UNIVERSIDADE FEDERAL DE MINAS GERAIS
Escola de Ciência da Informação
Programa de Pós-Graduação em Ciência da Informação

Daiane Coutinho da Rocha Ferreira

O PAPEL DO ARQUIVISTA PARA A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: as relações conceituais entre o gerenciamento arquivístico e a governança arquivística

Belo Horizonte
2025

Daiane Coutinho da Rocha Ferreira

O PAPEL DO ARQUIVISTA PARA A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: as relações conceituais entre o gerenciamento arquivístico e a governança arquivística

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Escola de Ciência da Informação da Universidade Federal de Minas Gerais, Correspondente a linha de pesquisa: Políticas Públicas e Organização da Informação, como requisito para obtenção do título de Mestre.

Orientador: Prof. Dr. Welder Antônio Silva

Belo Horizonte

2025

F383p

Ferreira, Daiane Coutinho da Rocha.

O papel do arquivista para a implementação da lei geral de proteção de dados pessoais [recurso eletrônico] : as relações conceituais entre o gerenciamento arquivístico e a governança arquivística / Daiane Coutinho da Rocha Ferreira. - 2025.

1 recurso online (177 f. : il., color.) : pdf.

Orientador: Welder Antônio Silva.

Dissertação (mestrado) – Universidade Federal de Minas Gerais, Escola de Ciência da Informação.
Referências: f. 158-168.
Apêndice: f. 169-177.
Exigência do sistema: Adobe Acrobat Reader.

1. Ciência da informação - Teses. 2. Arquivistas - Teses. 3. Proteção de dados - Teses. 4. Lei Geral de Proteção de Dados Pessoais (LGPD) - Teses. 5. Direito à privacidade - Teses. I. Silva, Welder Antônio. II. Universidade Federal de Minas Gerais. Escola de Ciência da Informação. III. Título.

CDU 004.6

Ficha catalográfica: Vanessa Marta de Jesus - CRB/6-2419
Biblioteca Profª Etelvina Lima, Escola de Ciência da Informação da UFMG

UNIVERSIDADE FEDERAL DE MINAS GERAIS
ECI - COLEGIADO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ATA DE DEFESA DE DISSERTAÇÃO

Às 15h00 horas do dia 17 de Junho de 2025, de modo Hibrido: Presencial (na sala 1000 Auditório Adriana Bogliolo Presencial) e Online, realizou-se a sessão pública para a defesa de Dissertação de mestrado de Daiane Coutinho da Rocha Ferreira**.** A presidência da sessão coube ao Welder Antônio Silva (Orientador). Inicialmente, o presidente fez a apresentação da Comissão Examinadora assim constituída: Cintia Aparecida Chagas (UFMG), Bianca Therezinha Carvalho Panisset (FCR) e Welder Antônio Silva (UFMG). Em seguida, a candidata fez a apresentação do trabalho que constitui sua dissertação de mestrado intitulada : ''O PAPEL DO ARQUIVISTA PARA A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: as relações conceituais entre o gerenciamento arquivístico e a governança arquivística''**.** Seguiu-se a arguição pelos examinadores e logo após a Comissão reuniu-se sem a presença da candidata e do público e decidiu considerar aprovada a dissertação de mestrado com o registro de sua relevância intelectual. A banca destacou o ineditismo do tema e recomendou a publicação em periódicos científicos. O resultado final foi comunicado publicamente à candidata pelo presidente da Comissão. Nada mais havendo a tratar, o presidente encerrou a sessão e lavrou a presente ata que depois de lida e aprovada, será assinada pela Comissão Examinadora.

Belo Horizonte, 17 de Junho de 2025.

Welder Antônio Silva (UFMG)

Cintia Aparecida Chagas (UFMG)

Bianca Therezinha Carvalho Panisset (UFF)

Documento assinado eletronicamente por **Welder Antonio Silva**, **Professor do Magistério Superior**, em 18/06/2025, às 11:14, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cintia Aparecida Chagas**, **Professora do Magistério Superior**, em 18/06/2025, às 12:53, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Bianca Therezinha Carvalho Panisset**, **Usuária Externa**, em 18/06/2025, às 13:42, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado condições para chegar até aqui e que, por meio do seu amor, me concedeu a força e a resiliência necessárias para os momentos de fraquezas e angústias.

Ao meu orientador e mentor, Dr. Welder Antônio Silva, pelos seus ensinamentos e pelas trocas diárias. Com sua generosidade, esteve sempre disponível, orientando-me durante toda essa trajetória, contribuindo para o meu desenvolvimento não só na temática da pesquisa, mas também no desenvolvimento de habilidades como planejamento, análise crítica e pensamento estratégico, e que, por muitas vezes, me ensinou a hora de parar. Agradeço imensamente pelas orientações.

Ao Programa de Pós-graduação em Ciência da Informação da Universidade Federal de Minas Gerais (PPGCI/UFMG), agradeço pelo espaço de aprendizagem, que contribuiu para a minha formação profissional e humana. Aos professores que colaboraram com as disciplinas, fomentando as discussões sobre a temática das políticas públicas e organização da informação. Em especial à professora Ivana Parrela, que trouxe vários apontamentos e boas reflexões sobre o tema da proteção de dados.

Ao meu companheiro de vida, Eder Lucas, que topou me acompanhar nessa jornada, sendo um pilar essencial para que eu pudesse dedicar meu tempo aos estudos e à pesquisa. Agradeço pelo amor e cuidado em nossa rotina, mesmo quando minha presença física não era sinônimo de presença real. Obrigada por tornar os dias mais leves, dando suporte a mim e aos meus pais. Eu amo você.

Com profunda gratidão, agradeço à minha mãe, Adenizia, ao meu pai, Sebastião, à minha avó, Carmita, à minha tia, Gircilene, e ao meu irmão, Marcos Vinícius. Agradeço o apoio constante e as orações de vocês para a minha jornada. Vocês me legaram valores inegociáveis como a humildade, a ética e o senso de justiça, alicerces que me sustentam. Nos momentos de necessidade, pude retornar ao meu lar, beber da fonte de suas experiências e sabedoria, e encontrar o equilíbrio e a força para seguir adiante com resiliência e alegria. Agradeço o amor e o carinho que compartilhamos de forma discreta e singela.

À querida amiga Elaine Almeida, minha dupla de orientação, sou grata ao destino por nos conectar. Agradeço-te pelo apoio constante nos momentos em que o desânimo e o cansaço insistiam em permanecer. Foram dias, meses e anos de muitas trocas e boas experiências ao seu lado. Te levarei comigo!

Um agradecimento especial a todos os meus amigos. Agradeço por cada mensagem de incentivo, por cada ligação e pela compreensão das minhas ausências. E às novas amizades que o mestrado me apresentou, em especial às amigas das aulas de segunda-feira, agradeço pelos momentos de descontração, acolhimento e espontaneidade.

À Associação dos Servidores Municipais da Prefeitura de Belo Horizonte (ASSEMPBH), meu local de trabalho, onde dedico parte da minha jornada à atuação no Programa de Privacidade e Proteção de Dados. Agradeço ao presidente Anselmo Horta Nassif, à minha gestora, Raquel Ribeiro, pela confiança no meu trabalho, e à minha equipe do Arquivo. Agradeço à Comissão Gestora de Privacidade e Proteção de Dados pelas trocas e aplicação prática diariamente. Em especial, agradeço a Danielle Santos e ao Victor Tavares por todo o apoio e as contribuições dos últimos cinco anos, em que unimos a Arquivologia, o Direito e a Tecnologia para a construção de um ambiente informacional seguro e com respeito aos direitos fundamentais.

Agradeço à banca avaliadora, que contribuiu para o desenvolvimento desta pesquisa com apontamentos e reflexões importantes. Professora Cíntia Aparecida Chagas, Professora Bianca Therezinha Carvalho Panisset, Professor Renato Venâncio e Professor Adalson de Oliveira Nascimento, minha imensa gratidão.

Agradeço às associações de arquivistas e ao Fórum Nacional das Associações de Arquivologia do Brasil (FNArq) pela valiosa contribuição na divulgação desta pesquisa, que alcançou arquivistas em todo o país. Por fim, minha gratidão a todos os arquivistas que colaboraram ao responder ao questionário e compartilhar informações tão importantes sobre a sua formação e experiências adquiridas na área de proteção de dados.

