção de dados pessoais estar interligada à integridade.

4.2.2.6 - Da coleta dos dados dos estudante: informação da Pró-reitoria de graduação

Tendo em vista que o aludido trabalho acadêmico tem como delimitação do tema os dados pessoais dos estudantes da UFRRJ, é crucial destacar como esses dados são colhidos pela Pró-Reitoria de Graduação (Prograd), desta forma, em contato com a referida pró-reitoria um servidor do setor informou que o processo seletivo é realizado pelo Sistema de Seleção Unificada (SISU)[20] e os documentos solicitados para a realização da matrícula encontram-se no edital de acesso aos cursos de graduação da UFRRJ que fica disponível no endereço eletrônico https://r1.ufrrj.br/sisu/editais/ da instituição, no referido site é possível visualizar todos os editais desde 2018. Para apresentar nesta pesquisa os documentos solicitados, foi utilizado o edital nº 45/2023 - PROGRAD/UFRRJ, que solicita em seu artigo 59 a documentação necessária para a matrícula

> Art. 59. Para solicitar o cadastro e matrícula, o(a) candidato(a) deverá apresentar os seguintes documentos: a) Documento de identificação civil oficial, com foto e válido (frente e verso); b) Cadastro de Pessoa Física -

[20] O Sistema de Seleção Unificada (Sisu) concentra em uma plataforma eletrônica, administrada pelo Ministério da Educação (MEC), as oportunidades disponibilizadas por instituições públicas de ensino superior em todo o país, sendo na maior parte oriundas de instituições federais, como universidades e institutos. Esse sistema realiza a seleção de estudantes com base nas notas obtidas no Exame Nacional do Ensino Médio (Enem). À medida que os candidatos fazem suas escolhas de cursos e modalidades de concorrência durante as duas edições anuais do Sisu, o sistema efetua a seleção, classificando-os em ordem decrescente de pontuação até o preenchimento das vagas oferecidas.

> CPF; c) Histórico Escolar do Ensino Médio, com assinatura e carimbo legíveis do responsável e da instituição que expediu o documento; d) Certificado de Conclusão ou Diploma de Ensino Médio, com assinatura e carimbo legíveis do responsável e da instituição que expediu o documento (frente e verso); e) Documento militar: Certificado de Dispensa de Incorporação (CDI), Certificado de Reservista (CR), Carteira de Militar (ATIVO) ou, provisoriamente, o Certificado de Alistamento Militar (CAM), provando estar em dia com suas obrigações militares, somente para candidatos do sexo masculino; f) Certidão de Quitação Eleitoral, obtida por meio do sítio eletrônico do Tribunal Superior Eleitoral (TSE) http://www.tse.jus.br/ ou fornecida pelos órgãos da Justiça Eleitoral. §1º. O candidato que não apresentar, no ato da solicitação de matrícula, os documentos contidos nos itens "c" e "d" do presente artigo, deverá apresentar Declaração de Conclusão de Ensino Médio com assinatura e carimbo legíveis do responsável e da instituição que expediu o documento. §2º. Para o candidato inscrito em qualquer modalidade de reserva de vagas, que exija a comprovação do Ensino Médio integral em rede pública de ensino, deverão estar discriminados os anos cursados na(s) instituição(ões) de ensino (ANEXO I).

A abordagem adotada no estabelecimento desses requisitos documentais parece alinhada aos princípios da LGPD, garantindo que a coleta das informações pessoais dos candidatos seja realizada de maneira estritamente necessária. A pesquisadora questionou ao servidor se esses documentos são compartilhados com outros setores, ele informou que até onde ele tem ciência, essas informações não são compartilhadas, que os demais setores que precisam de informações dos estudantes fazem sua própria coleta.

Para melhor esclarecimento, foi consultado o regulamento da graduação que normatiza a organização acadêmica dos cursos de graduação da UFRRJ. Este foi aprovado pelo Conselho de Ensino, Pesquisa e Extensão (CEPE) em 15 de março de 2023, por meio da deliberação nº 117/2023, sendo fruto de um extenso esforço coletivo de debate e análise acerca do funcionamento dos cursos de graduação na UFRRJ, compilando e atualizando uma série de decisões temáticas já existentes, além de propor novas iniciativas que visam aprimorar a qualidade da graduação na instituição. Assim, o regulamento contempla a respeito da guarda de documentos relativos ao ensino de graduação

> Art. 266. Na UFRRJ, a guarda de documentos relativos ao ensino de graduação é responsabilidade das seguintes instâncias acadêmico-administrativas: I – PROGRAD; II – Departamentos acadêmicos e unidades acadêmicas especializadas; e III – Coordenações de Cursos. Parágrafo único - A guarda de documentos deve ser preferencialmente feita em formato eletrônico. Art. 267. Compete à PROGRAD manter sob sua guarda: I – Documentos referentes ao cadastramento de estudantes; II – Históricos escolares de ingressantes a partir de 1970, cujos dados não estejam inseridos no sistema oficial de registro e controle acadêmico; III – Livros de registro de diplomas; IV – Livros de apostila de habilitações; V – Projetos

> pedagógicos dos cursos de graduação e suas alterações; VI – Registro de currículos extintos dos cursos de graduação; VII – Documentos relativos a programas por ela coordenados; VIII – Autos de processos e requerimentos nos quais seja ela a última instância de tramitação; IX – Documentos referentes à execução de convênios que digam respeito à graduação. Art. 268. Compete aos departamentos acadêmicos e unidades acadêmicas especializadas manter sob sua guarda: I – Autos de processos e requerimentos com referência aos quais eles sejam a última instância de tramitação; II – Diários de turma emitidos em forma não eletrônica e que não estejam incorporados ao sistema oficial de registro e controle acadêmico. Parágrafo único - Os instrumentos escritos de avaliação de aprendizagem devem, preferencialmente, ser devolvidos aos estudantes logo após o encerramento do prazo para revisão; caso não o sejam, devem ser mantidos sob a guarda dos professores durante o prazo mínimo de 30 dias após a consolidação final das notas daquele período letivo, após o que podem ser descartados. Art. 269. Compete às Coordenações de Curso manter sob sua guarda: I – Autos de processos e requerimentos com referência aos quais elas sejam a última instância de tramitação; Art. 285. Na UFRRJ, a guarda de documentos relativos ao ensino de graduação é responsabilidade das seguintes instâncias acadêmico-administrativas: I – PROGRAD; II – Departamentos Acadêmicos e unidades acadêmicas; e III – Coordenações de Cursos. Parágrafo único - A guarda de documentos deve ser preferencialmente feita em formato eletrônico. Art. 286. Compete à PROGRAD manter sob sua guarda: I – Documentos referentes ao cadastramento de estudantes; II – Históricos escolares de ingressantes a partir de 2001 cujos dados não estejam inseridos no sistema oficial de registro e controle acadêmico; III – Livros de registro de diplomas; IV – Livros de apostila de habilitações; V – Projetos pedagógicos dos cursos de graduação e suas alterações; VI – Registro de currículos extintos dos cursos de graduação; VII – Documentos relativos a programas por ela coordenados; VIII – Autos de processos e requerimentos nos quais seja ela a última instância de tramitação; IX – Documentos referentes à execução de convênios que digam respeito à graduação. Art. 287. Compete aos departamentos acadêmicos e unidades acadêmicas manter sob sua guarda: I – Autos de processos e requerimentos com referência aos quais eles sejam a última instância de tramitação; II – Diários de turma emitidos em forma não eletrônica e que não estejam incorporados ao sistema oficial de registro e controle acadêmico. III – Instrumentos de verificações de rendimento escolar- quando não retirados pelos discentes. Parágrafo único - Os instrumentos escritos de avaliação de aprendizagem devem, preferencialmente, ser devolvidos aos estudantes no transcorrer do período letivo; caso não o sejam, devem ser mantidos sob a guarda dos Departamentos durante um ano. Art. 288. Compete às Coordenações de Curso manter sob sua guarda: I – Autos de processos e requerimentos com referência aos quais elas sejam a última instância de tramitação; e II – Documentos referentes ao colegiado de curso.