RESUMO

Esta pesquisa investigou o papel do arquivista no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), n.º 13.709/2018, que visa proteger os direitos fundamentais de liberdade, privacidade e a livre formação da personalidade. Justificou-se, assim, a necessidade de aprofundar o entendimento e estimular o desenvolvimento do pensamento crítico acerca da cultura de privacidade e proteção de dados nas organizações públicas e privadas no Brasil, sobretudo a atuação do arquivista como possível responsável pelo tratamento de dados ou como membro de comitês de governança em privacidade. Para tanto, o estudo explorou leis de privacidade internacionais e sua relação com o cenário brasileiro e propôs a contextualização de conceitos e princípios relevantes para a temática. Ademais, a pesquisa analisou as diretrizes da LGPD, refletindo de forma comparativa entre a função do arquivista e do encarregado de dados no Brasil, analisando as competências e habilidades a partir da Lei n.º 6.546/1978 e da Resolução CD/ANPD n.º 18/2024 e outros normativos pertinentes. Identificaram-se as convergências e semelhanças entre as atribuições e competências desses profissionais. A pesquisa ainda se propôs a analisar, a partir dos princípios de governança (integridade, transparência, prestação de contas e responsabilidade), sua contribuição para a governança e gerenciamento arquivísticos, contribuindo para a efetiva implementação da LGPD, bem como a relevância para a avaliação da maturidade organizacional, nos aspectos da gestão de riscos. A metodologia adotada foi qualitativa e exploratória, com o propósito de estudar a experiência e vivência dos profissionais arquivistas e o processo de implementação da lei. A coleta e análise de dados ocorreu a partir de aplicação de questionário elaborado por meio da escala Likert, e seu desenvolvimento foi construído com base na definição de eixos centrais identificados durante a revisão de literatura. Além disso, procedeu-se à análise de fontes documentais, inclusive fontes primárias, visando obtenção de informações acerca da implementação da proteção de dados. Os resultados demonstraram que os profissionais arquivistas analisados compreendem a importância do tema para a área da Arquivologia. Também consideram, em diferentes níveis, porém de forma positiva, a responsabilidade arquivística e a gestão de riscos em favor de uma atuação eficaz para a implementação da governança organizacional. Por fim, enfatiza-se a importância de os profissionais arquivistas buscarem um processo contínuo de aquisição de conhecimento para a ocupação de espaços estratégicos que visam à promoção do acesso aos documentos.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD); governança arquivística; responsabilidade arquivística; gerenciamento de riscos; profissional arquivista

ABSTRACT

This research investigated the role of the archivist professional within the context of the General Data Protection Law (LGPD), n.º 13.709/2018, which aims to protect the fundamental rights of freedom, privacy, and the free development of personality. Thus, the need to deepen understanding and stimulate the development of critical thinking about the culture of privacy and data protection in public and private organizations in Brazil was justified, especially the archivist's role as a possible data controller or as a member of privacy governance committees. To this end, the study explored international privacy laws and their relationship with the Brazilian scenario and proposed the contextualization of relevant concepts and principles for the topic. Furthermore, the research analyzed the guidelines of the LGPD, comparatively reflecting on the function of the archivist and the data protection officer in Brazil, analyzing their skills and abilities based on Law n.º 6.546/1978 and Resolution CD/ANPD n.º 18/2024, and other pertinent regulations. The convergences and similarities between the duties and competencies of these professionals were identified. The research also aimed to analyze, based on the principles of governance (integrity, transparency, accountability, and responsibility), their contribution to archival governance and management, contributing to the effective implementation of the LGPD, as well as its relevance for assessing organizational maturity in the aspects of risk management. The methodology adopted was qualitative and exploratory, with the purpose of studying the experience and lived experiences of archivist professionals and the law's implementation process. Data collection and analysis occurred through the application of a questionnaire constructed based on the definition of central axes. In addition, documentary sources, including primary sources, were analyzed to obtain information about the implementation of data protection. The results demonstrated that the analyzed archivist professionals understand the importance of the topic for the field of Archival Science. They also consider, at different levels but positively, archival responsibility and risk management in favor of effective action for the implementation of organizational governance. Finally, the importance of archivist professionals seeking a continuous process of knowledge acquisition for occupying strategic spaces aimed at promoting access to documents is emphasized.

Keywords: General Law for the Protection of Personal Data (LGPD); archival governance; archival responsibility; risk management; archivist professional

LISTA DE GRÁFICOS

Gráfico 1 - Aceite dos profissionais ao questionário……..…...88
Gráfico 2 - Questão 01 do Questionário…….……..89
Gráfico 3 - Questão 02 do Questionário.…….…..……90
Gráfico 4 - Questão 03 do Questionário…….……..91
Gráfico 5 - Questão 04 do Questionário…….…..…….92
Gráfico 6 - Questão 05 do Questionário…….……..94
Gráfico 7 - Questão 06 do Questionário…….……..95
Gráfico 8 - Questão 07 do Questionário…….……..96
Gráfico 9 - Questão 08 do Questionário…….……..98
Gráfico 10 - Questão 09 do Questionário…….……99
Gráfico 11 - Questão 10 do Questionário……...…….100
Gráfico 12 - Questão 11 do Questionário……101
Gráfico 13 - Questão 12 do Questionário……...…102
Gráfico 14 - Questão 14 do Questionário……..…….104
Gráfico 15 - Questão 15 do Questionário……...……106
Gráfico 16 - Questão 17 do Questionário……...……108
Gráfico 17 - Questão 18 do Questionário……...……109

LISTA DE FIGURAS

Figura 1- Entendendo as dinâmicas do gerenciamento de dados centrada no indivíduo…….32
Figura 2 - Leis de Privacidade no Mundo…….....45
Figura 3 - Linha do tempo das fases da LGPD e leis correlatas……..….61
Figura 4 - LGPD - Objetivos e Princípios…….……64
Figura 5 - Competências e Habilidades para o Gerenciamento Arquivístico…….……..75
Figura 6 - Avaliação da Maturidade de Governança da Informação e de Documentos para a Gestão de Riscos……...152

LISTA DE QUADROS

Quadro 1 - Legislações de Proteção de Dados e Privacidade em todo o mundo……...……46
Quadro 2 - Leis de Privacidade dos Países Membros do Mercosul……52
Quadro 3 - Leis de Privacidade Países Membros do BRICS……...….57
Quadro 4 - Classificação Brasileira de Ocupações de Arquivista……77
Quadro 5 - Semelhanças e convergências entre as atribuições do Arquivista e do Encarregado……..83
Quadro 6 - Exemplos de Implementação de Boas Práticas - Questão n.º 13……..……103
Quadro 7 - Exemplos de Implementação na Gestão de Riscos - Questão n.º 16 do Questionário……..……..107
Quadro 8 - Princípios de Acesso a Arquivos: orientações para arquivos com restrições……129
Quadro 9 - Etapas da Elaboração para o Programa de Governança em Privacidade……..147

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
BRICS	Brasil, Rússia, Índia, China, South Africa
CBO	Classificação Brasileira de Ocupação
CIPFA	Chartered Institute of Public Finance and Accountancy
CGU	Controladoria Geral da União
CNJ	Conselho Nacional da Justiça
CNPD	Conselho Nacional de Proteção de Dados Pessoais e da Privacidade
DPO	*Data Protection Officer*
DPDPA	*Digital Personal Data Protection Act*
GARP-IG	*Modelo Information Governance Maturity Model / Generally Accepted Recordkeeping Principles – Information Governance*
GDPR	*General Data Protection Regulation*
ICA	*International Council on Archives*
ISO	*International Organization of Standardization*
ISO/IEC	*International Organization of Standardization / International Electrotechnical Commission*
KPI	*Key Performance Indicator*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
IBGC	Instituto Brasileiro de Governança Corporativa
PEID	Pequenos Estados Insulares em Desenvolvimento
PMD	Países Menos Desenvolvidos
PbD	*Privacy by Design*
MEC	Ministério da Educação
RBG	Referencial Básico de Governança
SERPRO	Serviço Federal de Processamento de Dados
TCU	Tribunal de Contas da União
UFMG	Universidade Federal de Minas Gerais
UNCTAD	Conferência das Nações Unidas sobre Comércio e Desenvolvimento

SUMÁRIO

1 INTRODUÇÃO..... 16

1.2 Contextualização da temática de pesquisa: a justificativa, os objetivos e o problema. 19

1.3 Procedimentos metodológicos..... 27

2 EVOLUÇÃO DAS LEIS DE PRIVACIDADE..... 30

2.1 Conceituação da privacidade como direito fundamental..... 34

2.2 O surgimento do direito à Autodeterminação Informativa..... 40

2.3 As Leis de Privacidade pelo Mundo e impactos no cenário brasileiro..... 43

3 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL..... 59

3.1 As diretrizes da Lei Geral de Proteção de Dados Pessoais..... 63

4 AVALIAÇÃO DAS COMPETÊNCIAS DO ARQUIVISTA NO CONTEXTO DA PROTEÇÃO DE DADOS..... 70

4.1 A Normatização da atuação do Arquivista..... 73

4.2 A função do encarregado pelo tratamento de dados pessoais..... 78

4.3 Análise comparativa dos regulamentos das funções do Arquivista e do Encarregado pelo tratamento de dados..... 82

5 ANÁLISE E APRESENTAÇÃO DOS RESULTADOS..... 86

5.1 Seleção da população e amostra..... 86

5.2 Análise da coleta e apresentação dos resultados..... 87

6 OS PRINCÍPIOS DE GOVERNANÇA EM RELAÇÃO À PROTEÇÃO DE DADOS A FAVOR DE UMA GOVERNANÇA ARQUIVÍSTICA..... 112

6.1 Os princípios de integridade, transparência, prestação de contas, responsabilidade no contexto dos arquivos..... 117

6.1.1 O Princípio da integridade..... 118

6.1.2 O princípio da transparência..... 121

6.1.3 O princípio da prestação de contas e responsabilidade (accountability)..... 132

6.2. A gestão de riscos como foco da governança em privacidade e proteção de dados.. 141

7 CONSIDERAÇÕES FINAIS..... 153

REFERÊNCIAS..... 159

APÊNDICE A - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO - TCLE..
…….170
APÊNDICE B - QUESTIONÁRIO APLICADO.....172

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) n.º 13.709, publicada em 14 de agosto de 2018, foi criada com o propósito de proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Essa lei versa sobre o tratamento de dados realizado por pessoas físicas ou jurídicas, abrangendo um amplo conjunto de operações tanto em meios manuais quanto digitais.

A LGPD possui como referência, a General Data Protection Regulation (GDPR)[1], regulamentação de proteção de dados sancionada pela União Europeia (EU), e em vigor desde 25 de maio de 2018. A GDPR visa harmonizar as leis de proteção de dados entre os países membros da União Europeia, estabelecendo um conjunto comum de regras para a proteção de dados pessoais. Apoiada a uma série de requisitos para que as organizações utilizem os dados pessoais, com o intuito de garantir o respeito aos princípios e diretrizes determinados na lei.

Como fundamentos principais, a Lei Geral de Proteção de Dados Pessoais se encontra pautada na Constituição Federal de 1988, especificamente nos artigos 1º e 5º. Isso diz respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião. Além disso, abrange a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico, 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.

A LGPD também se relaciona com outros dispositivos normativos[2], como a Lei de Acesso à Informação, cujo objetivo é garantir o direito dos cidadãos ao acesso à informação. Estabelece condições nas quais os dados e informações pessoais deverão ser tratados, a partir de uma definição de conjunto de direitos para os titulares dos dados, gerando obrigações específicas para as empresas. Essas obrigações estão relacionadas a uma série de procedimentos e normas que devem ser seguidas em concordâncias com os princípios da boa-fé, transparência, segurança, prevenção, a não-discriminação, a responsabilização, prestação de contas. Também aborda o acesso aos documentos e privacidade dos indivíduos.

Parte-se dos pressupostos que esses são princípios básicos para garantir a *compliance* regulatória, a governança corporativa e a governança arquivística, servindo como base para o tratamento adequado dos dados pessoais. Para elucidar o conceito de governança segundo o Referencial Básico de Governança:

---

[1] GDPR – tradução em português: Regulamento Geral de Proteção de Dados
[2] Lei n.º 8.078/1990; Lei n.º 12.527/2011; Lei 12.414/2011; Lei 12.965/2014

> Governança no setor público compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (Brasil, 2014, p. 26).

Observa-se uma aproximação e aplicabilidade que os arquivos têm a partir dos princípios da governança para a colaboração da prestação de contas, a responsabilidade e a transparência em órgãos públicos. Iacovino (2009), em *"Os arquivos como arsenais de responsabilidade"* destacou que:

> Os termos "prestação de contas" ou "responsabilidade" (*accountability*) são sinônimo de "transparência", "abertura" e "confiança", em oposição à "segredo", "escamoteação" e "corrupção". Em países que possuem governos democraticamente eleitos, esses termos são sinônimo de acesso aberto aos arquivos de Estado" (Iacovino, 2009, p. 261).

Essa pesquisa pretende analisar e propor reflexões, correlacionando as atribuições do arquivista, para além das funções arquivísticas, enquanto agente indispensável para a implementação da Lei Geral de Proteção de Dados no âmbito dos arquivos públicos e privados, respeitando os direitos fundamentais de privacidade e proteção de dados, bem como outros direitos do ordenamento jurídico.

Para organizar toda a estrutura exigida pela legislação, na transformação de suas diretrizes e princípios em ordenamentos jurídicos, procedimentos administrativos, medidas técnicas e de segurança da informação, e ainda, em aplicações das funções arquivísticas, percebe-se que há necessidade de um envolvimento interdisciplinar. A colaboração entre diversas áreas é essencial para garantir uma implementação eficaz da Lei Geral de Proteção de Dados (LGPD) e assegurar o cumprimento regulatório.

Nesse contexto, é fundamental reconhecer a possibilidade de o **arquivista** assumir esses papéis: tanto como responsável pelo tratamento de dados, atuando na função de **Encarregado pelo Tratamento de Dados (DPO)**, que é a pessoa indicada para mediar a relação entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), quanto como **membro de comitês de governança em privacidade e proteção de dados**.

Observa-se que o bom desempenho da função de arquivista é vital para os programas de privacidade e proteção de dados, uma vez que os documentos resultantes dessas atividades e do tratamento de dados, são objetos da área, independentemente do suporte utilizado.

Em consonância com essas considerações, é relevante validar o conceito de arquivo à luz das disposições gerais da política nacional de arquivos públicos e privados, conforme estabelecido na Lei de Arquivos (1991). De acordo com essa legislação, os arquivos são definidos como conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em virtude do exercício de atividades específicas, bem como por pessoas físicas, independentemente do suporte da informação ou da natureza dos documentos.

A partir disso, considera-se que, para a efetiva atuação dos arquivistas, são necessárias atualizações constantes para garantir que as práticas de gestão e governança arquivística estejam alinhadas com a LGPD. Diante desses aspectos, é importante refletir, sobre o seguinte problema de pesquisa: **de que maneira o conhecimento e a colaboração do arquivista podem contribuir para a conformidade da Lei Geral de Proteção de Dados, considerando os aspectos do gerenciamento arquivístico e da governança arquivística?**

Assim, o objetivo geral desta pesquisa será, analisar o papel do arquivista quando se encontra nessa condição de encarregado pelo tratamento de dados, destacando sua contribuição para a avaliação da maturidade organizacional e para o desenvolvimento de indicadores pertinentes para a gestão de riscos e a eficaz prestação de contas conforme as exigências legais.

A seguir, como desdobramento do objetivo geral, delineiam-se os seguintes objetivos específicos para seu desenvolvimento desta pesquisa:

a) compreender os princípios fundamentais da Lei Geral de Proteção de Dados;
b) avaliar as competências necessárias para que o arquivista possa atuar como mediador da gestão de riscos em um programa de privacidade e proteção de dados.
c) investigar os aspectos da governança arquivística, embasando-se nos princípios de integridade, transparência, prestação de contas e responsabilidade, a partir das diretrizes da LGPD.

Para melhor entendimento, esta pesquisa foi desenvolvida em sete seções. A primeira seção foi destinada à introdução e à contextualização da temática desta pesquisa, apresentando a justificativa, os objetivos, problema que norteou este estudo e procedimentos metodológicos.