O texto descreve a distribuição de responsabilidades para a guarda de documentos relacionados ao ensino de graduação na UFRRJ. A PROGRAD, departamentos acadêmicos e unidades acadêmicas especializadas, bem como as Coordenações de Cursos, são apontadas como instâncias responsáveis. Destaca-se a preferência pelo formato eletrônico na guarda de documentos. A PROGRAD tem a incumbência de manter diversos documentos, como cadastramento de estudantes, históricos escolares, livros de registro de diplomas, projetos pedagógicos e outros. Os departamentos acadêmicos e unidades especializadas têm responsabilidade sobre autos

de processos, diários de turma não eletrônicos, e instrumentos escritos de avaliação por determinado período. As Coordenações de Curso ficam encarregadas de manter autos de processos, documentos referentes ao colegiado de curso, entre outros. Essas responsabilidades são reiteradas nas versões subsequentes do texto.

4.4 - Planos de ação para a adequação e implementação

Com base nas entrevistas conduzidas e na documentação analisada ao longo desta seção, torna-se evidente que a UFRRJ tem empreendido esforços para se ajustar e implementar as diretrizes estabelecidas pela LGPD. Contudo, persistem vários desafios, e algumas práticas simples que ainda não foram adotadas e poderiam ser implementadas, proporcionando assim uma facilitação no percurso.

A análise revelou lacunas e áreas de aprimoramento, sugerindo que a universidade pode beneficiar-se de estratégias mais proativas e abrangentes no que diz respeito à conformidade com a LGPD. Portanto, neste tópico, serão abordados planos de ação que visam não apenas superar os desafios identificados, mas também promover uma cultura organizacional que valorize a proteção de dados e que esteja alinhada com as melhores práticas estabelecidas pela legislação vigente.

Logo, é importante se atentar para algumas etapas cruciais de adequação, como a análise e mapeamento de dados, esta primeira etapa envolve uma análise abrangente dos dados tratados pela UFRRJ. Isso inclui a identificação de categorias de dados, fontes de coleta e os propósitos específicos para os quais são utilizados. O mapeamento fornecerá uma visão clara da extensão dos dados tratados pela instituição. Quanto a este ponto foi possível verificar na entrevista com o encarregado de dados que a instituição já iniciou um planejamento para efetuar o inventário dos dados, entretanto, ainda há alguns pontos a serem superados, como a indicação de um setor piloto pela PROPLADI.

Por se tratar de uma entidade pública geralmente os processos ocorrem de forma mais lenta, devido a inúmeras burocracias e quantidade de demandas internas e externas, porém é crucial a conscientização da comunidade acadêmica quanto a importância da LGPD para que a sua implementação se torne prioritária. É necessário o investimento em mudança cultural, vez que o inventário será preenchido pelo dirigente de cada setor, sem a conscientização da relevância da tarefa desenvolvida e a

necessidade de urgência da demanda, o inventário pode não apresentar os dados de maneira consistente e assertiva.

É fundamental que o inventário apresente todos os dados tratados pela instituição e a finalidade que se destina, mas isto depende do empenho de cada servidor que estará responsável pelo preenchimento, ressaltando que esta não será uma atividade descontinuada, vez que a coleta dos dados pessoais pela instituição ocorre de forma permanente, assim o inventário deverá ser atualizado constantemente, sempre que houver nova coleta ou compartilhamento de dados.

Realizar o inventário institucional é de extrema importância, porém se este não se mantiver atualizado, será um desperdício do trabalho efetuado, e um risco aos dados pessoais tratados pela entidade de ensino, pois como ressaltou o encarregado de dados na entrevista, o inventário contribuirá na realização do Relatório de Impacto à Proteção de Dados.

Neste viés, a segunda etapa é a elaboração de políticas internas, com base no mapeamento, a UFRRJ deve desenvolver políticas internas claras e abrangentes que orientem o tratamento de dados. Isso inclui procedimentos para obtenção de consentimento, quando necessário, gestão de dados sensíveis e diretrizes para o compartilhamento responsável de informações. Essas políticas internas devem estar disponíveis aos titulares de dados.

A elaboração e execução de políticas internas focadas na proteção de dados será possível quando a instituição iniciar o inventário dos dados. Para que sejam eficazes, devem estar pautadas nos princípios da LGPD. Após inventariar os dados de cada setor é necessário verificar se estes estão cumprindo com a finalidade da coleta, de forma que a execução do processamento esteja atendendo a propósitos legítimos, específicos, claros e previamente informados ao titular, sem a possibilidade de realizar tratamento subsequente de maneira incompatível com essas finalidades a que foram destinados inicialmente.

Deve-se verificar se há conformidade do tratamento com os propósitos comunicados ao titular, em consonância com o contexto do processamento, caso não haja esta adequação, tais dados devem ser eliminados. Estes só podem ser tratados se houver necessidade, logo, é fundamental ter como política interna a restrição do processamento ao mínimo essencial para atingir seus objetivos, envolvendo dados

pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Como verificado no questionário aplicado aos estudantes, estes desconhecem quais são os seus dados tratados pela instituição e quais setores têm acesso a estes dados, e muitas vezes os servidores têm dificuldade de prestar esta informação, vez que os dados são coletados por diversos setores. É importante ter como política interna a centralização da armazenamento dos dados e o controle do compartilhamento entre os setores para que a instituição tenha uma maior segurança e mantenha o livre acesso aos titulares e a transparência, pois desta forma será assegurado a facilidade e gratuidade de consultar informações sobre a maneira e a extensão do tratamento, assim como a integridade de seus dados pessoais, bem como, deve assegurar aos titulares a precisão, transparência, relevância e atualização dos dados, conforme necessário e para cumprir a finalidade do seu processamento, mantendo a qualidade dos dados.