A segunda seção foi destinada à compreensão da evolução das leis de privacidade, à conceituação da privacidade como um direito fundamental e, em consequência, ao surgimento

do direito à autodeterminação informativa. Ademais, a seção busca compreender o desenvolvimento das leis de privacidade no mundo e seus impactos no cenário brasileiro, considerando ainda a livre circulação dados e a transferência internacional.

A seção três trata das fases de desenvolvimento da temática de proteção de dados no Brasil e sua evolução até a aprovação da Lei Geral de Proteção de Dados. Além disso, a seção aborda a reflexão das diretrizes e princípios que regem as atividades realizadas com os dados pessoais, sobretudo no contexto dos arquivos

A seção quatro destina-se a avaliar as competências do arquivista no contexto da proteção de dados. A proposta é compreender a normatização da atuação desse profissional em uma relação comparativa com a função do encarregado pelo tratamento de dados pessoais, buscando encontrar semelhanças e convergências.

A quinta seção destina-se à análise e apresentação dos resultados, o que compreende o delineamento da coleta de dados, a seleção da população referente aos arquivistas, os recursos e ferramentas utilizadas para o alcance desses profissionais e a contextualização das perguntas. O desenvolvimento do questionário teve como critérios aspectos que dizem respeito à proteção e integridade dos conteúdos dos documentos, à responsabilidade arquivística, à gestão de riscos e à prestação de contas em relação à transparência.

Em seguida, a sexta seção destina-se a compreender a contribuição da governança arquivística, tendo como base a análise dos princípios de governança institucional e corporativa, observando seus princípios e diretrizes para a proteção de dados, bem como sua relevância para a avaliação da maturidade organizacional. Diante disso, esta seção objetiva investigar como a governança se manifesta em relação aos princípios da integridade, da transparência, da prestação de contas e da responsabilidade.

Por fim, a sétima seção destina-se às considerações acerca desta pesquisa.

1.2 Contextualização da temática de pesquisa: a justificativa, os objetivos e o problema

Com o propósito de estimular o desenvolvimento do pensamento crítico acerca da cultura de privacidade e proteção de dados nas organizações públicas e privadas no Brasil, despertou-se o interesse pela temática, sob a perspectiva dos arquivos. Numa abordagem interdisciplinar com outras áreas, a pesquisa se caracteriza, pela aplicabilidade das questões tecnológicas e do direito, da teoria e a prática da segurança da informação e juntamente com a gestão de riscos para uma boa governança.

Apresenta-se ainda a justificativa sob a ótica da Ciência da Informação, corroborando nos argumentos de Gonzalez de Gomez (1990):

> O que constituiria um domínio da Ciência da Informação não seria, conforme esta análise, a qualidade de um campo de fenômenos de informação (informação científica, informação tecnológica, informação para a cidadania), mas a instauração de um "ponto de vista" que recorre a uma ampla zona transdisciplinar, com dimensões físicas comunicacionais, cognitivas e sociais ou antropológicas. Esse "ponto de vista" não teria como objeto a informação e suas especificações, mas antes as pragmáticas sociais de informação, ou, dito em termos mais frequentes, a metainformação e suas relações com a informação. Esse "objeto" da Ciência da Informação não seria logo uma "coisa" ou uma "essência" de uma região de fenômenos, mas um conjunto de regras e relações tecidas entre agentes, processos e produções simbólicas e materiais (Gómez, 1990, p. 121).

Nessa mesma direção, Jardim (2018) em ***"Governança Arquivística:*** *um território a ser explorado"* nos propõem a refletir sobre os redesenhos da teoria e a prática arquivísticas nas últimas décadas, com impactos na pesquisa e na formação do arquivista de forma intensa e complexa:

> É mais evidente em algumas realidades sociais do que em outras. Porém, perpassa várias "tradições arquivísticas" com impactos na gestão de instituições e serviços arquivísticos, na produção científica em Arquivologia e na formação e perfil do arquivista. Esses redesenhos na Arquivologia ocorrem sob forte influência das tecnologias da informação, da emergência de novos modelos organizacionais, dos princípios do governo aberto e das crescentes demandas sociais pelo direito à informação, à memória e à privacidade (Jardim, 2018, p. 12).

Refletir sobre a responsabilidade do arquivista, tanto no âmbito das obrigações legais quanto éticas, ganha significância ao explorar o conceito de "responsabilidade arquivística" proposto por Iacovino (2009), em relação ao desafio do cumprimento da legislação de privacidade e proteção de dados, bem como do acesso às informações.

Nessa abordagem, a autora descreve os arquivos como arsenais de responsabilidade, sendo possível compreender a importância do profissional para o papel da salvaguarda das informações e no cumprimento das normativas vigentes.

Conforme destacado por Iacovino (2009), embora os arquivos não tenham a capacidade de evitar a ocorrência da corrupção, desempenham um papel fundamental na sua detecção. A autora sustenta a ideia de que, mesmo que os arquivos não possam impedir a corrupção, eles são componentes essenciais para sua identificação, destacando, portanto, a

importância do arquivista na promoção da responsabilidade pública, consequentemente a prestação de contas e a transparência.

> No pensamento arquivístico, as ideias sobre essa qualidade foram moldadas por acontecimentos sociais e políticos, por mudanças tecnológicas e institucionais e por uma série de disciplinas, que inclui a ética, o direito, a história, as ciências sociais, a auditoria, a gestão de riscos, a informática e a própria ciência arquivística. A maneira como os arquivistas percebem a responsabilidade está atrelada à forma como a disciplina arquivística surgiu e se desenvolveu em cada país, especialmente em relação ao papel do arquivista na gestão de documentos. Boa parte do pensamento em questão concentrou-se no papel da autoridade arquivística pública, nas normas éticas do arquivista e no seu papel enquanto agente da responsabilidade (Iacovino, 2009, p. 262).

Na perspectiva da profissão do arquivista, Iacovino (2009) considera que enquanto agente de responsabilidade, nenhuma profissão pode permanecer alheio ao seu tempo e lugar, sendo esse de grande importância estar envolvido nos acontecimentos correntes, contribuindo para "liberdades de ação". Em concordância com as pesquisas de Bellotto (1991) ao afirmar ser fundamental e indispensável a compreensão da mudança no papel do arquivista, se tornando mais amplo e mais proativo, podendo ser considerado como instrumento da administração e do direito, ou do testemunho da história e do exercício da cidadania.

No que diz respeito sobre a importância dos arquivos para a sociedade, é irrefutável, ainda que de forma não tão clara, o reconhecimento pela população sobre a função do arquivo, o que é, e para que serve. Bellotto (2014, p. 221) afirmava que:

> A existência de arquivos e sua necessidade para o governo, para as empresas e para o cidadão são inquestionáveis. Nos países em que os arquivos "mostram a sua face" de maneira clara e evidente, seu uso faz se de forma eficiente; já nos países que tardaram em reconhecer-lhes a importância do fluxo, na transferência e na utilização da informação, torna-se difícil "achar" seu caminho (Bellotto, 1996)[3].

Cabe revisitar a resposta de Delmas (2010, p. 20), em "Arquivos servem para quê?", ao considerar a importância arquivos como continuidade para o funcionamento de uma sociedade organizada e a necessidade para a sua conservação:

> Conservar seus arquivos é um ato indispensável. Eles são o produto necessário do funcionamento de toda sociedade organizada. Quanto mais

[3] Trecho retirado do texto publicado originalmente em **Arquivo & História**, Rio de Janeiro, n. 2, p.7-16, 1996.

> uma sociedade se desenvolve, mais as atividades humanas são numerosas, diversificadas e interdependentes. Quanto mais documentos são usados para que os homens registrem seus atos e asseguram a sua continuidade e estabeleçam relacionamentos duráveis entre si, mais eles produzem e conservam arquivos (Delmas, 2010).

Conforme destacou Delmas (2010, p. 19-20), a conservação dos arquivos, é um ato indispensável, seja para **provar e defender os direitos**, seja lembrar sobre o que foi feito e conhecimento para agir, seja para **compreender o que foi feito**, descoberto e documentado ou para a **identificação da existência** e a **promoção das relações sociais**. Ainda que a sociedade não saiba responder com precisão, os arquivos impactam diariamente na vida das pessoas, sobretudo a continuidade das estruturas administrativas governamentais, a exemplo para a transparência ou prestação de contas de usos e gastos de recursos públicos.