Estruturar a implementação de medidas técnicas e administrativas eficazes para resguardar os dados pessoais contra acessos não autorizados, bem como situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, bem como adotar medidas para evitar a ocorrência de danos decorrentes do processamento de dados pessoais. Os dados não devem ser utilizados com finalidade discriminatória, logo é imperioso que haja uma política interna para resguardar o titular de possíveis discriminações, principalmente no que tange a dados sensíveis. Logo, é imprescindível que a instituição comprove a implementação de medidas eficazes e capazes de evidenciar a conformidade e o cumprimento das normas de proteção de dados pessoais, incluindo a eficácia dessas medidas.

Salienta-se que a UFRRJ possui o Plano de Desenvolvimento Institucional (PDI) 2023-2027[21], entretanto, ao efetuar a leitura do referido documento não foi

[21] (PDI, 2023, pg10) O Plano de Desenvolvimento Institucional (PDI) é um instrumento legal com previsão de cinco anos para execução, importante para o planejamento institucional e obrigatório para as Instituições de Ensino Superior (IES). Mais que um instrumento legal, o PDI é importante para nortear as ações da instituição, a fim de alcançar os objetivos estratégicos e a VISÃO de longo prazo da UFRRJ. Para que as instituições de educação superior (IES) funcionem da melhor forma possível, é necessário pensar cuidadosamente seus processos de gestão a curto, médio e longo prazo. (...) Em linhas gerais, o PDI é um instrumento indispensável para que as instituições sejam credenciadas e recredenciadas, consigam autorização de funcionamento dos seus cursos e alcancem bons resultados na avaliação do MEC. O Plano de Desenvolvimento Institucional é um documento que dispõe sobre a missão, visão, valores e funcionamento geral das IES. Além disso, estabelece ações estratégicas para se alcançar as metas da instituição, referentes à qualidade do ensino e de sua gestão. Ele serve para planejar o funcionamento das instituições de educação superior (IES) em período de tempo definido e acordado com a comunidade. Constitui-se, portanto, como um verdadeiro plano para melhorá-las, a partir da tomada de

possível identificar demandas diretamente direcionadas à implementação da LGPD na instituição, porém, há direcionamentos para a TI, capacitação dos servidores e implementação da política de governança. O que pode abarcar a adequação da proteção de dados na instituição e a elaboração de políticas internas efetivas. Com base no inventário que será realizado, é possível adequar a instituição à proteção de dados pessoais pautando-se no PDI do quadriênio 2023-2027.

Outra política interna relevante é a capacitação e conscientização, pois a efetivação requer a capacitação de todos os envolvidos no manuseio de dados, desde docentes até a equipe administrativa. Cursos de conscientização sobre os princípios da proteção de dados e as implicações legais são essenciais para criar uma cultura organizacional de responsabilidade.

Na entrevista com o encarregado de dados, o mesmo mencionou que há previsão da realização de tais cursos para início de 2024, bem como, no PDI menciona a capacitação dos servidores, porém não menciona em quais áreas ocorrerão as referidas capacitações, mas como há previsão no plano, provavelmente ocorrerá dotação orçamentária para que as mesmas sejam efetuadas. Importante destacar que o instrutor para a capacitação de proteção de dados pessoais será o encarregado de dados da instituição, este possui formação em Direito e Tecnologia da Informação, já atuou na comissão de fiscalização da ANPD e atualmente foi nomeado como um dos 20 membros do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade (CMPDPP) da cidade do Rio de Janeiro.

O aprimoramento de sistemas tecnológicos é uma política interna que deve ser adotada pela UFRRJ. Precisa-se avaliar e, se necessário, aprimorar seus sistemas tecnológicos para garantir a segurança e conformidade com a normativa de proteção de dados. Isso pode incluir a efetivação de medidas de segurança cibernética e a revisão de práticas de armazenamento. O PDI (2023, pg 102) informa os principais sistemas de informações da instituição

> Os principais Sistemas de Informações na UFRRJ são os Sistemas Integrados de Gestão (SIG), desenvolvidos pela UFRN (SIG-UFRN) que se encontram em processo de implementação desde 2016. Os sistemas SIG são compostos pelos seguintes componentes: ● Sistema Integrado de Gestão de Recursos

ações estratégicas. O processo de elaboração e revisão periódica do PDI contribui para o levantamento de diagnóstico da situação real da Instituição e as alternativas possíveis e viáveis para a implementação de mudanças. Dessa forma, é possível tomar providências mais bem fundamentadas de acordo com a capacidade institucional e de forma estruturada.

> Humanos (SIGRH) – Gestão de recursos humanos; ● Sistema Integrado de Patrimônio, Administração e Contratos (SIPAC) – Gestão de patrimônio, administração e contratos (financeiro, contabilidade, protocolo, materiais etc); ● Sistema Integrado de Gestão de Atividades Acadêmicas (SIGAA) – Gestão de atividades acadêmicas (alunos, disciplinas, documentos). Esse Sistema Integrado de Gestão é responsabilidade técnica da Coordenadoria de Tecnologia da Informação e Comunicação (COTIC), que está vinculada à Pró-reitoria de Planejamento, Avaliação e Desenvolvimento Institucional (PROPLADI). Seu corpo técnico tem sido treinado permanentemente para atender as demandas das Unidades. Os principais processos desenvolvidos pela área de TI na UFRRJ são: 1) Desenvolvimento de Sistemas (Manutenção de Sistemas, Criação de Novos Sistemas); 2) Manutenção (Sistemas Operacionais, Suítes de Escritório, Antivírus, Software de Periféricos); 3) E-mail (E-mail Institucional, Cadastro de conta de e-mail); 4) Sites, Portais e Hosting (Desenvolvimento de sites, Hospedagem de sites, Solicitação de serviços web); 5) Consultoria (Gerenciamento de Projetos, Aquisição de Bens e Serviços de TI); 6) Rede e Telefonia (VoIP, Gerenciamento de Rede e Infraestrutura, Projeto de Instalação de Redes, Mensagens Instantâneas Internas); 7) Servidores e Data Center (Gerenciamento de Pastas de Compartilhamento, Gerenciamento do Data Center (NOC), Backup, Virtualização); 8) Software de Governo (Suporte a Soluções do Portal do Software Público Brasileiro, Suporte a Soluções de Softwares Recomendados pelo Governo Federal); 9) Aquisições de Recursos Computacionais (Aquisição de equipamentos e componentes de TI, Aquisição de softwares, Especificações de equipamento e softwares); Apesar de relacionar os principais sistemas acima, ao todo são 40 (quarenta) sistemas de informações que se constituem em projetos desenvolvidos pela equipe.

O trecho destaca os Sistemas Integrados de Gestão (SIG), desenvolvidos pela UFRN, que estão em processo de implementação desde 2016. Esses sistemas, compreendendo o SIGRH, SIPAC e SIGAA, desempenham papéis cruciais na gestão de recursos humanos, patrimônio, administração, contratos e atividades acadêmicas, abrangendo diversas áreas da universidade e os mesmos devem ser avaliados e, se necessário, aprimorados para garantir a segurança e conformidade com a LGPD.

É notável a responsabilidade técnica atribuída à COTIC na gestão desses sistemas. A constante formação técnica do corpo da COTIC de fato é essencial para atender às demandas das unidades da UFRRJ. A descrição dos principais processos desenvolvidos pela área de TI abrange desde o desenvolvimento e manutenção de sistemas até a gestão de e-mails, consultoria, rede, telefonia, servidores, *data center*, *software* de governo e aquisições de recursos computacionais. Destaca-se a amplitude e diversidade dessas atividades, indicando uma abordagem abrangente e integrada para atender às demandas tecnológicas da instituição. Ressaltando que de acordo com a entrevista com o coordenador desta unidade, o corpo técnico é desproporcional à necessidade institucional.

A menção de 40 sistemas de informações de projetos desenvolvidos pela equipe destaca a complexidade e a diversidade das soluções de TI na instituição. Isso ressalta a importância estratégica da área de Tecnologia da Informação na universidade, sendo essencial para o funcionamento eficaz e a modernização de processos em diferentes setores. Cabe mencionar que um projeto que está sendo desenvolvido é o sistema de inventário que será fundamental para a adequação e implementação da LGPD na entidade de ensino.

Mesmo após a adoção de inúmeras políticas internas, não haverá eficácia se não ocorrer o monitoramento e avaliação contínua, vez que a implementação da política não é uma tarefa única, esta requer acompanhamento constante e avaliação das práticas de tratamento de dados. Mecanismos de *feedback* e canais para relatar violações de dados devem ser estabelecidos para garantir uma resposta rápida a eventuais incidentes.

5. CONCLUSÃO

A análise apresentada nesta dissertação destacou que a proteção dos dados pessoais é um desdobramento natural do processo evolutivo da privacidade ao longo do tempo. Ressaltou-se a evolução do conceito de privacidade no decurso das décadas recentes, salientando as mudanças em sua natureza devido à complexidade de interesses e valores envolvidos. O direito à privacidade não se restringe mais à mera preservação do segredo, mas também à gestão e controle da circulação de informações. Além disso, a evolução da privacidade está intrinsecamente ligada à consolidação da teoria dos direitos da personalidade. Na era da informação, a proteção da privacidade avança para novos territórios, sendo reconhecida como um elemento essencial para proporcionar ao indivíduo os meios necessários para construir e consolidar sua esfera privada.

Foi abordado o papel positivo da proteção da privacidade no contexto das interações sociais e dos relacionamentos individuais. Esta função é considerada crucial para o desenvolvimento da personalidade como um todo, ganhando ainda mais importância quando aspectos como escolhas pessoais e vida privada estão em consideração, abrangendo desde questões íntimas até implicações políticas e sociais.

Logo, foi demonstrada a complexidade e a relevância contínua do tema, destacando como a proteção de dados pessoais tornou-se uma ferramenta indispensável na contemporaneidade para garantir não apenas a privacidade individual, mas também para preservar a integridade das relações sociais e promover um ambiente de confiança e segurança na era digital.

Este estudo abordou a complexidade e a natureza multifacetada da privacidade, conforme discutido por Solove. Argumenta-se que a privacidade não pode ser simplificada em uma essência única ou universal, mas deve ser compreendida como uma interseção de diversos elementos distintos, os quais, embora não possuam um traço comum específico, compartilham semelhanças entre si. Esse entendimento ressalta a diversidade de preocupações e contextos que permeiam a noção de privacidade.

Além disso, a análise enfatizou a crescente importância da privacidade da informação no âmbito público, evidenciada pela agenda legislativa do Congresso e das legislaturas estaduais nos Estados Unidos, bem como em muitos outros países. Questões de privacidade frequentemente ganham destaque nos meios de comunicação e

tornam-se objetos de litígio, o que demonstra a relevância atribuída a essa temática na esfera pública. Uma terceira dimensão abordada refere-se aos recentes desenvolvimentos legais e normativos relacionados à privacidade da informação, caracterizando-a como uma área em expansão no campo do direito.

O aumento da legislação, regulamentação e conscientização pública sobre privacidade tem motivado diversas empresas de setores variados a enfrentarem ativamente os desafios associados à privacidade. Este panorama abrangente delineado por Solove e Schwartz ofereceu uma compreensão atualizada das dinâmicas envolvidas na preservação da privacidade da informação na sociedade contemporânea.

Como colocado, diante da relevância dessa temática para o ordenamento jurídico brasileiro e a pressão externa exercida após a implementação do GDPR pela União Europeia, o Brasil promulgou a LGPD, representando um avanço significativo na construção de uma política pública de proteção de dados pessoais no país.

Deste modo, a teoria dos direitos da personalidade emerge como um componente vital no contexto da privacidade e proteção de dados pessoais, pois ela não apenas busca resguardar a personalidade, mas também dialoga com a dignidade da pessoa humana e outros princípios constitucionais. Esta teoria assume um papel de destaque em uma sociedade contemporânea onde a tecnologia da informação avança rapidamente, tornando difícil o acompanhamento simultâneo pelo ordenamento jurídico. Assim, é crucial enfatizar a proteção de dados pessoais como uma política pública reconhecida no ordenamento jurídico brasileiro como Direito Fundamental.

Como visto, o trabalho acadêmico baseou-se na teoria geral do direito da personalidade e na teoria do direito fundamental, ambas fundamentadas na dignidade da pessoa humana, visto que a proteção de dados pessoais representa uma evolução do direito à privacidade, visando assegurar a segurança das informações pessoais do titular dos dados.

Seguindo essa base teórica, o estudo explorou a proteção da pessoa como titular dos dados e a política pública de proteção dos dados pessoais como direito fundamental. Especificamente, investigando a aplicação da política pública de proteção de dados pessoais às informações dos estudantes na UFRRJ. Vez que, o trabalho acadêmico apontou como problema a adequação da universidade à política pública de proteção de dados pessoais à luz da LGPD, surgindo a seguinte questão central: quais as

providências foram ou estão sendo tomadas para que ocorra a devida adequação às exigências legais e a prevenção dos riscos inerentes?