Na direção da abordagem de Delmas, o arquivista desempenha um importante papel na "conservação dos arquivos", enquanto produto de desenvolvimento da sociedade e das relações humanas. Jardim (2018, p. 12) também destacou a complexidade e intensidade das relações sociais e os impactos desse cenário na gestão de instituições e serviços arquivísticos, sobretudo no que confere a formação e o perfil do arquivista, inclusive na condição de gestor "de um determinado tipo de recursos vital às organizações: as informações registradas nos documentos que derivam de suas ações" (Jardim, 2018, p. 12).

Nesse sentido, aborda-se como pressuposto nessa pesquisa à possível atuação do arquivista como agente responsável da condução do cargo de Encarregado pelo Tratamento de Dados Pessoais, considerando os aspectos de gestão e governança, conforme transcende a ideia reducionista de organização dos arquivos. Uma vez que, gerenciar também envolve "administrar pessoas, tecnologias da informação, infraestrutura física, legislação, orçamentos, ademais de requerer um grande conhecimento do contexto contemporâneo das organizações e suas alterações ao longo do tempo"(Jardim, 2018, p.12).

Destaca-se a relevância em analisar e identificar as atribuições que o arquivista precisa adquirir ou aprimorar para desempenhar efetivamente essa função. Considerando diversos aspectos, tais como a proteção e integridade do conteúdo dos documentos, a responsabilidade arquivística, desde o momento de sua produção, a formulação de indicadores para controle e monitoramento no gerenciamento de riscos associados à utilização dos dados.

A Lei Geral de Proteção de Dados determinou responsabilidades ao profissional a ocupar a função de encarregado pelo tratamento de dados pessoais, que compreende as seguintes atribuições:

> Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e contratados da entidade sobre a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (Brasil, 2018).

Com base nisso, faremos uma breve análise das competências e habilidades exigidas para as funções de arquivista e encarregado pelo tratamento de dados (DPO). É fundamental compreender as semelhanças entre suas atribuições, conforme delineado pela Lei do Arquivista (n.º 6.546/1978) e pela Lei Geral de Proteção de Dados (n.º 13.709/2018), respectivamente. A propósito, vale destacar as atribuições e responsabilidades destinada ao arquivista, conforme rege o artigo 2º:

> Art. 2º - São atribuições dos Arquivistas - planejamento, organização e direção de serviços de Arquivo; II - planejamento, orientação e acompanhamento do processo documental e informativo; III - planejamento, orientação e direção das atividades de identificação das espécies documentais e participação no planejamento de novos documentos e controle de multicópias; IV - planejamento, organização e direção de serviços ou centro de documentação e informação constituídos de acervos arquivísticos e mistos; V - planejamento, organização e direção de serviços de microfilmagem aplicada aos arquivos; VI - orientação do planejamento da automação aplicada aos arquivos; VII - orientação quanto à classificação, arranjo e descrição de documentos; VIII - orientação da avaliação e seleção de documentos, para fins de preservação; IX- promoção de medidas necessárias à conservação de documentos; X - elaboração de pareceres e trabalhos de complexidade sobre assuntos arquivísticos; XI- assessoramento aos trabalhos de pesquisa científica ou técnico-administrativa; XII - desenvolvimento de estudos sobre documentos culturalmente importantes (Brasil, 1978).

Acompanhando essa análise, vale acrescentar as competências desenvolvidas pelo *Data Protection Officer* (DPO) pelo *General Data Protection Regulation* (GDPR), uma vez que o desenvolvimento da lei brasileira foi inspirada nos parâmetros da lei europeia e outros ordenamentos jurídicos internacionais. Apesar de existir diferenças entre os dois regimes, é notável que o papel do encarregado pelo tratamento de dados, ainda em discussão no contexto brasileiro, guarda semelhanças marcantes com as atribuições e responsabilidades do *Data Protection Officer*. Torna-se crucial compreender a natureza intrínseca desse papel desempenhado pelo arquivista, uma vez que, suas contribuições já desempenhadas nas práticas arquivísticas, podem enriquecer significativamente as práticas e a eficácia na proteção de dados.

No que diz respeito às atribuições do *Data Protection Officer (DPO)*, conforme o Artigo 39 do regulamento europeu, compete ao responsável pela proteção de dados:

> [...] a) informar e aconselhar o responsável pelo tratamento ou o subcontratante e os funcionários que efetuam o tratamento das suas obrigações nos termos do presente regulamento e de outras disposições da União ou dos Estados-Membros em matéria de proteção de dados; b) para monitorizar o cumprimento do presente regulamento, de outras disposições da União ou dos Estados-Membros em matéria de proteção de dados e das políticas do responsável pelo tratamento ou do subcontratante em relação à proteção de dados pessoais, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal envolvido nas operações de tratamento, e as auditorias conexas; c) prestar aconselhamento, quando solicitado, relativamente à avaliação de impacto da proteção de dados e monitorizar o seu desempenho nos termos do artigo 35.º ; d) cooperar com a autoridade de supervisão; e) atuar como ponto de contacto da autoridade de controlo em questões relacionadas com o tratamento, incluindo a consulta prévia referida no artigo 36.º , e consultar, quando adequado, sobre qualquer outra matéria. 2. O encarregado da proteção de dados, no exercício das suas funções, terá em devida conta os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento (União Europeia, 2016).

Corroborando com as responsabilidades do *Data Protection Officer (DPO)* no contexto europeu em face da inspiração brasileira, cabe observar que as responsabilidades do arquivista nesta posição, não se limitam à simples implementação das diretrizes da LGPD, mas pode se estender à complexa avaliação ética do profissional. Essa dimensão se mostra particularmente essencial ao considerar a transparência administrativa, a responsabilidade democrática e a preservação da memória individual e coletiva, sobretudo no que tange à proteção de dados pessoais.

Percebe-se ainda que analisar a complexidade das responsabilidades inerentes ao arquivista, sob a perspectiva da prestação de contas, da transparência administrativa e gestão de riscos (*accountability)*, permite-se reconhecer que tais dimensões estabelecem conexões fundamentais para que os arquivos possam contribuir de forma estratégica na promoção da proteção à privacidade e proteção de dados pessoais. A partir da visão de Iacovino (2009, p. 267), a qual é reiterado a respeito do debate sobre a "dicotomia entre o documento enquanto memória e o documento enquanto prova" em que considera que "a dimensão memorial do documento é a sua capacidade de prestar testemunho sobre fatos sociais e de fornecer memória pessoal e organizacional de seu criador". Ao mesmo tempo, a autora analisa que a relação da "dimensão probatória de um documento surge da sua capacidade de prestar contas

das ações de indivíduos ou organizações através da manutenção de seu contexto de criação, uso e preservação" (2009, p. 267).

Rodrigues (2019), por sua vez, faz uma considerável avaliação na nota de abertura da edição brasileira do livro *"Sem Consentimento: a **ética** na divulgação de informações pessoais em arquivos públicos"* a respeito da tensão entre o direito da informação e o direito à privacidade. A autora destacou que apesar de terem se passado três décadas o estudo realizado no Canadá, ainda preserva a importante argumentação ao pautar "a existência do dilema ético envolvendo a garantia do **direito de acesso** às informações em poder das instituições públicas e o dever de garantir a privacidade dos indivíduos, privacidade em muitas vezes de difícil definição e de contornos fluidos" (Rodrigues, 2019, p. 9).

Rodrigues (2019) destaca a estreita relação e a colaboração da Organização das Nações Unidas (UNESCO) com o Conselho Internacional de Arquivos (ICA)[4], nos últimos anos, na luta do reconhecimento dos arquivos na defesa dos direitos humanos, como mostra na 36ª sessão plenária:

> [...] o caráter singular dos arquivos como evidência autêntica das atividades administrativas, culturais e intelectuais e como um reflexo da evolução das sociedades; o caráter fundamental dos arquivos no apoio à condução eficiente, **responsável e transparente de negócios**, **proteção dos direitos dos cidadãos**, fundamentação da memória individual e coletiva, compreensão do passado, documentação do presente e orientação das ações futuras; a diversidade dos arquivos ao registrarem todas as áreas da atividade humana; a multiplicidade de suportes e formatos em que os documentos são produzidos, incluindo papel, audiovisual, digital e outros; **o papel dos arquivistas, profissionais qualificados, com formação apropriada e contínua**, que servem às suas sociedades, apoiando a produção, seleção e conservação dos documentos, e os tornam disponíveis para uso; **a responsabilidade de todos, cidadãos, gestores e autoridades públicas,** proprietários ou detentores de arquivos públicos ou privados, arquivistas e outros profissionais do campo da informação, na gestão de arquivos" (Unesco, 2010, grifo nosso).