Logo, tendo como ponto norteador este questionamento, bem como, ponderando que a pesquisa teve como recorte os dados pessoais dos estudantes, coube realizar a análise dos princípios que regem o tratamento dos dados pessoais. A análise da legislação que embasa a pesquisa e a importância dos princípios que regem a proteção de dados pessoais proporcionou uma compreensão aprofundada da temática e orientará futuras ações no campo da proteção de dados pessoais.

A dissertação destacou que a conformidade com a legislação traz consigo uma série de vantagens com implicações significativas no que tange à salvaguarda dos direitos humanos, dignidade e cidadania, além de outros aspectos de relevo. Salientou que a proteção dos direitos humanos é um dos pilares fundamentais da legislação, concebida com o objetivo de resguardar os direitos fundamentais dos indivíduos no que diz respeito ao tratamento de seus dados pessoais. Isso abrange a proteção dos direitos à privacidade, liberdade de expressão, bem como a salvaguarda da intimidade, honra e imagem das pessoas.

Além disso, a lei confere particular ênfase à proteção da privacidade das pessoas, estabelecendo a obrigatoriedade de que as organizações coletem e processem dados pessoais de maneira transparente, informando aos titulares dos dados de que forma suas informações serão utilizadas. Ressaltou-se que a normativa não veda a liberdade de expressão, mas estabelece balizas para garantir que o tratamento de dados pessoais seja conduzido de maneira ética e respeitosa, sem infringir a privacidade.

Ademais, a LGPD também fomenta o livre desenvolvimento econômico e tecnológico, fornecendo orientações para que as organizações processem dados pessoais de maneira responsável. Isso pode impulsionar a inovação tecnológica e o desenvolvimento de novos serviços, contribuindo assim para o progresso econômico e social do país.

A conscientização dos titulares de dados pessoais, bem como dos agentes de tratamento, foi apontada como elemento fundamental para a eficácia da legislação. A ausência de um entendimento claro dos direitos e responsabilidades vinculados à proteção de dados pode resultar em desafios significativos na implementação da legislação, podendo até mesmo comprometer sua eficácia.

Desta forma, a implementação de políticas públicas voltadas para a conscientização tem sido reconhecida como uma medida crucial. Isso abarca desde campanhas de educação pública até o fornecimento de treinamento específico para profissionais de privacidade de dados, orientações para empresas e entidades/órgãos governamentais, bem como a aplicação de medidas de fiscalização e cumprimento para garantir a aderência à LGPD.

Logo, a conscientização não deve ser tratada como um esforço isolado e pontual, mas sim como um processo contínuo. À medida que o cenário de privacidade de dados continua a evoluir, é fundamental que a conscientização seja constantemente reforçada e atualizada. Nesse contexto, a LGPD, assim como outras regulamentações de proteção de dados em âmbito global, representa um avanço significativo na busca pelo equilíbrio entre o uso de dados pessoais e a proteção dos direitos individuais, bem como na promoção da confiança do público nas instituições que lidam com esses dados.

Para além, a ênfase na governança em privacidade, conforme delineada no texto legal, não apenas denota um compromisso com a conformidade, mas também representa uma busca por padrões de excelência que transcendem a mera adesão às obrigações normativas. Ao contemplar a natureza, abrangência, propósito e riscos inerentes ao tratamento de dados pessoais, as diretrizes de governança estabelecem um arcabouço regulatório destinado a equilibrar os interesses legítimos das organizações com os direitos fundamentais dos titulares dos dados.

Demonstrou-se que a implementação eficaz das políticas públicas de proteção de dados está intrinsecamente relacionada à presença de uma governança robusta. Esta abordagem não apenas confere maior segurança jurídica às organizações, mas também fomenta a confiança dos titulares dos dados e contribui para a construção de um ambiente digital mais ético e transparente.

Ao efetuar a análise do Decreto nº 9.203/2017 ficou evidente que este sublinha a importância da monitorização do desempenho e da avaliação de políticas e ações prioritárias para assegurar a adesão às diretrizes estratégicas. Ainda, destaca a relevância da transparência, incentivando a divulgação aberta e transparente das atividades e resultados da organização para fortalecer o acesso público à informação. Ao enfatizar a implementação de controles internos baseados na gestão de riscos, visa privilegiar ações estratégicas de prevenção antes de procedimentos sancionatórios, contribuindo para uma gestão mais eficaz e prevenindo irregularidades.

Portanto, o Decreto nº 9.203/2017 desempenha um papel crucial ao fornecer um arcabouço normativo que orienta a atuação da administração pública federal, promovendo princípios e diretrizes que visam uma gestão mais eficiente, ética e transparente, alinhada com as necessidades e expectativas da sociedade. Destaca-se a importância de editar e revisar atos normativos pautando-se por boas práticas regulatórias, além da legitimidade, estabilidade e coerência do ordenamento jurídico. Essa foi a premissa adotada pela LGPD ao incentivar a adoção de boas práticas e governança.

Quando os agentes de tratamento optam por adotar regras de boa prática e governança no contexto do tratamento de dados, estão evidenciando um compromisso sólido com a ética e a responsabilidade. Essa postura transcende a mera conformidade com as regulamentações, representando uma abordagem proativa para garantir a segurança e a integridade dos dados pessoais.

No caso de um incidente fortuito, como um vazamento de dados, a presença de regras de boa prática e governança pode indicar a boa fé por parte dos agentes de tratamento. Isso porque essas regras não apenas estabelecem medidas preventivas, mas também delineiam procedimentos claros para lidar com incidentes, incluindo a notificação rápida aos titulares afetados e às autoridades competentes.

Ao demonstrar boa fé por meio da adoção dessas práticas, os agentes de tratamento não apenas cumprem requisitos legais, mas também estabelecem um padrão elevado de responsabilidade e transparência. Isso contribui para a construção de confiança com os titulares de dados e reforça a reputação da entidade e do órgão público, mesmo em situações adversas, ao demonstrar um compromisso genuíno com a proteção e o respeito aos direitos individuais.

Neste sentido, as sanções têm como objetivo garantir a conformidade com a lei e promover a proteção dos dados pessoais dos indivíduos, incentivando as organizações a adotarem boas práticas e governança na implementação da política pública de proteção de dados pessoais. De acordo com o § 3^0 do artigo 52 da LGPD, as sanções administrativas pecuniárias não se aplicam às entidades e aos órgãos públicos, o que implica que a ANPD não poderá aplicar as sanções de multa previstas nos incisos II e III do caput do referido artigo.

As sanções são mais do que meramente punitivas, elas servem como um

mecanismo regulatório destinado a influenciar o comportamento das organizações em relação à proteção de dados. Ao examinar casos de não conformidade, a autoridade oferece orientações claras sobre as expectativas em relação à implementação de práticas eficientes de proteção de dados.

Essas sanções têm um impacto direto no incentivo para que as organizações adotem boas práticas. O cumprimento dessas práticas não apenas reduz o risco de punibilidade, mas também demonstra um compromisso proativo com a proteção da privacidade e o respeito aos direitos dos titulares dos dados. Assim, as boas práticas se tornam não apenas uma obrigação legal, mas também uma estratégia de gestão de riscos essencial.

A governança, entendida como a estrutura organizacional que guia e supervisiona o tratamento de dados, emerge como um fator chave na prevenção de violações e, consequentemente, na aplicação de punição. Organizações que implementam práticas de governança robustas demonstram um compromisso estratégico com a conformidade contínua e a proteção dos direitos dos titulares dos dados.

As primeiras sanções aplicadas pela ANPD estabelecem um importante precedente na aplicação da LGPD e incentivam a adoção generalizada de regras de boas práticas e governança. Destaca-se, portanto, a importância de as organizações não apenas cumprirem os requisitos legais, mas também internalizarem uma cultura de proteção de dados que transcenda a conformidade, promovendo confiança e integridade no tratamento de informações pessoais em um ambiente digital em constante evolução.

Para garantir uma efetiva implementação da política pública de proteção de dados, é imperativo que entidades e órgãos públicos adotem medidas de segurança, regras de boas práticas e governança para salvaguardar os dados pessoais contra acessos não autorizados, vazamentos e violações. Fomentar uma cultura de conformidade com a LGPD requer o treinamento de funcionários, a implementação de políticas de privacidade e a nomeação de um Encarregado de Proteção de Dados.

Dois elementos cruciais nesse contexto são o papel do encarregado e a elaboração do RIPD. O encarregado atua como ponto de contato entre a organização, os titulares dos dados e a ANPD, desempenhando um papel estratégico na promoção de uma cultura de proteção de dados. Ele orienta funcionários, responde às solicitações dos

titulares e da autoridade nacional, contribuindo para o cumprimento das normas legais e a transparência na gestão de informações.

O RIPD, embora não seja explicitamente exigido pela LGPD, é uma ferramenta recomendada em diversos setores. Ele visa identificar e mitigar potenciais riscos à privacidade dos titulares durante o tratamento de dados pessoais, proporcionando uma visão clara dos procedimentos adotados pela organização para proteger as informações sob sua responsabilidade. O encarregado, por estar ciente das operações internas, pode desempenhar um papel fundamental na condução ou supervisão da elaboração do RIPD, contribuindo para uma análise mais abrangente e criteriosa.

Assim, a designação de um Encarregado e a elaboração do RIPD não apenas atendem aos requisitos legais, mas também refletem um compromisso ético e responsável por parte das organizações. Além de mitigar riscos legais e financeiros, essas práticas fortalecem a confiança dos titulares, melhoram a reputação da instituição e demonstram um alinhamento proativo com os princípios de proteção de dados pessoais. Em um cenário dinâmico e desafiador, investir na integração efetiva desses elementos é essencial para promover a governança da informação e a sustentabilidade das operações no universo digital.

Para além, no decorrer desta dissertação, foi constatado que as atividades de coleta de dados, tais como matrículas, estágios, controle de presença e avaliação acadêmica, não se enquadram nas exceções previstas pela LGPD para atividades acadêmicas. Diante desse cenário, a hipótese de tratamento e compartilhamento de dados mais relevante para embasar as práticas da universidade é aquela relacionada à execução de políticas públicas. Conforme preconizado pela lei, essa hipótese autoriza a administração pública, como a UFRRJ, a realizar o tratamento de dados necessários à execução de políticas públicas previstas em leis, regulamentos, contratos, convênios ou instrumentos semelhantes.

Após uma análise do panorama da UFRRJ e do cenário atual quanto à adequação e implementação à LGPD, torna-se evidente a necessidade de medidas concretas para garantir a conformidade institucional e proteger os dados pessoais dos estudantes e demais partes envolvidas.

No âmbito do conhecimento dos estudantes sobre a LGPD, a análise do questionário aplicado revelou lacunas significativas, ressaltando a importância de

programas de conscientização e educação sobre proteção de dados. Com base na amostragem realizada, torna-se evidente que a maioria dos estudantes desconhecem a LGPD, uma análise mais aprofundada das respostas revela que mesmo aqueles que estão cientes da legislação desconhecem os seus direitos como titular dos dados

Além disso, foi constatado que a UFRRJ não promove uma divulgação adequada sobre a LGPD entre seus discentes. Embora haja informações sobre o encarregado de dados disponíveis no site, estas não alcançaram os titulares dos dados, uma vez que os mesmo desconhecem quem é o encarregado e não sabem como contactá-lo. Adicionalmente, não há informações claras quanto aos setores que podem acessar os dados tratados pela instituição.

Com base nas análises efetuadas, torna-se inevitável que a universidade adote medidas concretas visando a conscientização dos estudantes acerca da LGPD, a fim de assegurar a efetividade da política pública de proteção de dados, alcançando verdadeiramente os titulares dos dados pessoais. Tal conscientização deve ser disseminada entre os estudantes matriculados atualmente, contudo, para uma maior abrangência, é recomendável a realização de palestras elucidativas sobre a relevância da LGPD durante o período de ingresso dos novos discentes.

É recomendável que a instituição promova uma divulgação contínua e abrangente das medidas adotadas em relação à LGPD por meio das redes sociais, incluindo, mas não se limitando ao Instagram institucional. Esta plataforma em particular desfruta de uma considerável popularidade entre os estudantes, os quais frequentemente a utilizam como meio de acompanhamento e interação com a vida acadêmica e eventos relacionados à instituição. Assim, a divulgação regular de informações sobre a normativa através desses canais de comunicação pode garantir uma maior conscientização e engajamento por parte dos alunos, contribuindo significativamente para a eficácia das iniciativas de conformidade com a legislação de proteção de dados.

Além disso, a investigação do contexto institucional, por meio de entrevistas com representantes-chave da UFRRJ, demonstrou a necessidade de uma abordagem estratégica para a implementação da política de proteção de dados. O questionário aplicado a Pró-reitora Adjunta da PROPLADI e as entrevistas como o Encarregado de Dados, o Coordenador da Coordenadoria de Tecnologia da Informação e Comunicação, a servidora responsável pela segurança da informação e a servidora responsável pelo

Núcleo de Governança de Integridade ofereceram percepções valiosas sobre os desafios e oportunidades enfrentados pela instituição nesse processo.