Nessa mesma assembleia, que reuniu a UNESCO e o ICA e culminou na elaboração na Declaração Universal de Arquivos, as entidades se comprometeram, entre outros aspectos, a trabalhar para que os arquivos sejam geridos e conservados para garantir a sua autenticidade e confiabilidade. Comprometeram-se também a garantir que fossem acessíveis, respeitando a legislação vigente e os direitos dos indivíduos, produtores, proprietários e usuários, a fim de que possam ser utilizados na promoção de uma cidadania responsável.

[4] O Conselho Internacional de Arquivos (ICA) é uma organização internacional não governamental, sem fins lucrativos, regida pela lei francesa relativa às associações de 1º de julho de 1901.

Na abordagem de Rodrigues (2019, p.10), ficou evidente a necessidade de sopesar os direitos relacionados ao acesso às informações e à proteção da privacidade do indivíduo, especialmente diante das mudanças no contexto histórico e o avanço das tecnologias, que afetam consideravelmente as formas de uso das informações pessoais. Isso é corroborado pela definição de "informações pessoais" proposta por Terry Cook (1991):

> Informações pessoais são quaisquer informações sobre um indivíduo identificável registradas em qualquer formato. A Lei de Privacidade do Canadá, para citar um exemplo de orientação geral, fornece uma definição ampliada de informações pessoais para incluir o seguinte: informações relacionadas à raça, origem nacional ou étnica, cor, religião, idade ou estado civil; o histórico ou situação educacional, médica, criminal e profissional do indivíduo; transações financeiras em que o indivíduo está envolvido; qualquer número, símbolo ou código de identificação atribuído ao indivíduo; endereço, impressões digitais ou tipo sanguíneo do indivíduo: opiniões e pontos de vista pessoais do indivíduo (com certas exceções restritas em relação a subsídios e prêmios): correspondência enviada a uma agência governamental pelo indivíduo "que seja implícita ou explicitamente de natureza privada ou confidencial "e respostas a essa correspondência que revelariam o conteúdo da correspondência original; os pontos de vista e opiniões de outra pessoa sobre o indivíduo; e o nome do indivíduo quando aparecer num contexto geral, cuja divulgação revelaria implicitamente informações sobre o indivíduo. De outra perspectiva, mais geral, as informações pessoais incluem consultas, reclamações ou observações recebidas de um indivíduo sobre qualquer programa governamental, informações sobre casos de aplicação da lei ou sobre quaisquer transações do indivíduo com o Estado para programas sociais ou outros programas de benefícios, informações estatísticas ou informatizadas. Sobre o indivíduo e arquivos sobre funcionários públicos atuais ou antigos. As informações pessoais acima podem aparecer em vários tipos de registros. Estes incluem requerimentos, declarações, inquéritos e reclamações, recursos, pedidos, reclamações, relatórios, contratos, listas, registos, listas, prêmios, subsídios, subvenções, faturas, certificados, empréstimos, pagamentos, exames, questionários, audiências, acordos, testamentos, arrendamentos., licenças e autorizações: registros de patentes, passaportes, subsídios e muitos, muitos outros. Esses tipos de documentos são geralmente formulários elaborados, mas sua função também pode ser expressa em cartas e memorandos, todos geralmente agregados em arquivos de casos. É função do gestor de documentos identificar, descrever e proteger registros de informações pessoais de acordo com a lei de privacidade da jurisdição envolvida e com boas práticas de gerenciamento de registros [5](Cook, 1991, tradução nossa).

---

[5] *Personal information is any information about an identifiable individual that is recorded in any format. The Privacy Act of Canada, to cite one example for general guidance, gives an extended definition of personal information to include the following: information relating to race, national or ethnic origin, colour, religion, age, or marital status; the educational, medical, criminal, and employment history or status of the individual; financial transactions in which the individual is involved; any identifying number, symbol, or code assigned to the individual; address, fingerprints, or blood type of the individual: personal opinions and views of the individual (with certain narrow exceptions regarding grants and awards): correspondence sent to a government agency by the individual "that is implicitly or explicitly of a private or confidential nature" and replies to that*

É fundamental desenvolver mecanismos que permitam uma avaliação criteriosa da maturidade na utilização de informações pessoais e dados registrados nos documentos, promovendo uma abordagem responsável por parte do arquivista. Nesse sentido, é essencial que essa abordagem seja desenvolvida levando em conta as dinâmicas próprias do contexto contemporâneo e as legislações vigentes, garantindo a integridade e a ética no manejo de dados pessoais.

1.3 Procedimentos metodológicos

Com o propósito de atingir os objetivos delineados, a pesquisa adotou uma abordagem **qualitativa e exploratória**, alinhada aos princípios apresentados por Gil (1991), cujo qual tem como principal finalidade desenvolver, esclarecer e modificar os conceitos e ideias. Considerando a formulação de problemas mais precisos ou hipóteses a serem testadas em estudos posteriores. A pesquisa pretendia proporcionar visão geral, acerca de determinado fato, tendo em vista que o tema escolhido foi pouco explorado na área, tornando-se de difícil formulação de hipóteses mais precisas e operacionalizáveis.

A escolha metodológica justificou-se pela necessidade de aprofundar o entendimento sobre o papel do arquivista exercendo a função de responsável pelo tratamento de dados ou como membro de um comitê de governança em privacidade. Além disso, propôs a analisar o desenvolvimento de indicadores relevantes para a gestão de riscos em programas de

---

correspondence which would reveal the contents of the original correspondence; the views and opinions of another person about the individual; and the name of the individual where it appears in a general context the disclosure of whigh would implicitly reveal information about the individual. From another, more general perspective, personal information includes inquiries or complaints or observations received from an individual about any government programme, information on law enforcement cases or about any transactions of the individual with the state for social or other benefit programmes, statistical or computerized information about the individual3 and files on current or former government employees. The above personal information can appear in many types of records. These include applications, declarations, inquiries and complaints, appeals, requests, claims, reports, contracts, lists, registers, rolls, awards, subsidies, grants, invoices, certificates, loans, payments, examinations, questionnaires hearings, agreements, wills, leases, licences and permits: patents4 registrations, passports, allowances, and many, many others. These types of records are usually designed forms, but their function can be expressed in letters and memoranda as well, all of which are usually aggregated in case files. It is the role of the records manager to identify, describe, and protect personal information records in accordance with the privacy act of the jurisdiction involved and with good records management practices.

privacidade e proteção de dados, para a contribuição da avaliação da maturidade organizacional, sob a ótica do gerenciamento e a governança arquivísticos.

O referencial teórico foi construído por meio da análise de livros, artigos e periódicos e ainda análise documental das legislações que dizem respeito à proteção e privacidade de dados no Brasil, bem como legislações correlatas no mundo, e que também contribuíram para o desenvolvimento das leis no país.

Posteriormente, foi realizada a coleta de dados através da aplicação de um questionário, que orientada pelos objetivos da pesquisa, teve o propósito de obter informações a respeito do conhecimento e as práticas dos profissionais que atuaram ou estiveram em atividade. A escolha por esse modelo de coleta se deu pela possibilidade de um maior alcance de pessoas dispersas em uma área geográfica extensa, o que também implicaria em menor tempo e nenhum custo financeiro, quanto ao deslocamento (Gil, 2008). Além disso, o anonimato dos participantes seria garantido pelos recursos do *Google Forms*[6].

Com vistas a alcançar uma taxa razoável de retorno, considerando também o tempo de vigência da LGPD e o prazo previamente determinado para aplicação e análise dos dados, considerou para a construção do questionário: a extensão, o formato e a ordem das questões. Essa última objetivava uma crescente, a qual considerou a proteção e integridade, como considerava suas responsabilidades, como entendia e se comportava a respeito da gestão de riscos e por fim como entendia a prestação de contas e a transparência.

Para a elaboração das perguntas utilizou-se como referência a escala Likert e seu desenvolvimento se deu a partir dos seguintes eixos centrais identificados durante a revisão de literatura:

a) A proteção e integridade do conteúdo dos documentos arquivísticos.
b) A responsabilidade arquivística nos aspectos da produção até a destinação final dos documentos.
c) A gestão de riscos para controle e monitoramento dos incidentes à utilização dos dados.
d) A prestação de contas no desenvolvimento de políticas de acesso/privacidade.