Em síntese, as respostas obtidas no questionário aplicado à Pró-reitora Adjunta evidenciam uma intenção clara de alinhar a UFRRJ às exigências estabelecidas pela LGPD, além de demonstrar o desejo de implementar boas práticas e governança na instituição. No entanto, também destacam desafios significativos que requerem esforços coordenados e a adoção de estratégias específicas.

Salienta-se que foi constatado que a nomeação do encarregado e a divulgação de seu contato no site institucional representam uma prática positiva já adotada pela universidade, evidenciando um passo inicial na direção da conformidade com a LGPD. A entrevista com o encarregado revelou-se não apenas esclarecedora, mas também indicou uma atuação eficaz desse profissional na UFRRJ, direcionada para a conformidade com a lei. O início do processo de inventário na universidade é destacado como um passo crucial, fornecendo dados indispensáveis para a avaliação dos riscos associados ao tratamento de informações pessoais.

A conscientização da alta administração surge como um fator decisivo nesse contexto, pois a compreensão e o comprometimento das lideranças são essenciais para o êxito na implementação das diretrizes da legislação. Além disso, a capacitação dos servidores, prevista para início de 2024, desempenhará um papel significativo, sendo um elemento-chave para a aplicação efetiva das medidas estipuladas pela legislação.

A entrevista realizada com o Coordenador da COTIC proporcionou uma valiosa fonte de informações para a pesquisa. Ficou evidente a dificuldade enfrentada pela coordenadoria em estabelecer um padrão de excelência, principalmente devido à escassez de mão de obra, agravada pela ausência de códigos de vagas, cujo aumento está condicionado à liberação do MEC. Apesar da estrutura organizacional robusta da coordenadoria, a falta de servidores compromete a eficácia das operações.

É importante destacar que a ausência de um servidor designado para o núcleo de governança resulta na atribuição dessa função ao próprio coordenador, especialmente quando demandado por órgãos externos. Embora demonstre comprometimento da liderança, essa prática também evidencia as limitações operacionais decorrentes da escassez de recursos humanos especializados.

Essas questões, sob a perspectiva da proteção de dados, representam potenciais

pontos de vulnerabilidade. A falta de recursos humanos adequados pode impactar diretamente na capacidade da coordenadoria em garantir a segurança e a integridade dos dados. Portanto, torna-se imprescindível considerar medidas para fortalecer as práticas de governança, visando mitigar possíveis riscos e assegurar a conformidade com as normativas de proteção de dados em vigor.

A entrevista realizada com a servidora encarregada pela segurança da informação desempenhou um papel de destaque para os objetivos desta pesquisa. A colaboração entre o setor de segurança da informação e o encarregado de dados reflete o compromisso institucional em garantir a integridade e a proteção dos dados, reforçando a importância de uma abordagem colaborativa e integrada na implementação das políticas de proteção de dados. Esta colaboração tem o objetivo de garantir o cumprimento das diretrizes estabelecidas pelo Governo Federal em relação à segurança da informação e ao controle da privacidade. A sinergia de esforços representa um avanço significativo para a universidade em seu processo de adequação à lei.

A entrevista conduzida com a servidora responsável pelo Núcleo de Governança de Integridade revela a urgência de fortalecer a governança na UFRRJ, evidenciando lacunas nas práticas existentes que carecem de uma maior integração. A servidora destacou a necessidade de uma governança mais estruturada, centralizada na Reitoria, que englobe diversos aspectos, inclusive a proteção de dados pessoais, que deve ser integrada à garantia da integridade institucional.

Com base nas entrevistas realizadas e na documentação analisada, fica claro que a UFRRJ está empenhada em ajustar-se e implementar as diretrizes da LGPD. No entanto, ainda existem desafios a serem superados e práticas simples que podem ser adotadas para facilitar esse processo. A análise identificou lacunas e áreas de melhoria, sugerindo a necessidade de estratégias mais proativas e abrangentes para garantir a conformidade com a LGPD.

Portanto, foram apontados planos de ação que visam a superação dos desafios identificados e a promoção de uma cultura organizacional alinhada com as melhores práticas estabelecidas pela legislação vigente. Etapas cruciais incluem a análise e mapeamento de dados, seguida pelo desenvolvimento de políticas internas claras e abrangentes. A conscientização e capacitação de todos os envolvidos no manejo de dados também são essenciais para criar uma cultura de responsabilidade.

Além disso, é fundamental avaliar os sistemas tecnológicos da instituição para garantir a segurança e conformidade com a LGPD. O PDI 2023-2027 oferece uma estrutura que pode ser adaptada para abranger a proteção de dados pessoais, e há planos para capacitar os servidores com cursos ministrados pelo encarregado de dados da instituição. A colaboração entre o setor de segurança da informação e o encarregado é um ponto positivo, sendo essencial para garantir a integridade e proteção dos dados.

Essas medidas, quando implementadas de forma eficaz, contribuirão significativamente para a conformidade da instituição à LGPD e a proteção dos dados pessoais dos estudantes. É fundamental que a universidade assuma a responsabilidade pela proteção dos dados pessoais de sua comunidade acadêmica e adote providências para garantir a segurança e privacidade dessas informações. Somente assim poderá cumprir sua missão de fornecer um ambiente educacional seguro e ético para seus discentes e colaboradores.

REFERÊNCIAS

ALENCAR, Leandro Zannoni Apolinário. **O novo Direito Administrativo e a Governança Pública: responsabilidade, metas e diálogo aplicados à Administração Pública no Brasil.** Belo Horizonte: Fórum, 2018.

ANPD. **ANPD conclui processo sancionador contra órgão público.** Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-conclui-processo-sancionador-contra-orgao-publico. Acesso em: 10 nov.2023.

ANPD. **ANPD lança Guia Orientativo sobre Tratamento de Dados Pessoais para Fins Acadêmicos.** Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-orientativo-sobre-tratamento-de-dados-pessoais-para-fins-academicos. Acesso em: 27 jun. 2023.

ANPD. **ANPD sanciona mais um órgão público.** Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-mais-um-orgao-publico. Acesso em: 10 nov.2023

ANPD. **Despacho decisório**. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4286376_relatorio_2_2023.pd. Acesso em: 01 nov. 2023.

ANPD. **No Dia Internacional da Proteção de Dados, ANPD publica Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público.** Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico. Acesso em: 02 jun. 2023.

ANPD. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD).** Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p1. Acesso em: 02 nov. 2023

ANPD. **Resolução CD/ANPD nº1/2021**.Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021. Acesso em: 01 nov 2023.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In:* CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel. **Lei geral de proteção de dados** (Lei no 13.709/2018). São Paulo: Revista dos Tribunais, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. São Paulo: Forense, 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público**. Brasília, 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília, 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas**. Brasília, 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **RESOLUÇÃO CD/ANPD Nº 2.** Diário Oficial da União: Seção: 1, Brasília, DF, n. 20, p. 06, 28 jan. 2022. Disponível em:https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 30 set. 2023.

BRASIL. Congresso Nacional. **Proposta de Emenda à Constituição nº 17 de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Congresso Nacional, 2019. Disponível em: https://www.congressonacional.leg.br/materias/materias- bicamerais/-/ver/pec-17-2019. Acesso em 10 mar. 2023.

BRASIL. Ministério da Economia. **Instrução Normativa SGD/ME nº 117.** Diário Oficial da União: Seção: 1, Brasília, DF, n. 222, p. 92, 20 nov. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596. Acesso em: 10 set. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Processo Administrativo Sancionador nº 00261.000489/2022-62.** Despacho. Diário Oficial da União: seção 1, Brasília, DF, n. 127, p. 74, 06 jul. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/2022-62-dou-imprensa-nacional.pdf. Acesso em: 01 set. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Processo Administrativo Sancionador nº 00261.001969/2022-41.** Despacho. Diário Oficial da União: seção 1, Brasília, DF, n. 192, p. 77, 06 out. 2023. Disponível em: https://www.in.gov.br/web/dou/-/despacho-decisorio-514655381. Acesso em: 01 nov. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Instrução Normativa Conjunta nº 1, de 10 de maio de 2016.** Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/Normativos/instrucao-normativa-conjunta-no-1-de-10-de-maio-de-2016-imprensa-nacional.pdf/view. Acesso em: 03 out. 2023.

COSTA, Marco Antônio F. da; COSTA, Maria de Fátima Barrozo. **Metodologia da Pesquisa: abordagens qualitativas.** Rio de Janeiro: Dos Autores, 2019. e-book.

CRESWELL, John W.; CRESWELL, J. David. **Projeto de pesquisa: Métodos qualitativo, quantitativo e misto**. Tradução de Sandra Maria Mallmann da Rosa. 5 ed. 5 Porto Alegre: Penso, 2021, e-book

DEMO, Pedro. **Pesquisa e informação qualitativa.** Campinas: Papirus , 2017, e-book.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 3. ed. São Paulo: Revista dos Tribunais, 2021, e-book.

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011.

FILGUEIRAS, Fernando. Accountability, democracia e políticas públicas no Brasil. In: RODRIGUES, Marta Maria Assumpção (Org.). **Governança, qualidade da democracia e políticas públicas.** Rio de Janeiro: UFRJ, 2018.

FONTE, Felipe de Melo. **Políticas públicas e direitos fundamentais**. 3. ed. São Paulo: Saraiva, 2021.

FREITAS, Daniel Paulo Paiva de; BLANCHET, Luiz Alberto. A adoção explícita do compliance pela Administração Pública Direta. **Revista do Direito Público**, Londrina, v. 15, n. 3, p. 30-47, dez. 2020.

KISSLER, Leo; HEIDEMANN, Francisco G. Governança pública: novo modelo regulatório para as relações entre Estado, mercado e sociedade? **Revista de Administração Pública**, v.40, n.3, p.479-499, Maio/junho, 2006.

MATTIETTO, Leonardo. Dos Direitos da Personalidade à Cláusula Geral de Proteção da Pessoa. **Revista de Direito da Procuradoria Geral**, Rio de Janeiro: edição especial, 2017, p. 218-232.

MUNIZ, Francisco José; OLIVEIRA, José Lamartine Corrêa de. O Estado de Direito e os Direitos da Personalidade. **Revista de Direito Civil Contemporâneo**, v. 24, memória do direito civil, 2020.

NASCIMENTO, Almir Lima. Instrumentos Jurídicos de Governança e Implementação de Dispositivos da Legislação Brasileira. Revista Latino-americana de Governança, Distrito Federal: v. 2, ed. 037, 2022, p.01-11.

REYMÃO, Ana Elizabeth Neirão; OLIVEIRA, Lis Arrais; KOURY, Suzy Elizabeth Cavalcante. A ANPD e a fiscalização da governança corporativa de proteção de dados. **Revista do Direito Público**, 2023, v.18, n.2, 30–47

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda, Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTOS, Marcelo Pereira dos Santos. **Governança e compliance na administração pública direta**. Rio de Janeiro: Lumen Juris, 2022

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, ano 14, n. 42, p. 179-218, 2020.

SARLET, Ingo Wolfgang; SAAVEDRA, Agostini Giovani. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais. **Revista Direito Público**, v.17, n. 93, p. 33-57, 2020.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 36. ed. São Paulo: Malheiros, 2012.

SOLOVE, Daniel J. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. **San Diego Law Review**, v. 44, n. 4, p. 745-772, Nov./Dec. 2007.

SOLOVE, Daniel J. Understanding Privacy. Estados Unidos da América: Harvard University, 2008. E-book.

SOLOVE, Daniel J.; SCHWARTZ, Paul M. **Consumer Privacy and Data Protection** Estados Unidos da América: Aspen, 2021. E-book

SOLOVE, Daniel J.; SCHWARTZ, Paul M. **Eu Data Protection and the GDPR**. Estados Unidos da América: Aspen, 2021. E-book

SUPREMO TRIBUNAL FEDERAL. **Tema 698**. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=4237089&numeroProcesso=684612&classeProcesso=RE&numeroTema=698. Acesso em: 02 nov. de 2023.

UFRRJ. **Relatório de gestão 2022**. Seropédica, 2022. Disponível em: https://portal.ufrrj.br/wp-content/uploads/2023/05/RG_2022.pdf. Acesso em: 21 out. 2023.

UFRRJ. **Acesso à Informação.** Seropédica, 2023. Disponível em: https://institucional.ufrrj.br/acessoainformacao/protecao-de-dados-pessoais/. Acesso em: 04. nov. 2023.

UFRRJ. **Ouvidoria.** Seropédica, 2022. Disponível em: https://portal.ufrrj.br/ouvidoria/protecao-de-dados-pessoais/. Acesso em: 04. nov. 2023.

USP. **Cálculo Amostral**. São Paulo: 2023. Disponível em: http://estatistica.bauru.usp.br/calculoamostral/ta_ic_proporcao.php. Acesso em: 14 set. 2023.

VALLE, Vanice Regina Lírio do; SANTOS, Marcelo Pereira dos. Governança e compliance na administração direta: ampliando as fronteiras do controle democrático. **Revista de Direito Administrativo & Constitucional**, ano 19, n. 75, 2019.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy.**Harvard Law Review**, v. 4, n. 193, 1890.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.