Após revisão e testes preliminares para identificar possíveis falhas e garantir a clareza e precisão dos termos, algumas questões foram desmembradas. A atenção também se

[6] O *Google Forms* é uma ferramenta oferecida pelo Google que permite a criação de formulários e questionários para pesquisa.

desdobrou ao filtro inicial para que somente arquivistas fossem direcionados à próxima etapa. O questionário foi enviado por meios eletrônicos e disponibilizado nas mídias sociais. Adicionalmente, foi solicitado o apoio das associações de classe e dos colegiados de graduação de Arquivologia para o ampliar o alcance da divulgação.

Na sequência a aplicação do questionário, procedemos com a análise qualitativas dos dados. A tabulação e organização sistemática das informações em tabelas e gráficos permitiram a realização de uma análise de conteúdo mais aprofundada, possibilitando a identificação de padrões e a interpretações das respostas dos participantes. Com vistas a aproximação da revisão teórica a respeito da privacidade e proteção dos dados, a implementação da LGPD e a realidade profissional dos arquivistas.

2 EVOLUÇÃO DAS LEIS DE PRIVACIDADE

A expansão das tecnologias de comunicação pelo mundo desencadeou inúmeros avanços e benefícios, ampliou e facilitou a comunicação, o acesso à informação e a realização de diversas outras atividades a partir do seu desenvolvimento. Contribuiu também com o estreitamento dos laços entre as pessoas, aproximando-as sem que precisassem sair de suas casas. No entanto, apesar da facilidade da conectividade, aumentaram, também, as preocupações e as fragilidades a respeito da privacidade e da proteção das informações dos indivíduos.

De acordo com Bagatini (2021, p. 2) o uso da internet móvel se tornou essencial no dia a dia, o serviço fornecido por empresas de telefonia, expandido ao uso de dispositivos inteligentes, como *smartphones,* relógios e pulseiras inteligentes. O autor ressaltou que:

> O uso de soluções informatizadas em rede, que se expandiu de forma acelerada e acrítica, possibilitou ao cidadão contemporâneo realizar quase todas as suas tarefas cotidianas de forma conectada – ler notícias, agendar atendimento em repartições públicas, conectar-se com amigos, assistir a filmes e fazer compras on-line (Bagatini 2021, p. 2).

Bagatini (2021, p. 2) observou que com a disseminação dos *smartphones* e também dispositivos *wearables*, intensificou-se a produção de dados, afetando aspectos mais privados da vida dos indivíduos. Exemplo como uma “simples locomoção comum *smartphone* no bolso, ou vestindo um relógio inteligente, pode gerar dados como a quantidade de passos, o caminho percorrido, a frequência cardíaca, a altura, o peso e os locais frequentados” (Bagatini, 2021, p. 3). Além disso, a expansão da tecnologia, também resultou numa maior capacidade de armazenamento de informações em bancos de dados e do processamento em sistemas dessas informações pessoais acerca dos cidadãos por parte dos governos, um desafio a ser enfrentado na atualidade.

No contexto da economia de dados, Rockembach (2020) propõe uma reflexão análoga aos "filtros-bolhas" para analisar a coleta e o tratamento de dados sob a perspectiva do estudo de usuários e do custo da personalização. O autor explora esse cenário em três dimensões: a primeira, em que o indivíduo se isola em uma bolha, afastando-se de outras pessoas; a segunda, caracterizada pela não transparência dos critérios das plataformas (bolha invisível); e a terceira, onde ocorre um direcionamento consciente quando o usuário opta por não aderir à

bolha, definindo suas escolhas nas plataformas digitais. Essas interações com o sistema impactam a personalização dos dados, gerando potenciais efeitos positivos e negativos.

Nesse contexto, MacNeil (1992, p. 19) refletiu a respeito das preocupações contemporâneas sobre a perda da privacidade, considerando principalmente a respeito da "quantidade de informação conhecida acerca de um indivíduo, e [que] surgiram em resposta a situações criadas pelas práticas de captação de informações, ignoradas nas interpretações tradicionais de invasão de privacidade". A autora considerou ainda os potenciais impactos na sociedade sobre o viés das liberdades civis, ponderando que:

> Os defensores da liberdade civis sustentam que, ainda que nada de inerentemente privado ou indevidamente depreciativo seja armazenado em um banco de dados, existe a possibilidade de que as vastas quantidades de informações aparentemente inócuas sobre os cidadãos, em conjunção com a capacidade tecnológicas de cruzar informações de uma variedade de fontes, resultarão em uma sociedade menos espontânea e, em uma última instância, menos livre (MacNeil, 2019).

Nesse cenário, onde empresas e organizações passaram a coletar uma quantidade significativa de dados e informações pessoais, e que por vezes, pecam pela utilização de forma excessiva. Em muitos casos os usuários não se dão conta sobre qual é a real intenção por trás da utilização dessas informações. Às vezes, justificam a coleta mediante a oferta de serviços oferecidos em troca de descontos ou de brindes, ou ainda, a utilização se dá com a justificativa de personalização da experiência do cliente. Contudo, para que a utilização aconteça de forma legítima seria necessário a obtenção de fundamento legal válido, o qual, atendesse aos propósitos específicos, explícitos, que legitimasse o tratamento das informações pessoais.

Ademais, os modelos de negócios centrados na coleta de dados pessoais que visam ao desenvolvimento de produtos e serviços através da vigilância, denominada como "economia dos dados". São baseados na perspectiva do consumo, modelos estes que podem comprometer a privacidade do indivíduo, resultando em violação de direitos. Esses aspectos foram bem destacados por Bagatini, Chaves e Sant'ana (2021, p. 4) que, por sua vez, explicou que esses "dados passam por um processo de *commoditização,* tornando-se em insumo para diversas atividades econômicas". Os autores (2021, p. 4) destacou que:

> Ao referirem-se àquilo que denominam economia da privacidade, a qual é composta por empresas que possuem seus modelos de negócios voltados à vigilância e orientam seus negócios e produtos para a coleta e processamento

> de dados pessoais, estabelecendo uma faceta do capitalismo que se fundamenta no enfraquecimento do direito à privacidade (Bagatini; Chaves; Sant'ana , 2021).

A representação neste estudo (Figura 1) foi elaborada com base no estudo realizado por Bagatini, Chaves e Sant'ana (2021), os quais consideraram a dinâmica do gerenciamento de dados pessoais em arquivos sob uma abordagem centrada no indivíduo. Foram destacados o uso de dados por organizações e os direitos individuais, sob a perspectiva da ética e privacidade, a fim de descrever as dinâmicas do gerenciamento de dados centrado no indivíduo e compreender a problemática da **garantia da privacidade e da autodeterminação informativa.**

Os autores avaliaram a preocupação da sociedade em relação à privacidade, bem como a necessidade de proteção, a autonomia, o autodesenvolvimento e autoavaliação como sendo fundamental para o indivíduo. Na contramão da economia da privacidade, pois a "privacidade e lucro são inversamente proporcionais: quanto maior for o nível de privacidade, menor é o lucro obtido a partir dos dados capturados", representado na figura nos itens 1 e 2, em referência a "economia de privacidade" e "*data shadow*".

Figura 1 - Entendendo as dinâmicas do gerenciamento de dados centrada no indivíduo

Fonte: Elaboração própria, baseado no estudo de Bagatini, Chaves e Sant'ana (2021)

Neste contexto do crescente volume de dados pessoais, torna-se um desafio para os profissionais da informação, em especial aos arquivistas que têm seu trabalho orientado pelo gerenciamento dos documentos e informações, "tornando necessário que esses profissionais desenvolvam um novo conjunto de habilidades para poder classificar, organizar e disseminar informações que hoje nem sempre se manifestam nos formatos tradicionais" (Bagatini; Chaves; Sant'ana, 2021, p. 7).

Em relação aos papéis e responsabilidades dos envolvidos em um processo de tratamento dos dados, estes podem assumir posições diferentes de (o titular, o controlador e o operador) dependendo das dinâmicas e do processos em que se assume. No contexto dos arquivos, os autores consideraram que:

> [...] o desenvolvimento de suas atividades pode fazer com que assumam tanto o papel de controlador, quando lidam com a coleta, armazenamento, recuperação e descarte de dados pessoais que são essenciais para a execução de suas atividades, tais como aqueles que compõem base de dados de usuários, controle de acesso, empréstimo, colaboradores, etc.; quanto o papel de operador, quando o arquivo passa a ser responsável pela salvaguarda de dados pessoais capturados a partir do interesse de outra instituição. Ou seja, os dados pessoais em arquivos podem assumir duas características distintas e serem reconhecidos como documentos ou dados de operacionalização das atividades que constituem o cerne do fazer de uma unidade arquivística (Bagatini, Chaves e Sant'ana, 2021, p. 7-8).

No mesmo estudo, os autores apontaram uma relação do partir do modelo de ciclo de vida dos dados (CDV), composto por quatro fases, sendo: (1) coleta, (2) armazenamento, (3) recuperação e (4) descarte. Corroborando com a visão de Romansky (2015) que considerou sete as fases com observando os dados pessoais, sendo: (1) coleta, (2) preservação, (3) utilização, (4) atualização, (5) transferência/doação, (6) arquivamento e (7) destruição. Nesse sentido, os desafios para a privacidade estão transpostos por fatores que dizem respeito a **"integração, qualidade, direitos autorais, disseminação, preservação e privacidade"**, os quais, impactam ativamente nas diferentes fases do ciclo de vida dos dados (Bagatini; Chaves; Sant'ana, 2021, p. 9), a saber:

> Na coleta, faz-se necessário identificar, nas fontes utilizadas, aspectos que possam configurar violação da privacidade do titular; no armazenamento, deve-se ter preocupação com questões como quem poderá acessar os dados anteriormente coletados e onde os dados serão armazenados, já que uma base desconectada da rede pode estar mais segura com relação a acessos ou usos indevidos do que uma que esteja armazenada em um servidor de dados conectado à internet; na etapa de recuperação, deve-se

> considerar os envolvidos com os dados, identificando estruturas e possíveis usuários, lembrando-se de prever a vinculação desses dados com outros, especialmente se forem dados sensíveis, havendo assim a necessidade de considerar a aplicação de técnicas de anonimização, mesmo que deteriorem o nível de utilidade da base de dados; por fim, no descarte, é preciso atentar para o fato de que um indivíduo pode ter o direito, ou pode vir a ter a necessidade, de excluir seus dados de uma determinada base e garantir o que poderíamos identificar com o conceito do direito ao esquecimento (Bagatini; Chaves; Sant'ana, 2021, p. 9).

Em sequência do estudo realizado por Bagatini, Chaves e Sant'ana (2021), sugere a construção de uma abordagem mais centrada no indivíduo, ou seja, a pessoa detentora de seus dados, ficaria ao centro, podendo ter o acesso e controle aos dados pessoais coletados. Nessa proposta, haveria o fortalecimento da proteção aos direitos humanos, inclusive na esfera digital, e ainda, a possibilidade de fortalecimentos de confiança para os negócios desenvolvidos a partir desse modelo. Vale destacar, que o modelo de nome *MyData* (item 7 da figura), propõem uma mudança da perspectiva onde o gerenciamento e o processamento dos dados pessoais focada no ser humano, em concordância com três princípios de determinam:

> 1) controle centrado no ser humano e privacidade – indivíduos são atores capacitados, não alvos passivos, na gestão de suas vidas pessoais, tanto on-line quanto off-line; eles têm direito e meios práticos para gerir seus dados e sua privacidade; 2) dados utilizáveis – é essencial que os dados pessoais sejam tecnicamente fáceis de serem acessados e utilizados, acessíveis em formatos legíveis por máquina por meio de APIs (application programming interfaces) seguras e padronizadas; [...] 3) ambiente de negócios aberto – a infraestrutura compartilhada do MyData permite gestão descentralizada dos dados pessoais, melhora a interoperabilidade, torna mais fácil o cumprimento dos rigorosos regulamentos de proteção de dados pelas empresas e permite que os indivíduos mudem prestadores de serviços sem *lockins* pelos proprietários dos dados (Bagatini; Chaves; Sant'ana 2021, p. 12).

Como uma possível solução para o desenvolvimento de políticas e soluções em arquivos, para o controle da coleta de informações e dados de forma indiscriminada, Bagatini, Chaves e Sant'ana (2021), propôs uma abordagem com vistas a auxiliar de forma transversal na construção de ambientes que respeitem o direito à privacidade e a proteção de dados desde a concepção e durante todo o ciclo de vida de um determinado projeto, sistema, serviços, produto ou processo.

2.1 Conceituação da privacidade como direito fundamental

Ao propor uma conceituação de privacidade, é relevante antes expor a dificuldade de estabelecer um consenso sobre o termo, tanto na doutrina brasileira quanto na estrangeira (Doneda, 2021, p. 101). O conceito de privacidade passou por diversas definições ao longo do tempo, sendo considerado por alguns autores como sinônimo de vida privada e intimidade. Adicionalmente, cabe uma reflexão exploratória, ainda que não exaustiva, acerca de sua relação com a inviolabilidade da intimidade, da vida privada, da honra e da imagem, bem como com o desenvolvimento da autodeterminação informativa.

Na antiguidade, o termo evidenciava os aspectos da vida privada, com características aproximadas à "privação" e ao "isolamento". A partir do século XV, com as evoluções, passou-se a associar o termo "privado" a alguma vantagem, como uma forma de obtenção de privilégios. A caráter de exemplo, MacNeil (1992. p.17) citou a educação privada, os clubes privados e as propriedades privadas.

No caminhar dos séculos, mais precisamente entre os séculos XVI e XVIII, o termo evoluiu para uma compreensão dos aspectos de "independência" e de "intimidade", no que concerne à apreciação de uma vida tranquila[7] (MacNeil, 1992, p.18).

Conforme as reflexões de Silva (2018), percebe-se a inexistência de um consenso no que diz respeito aos termos **"intimidade", "vida privada" e "privacidade**", tanto em suas definições quanto em seus conteúdos. O autor destaca que diversos autores consideram os termos "direito à privacidade", "direito à vida privada" e "direito à intimidade" como sinônimos, sendo por diversas vezes utilizados de maneira ambígua e até equivocada.

No que concerne o direito à intimidade, pode ser relacionado, com os chamados "direitos da personalidade", pois são inerentes ao próprio homem e têm por finalidade resguardar a dignidade da pessoa humana (Hirata, 2017). Os direitos de personalidades são assegurados pela Constituição Federal de 1988, o Código Penal e também pelo Código Civil. No entanto, no Código Civil, eles foram regulamentados de forma mais específica, utilizando-se de um capítulo, que estabelece o seguinte:

> Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o

[7] *Raymond Williams, Keyywords: A Vocabulary of Culture and Society, Glasgow*, Fontana, 1976, p. 203-204.

> quarto grau. Art. 13. Salvo por exigência médica, é defeso o ato de disposição do próprio corpo, quando importar diminuição permanente da integridade física, ou contrariar os bons costumes. Parágrafo único. O ato previsto neste artigo será admitido para fins de transplante, na forma estabelecida em lei especial. Art. 14. É válida, com objetivo científico, ou altruístico, a disposição gratuita do próprio corpo, no todo ou em parte, para depois da morte. Parágrafo único. O ato de disposição pode ser livremente revogado a qualquer tempo. Art. 15. Ninguém pode ser constrangido a submeter-se, com risco de vida, a tratamento médico ou a intervenção cirúrgica. Art. 16. Toda pessoa tem direito ao nome, nele compreendido o prenome e o sobrenome. Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória. Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial. Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome. Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes. Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma (Brasil, 2002).

Cabe lembrar, que alguns autores[8], consideram de formas distintas o direito à intimidade em relação ao direito à vida privada:

> Entende que a esfera íntima da pessoa se divide em direito à *riservatezza* e o direito à *segretezza*. O direito à intimidade pode ser conceituado como aquele que visa a resguardar as pessoas dos sentidos alheios, principalmente da vista e dos ouvidos de outrem. Ou seja, é o direito da pessoa de excluir do conhecimento de terceiros tudo aquilo que a ela se relaciona. O direito à intimidade é, ainda, o poder correspondente ao dever de todas as outras pessoas de não se imiscuir na intimidade alheia, opondo-se a eventuais descumprimentos desse dever, realizados por meio de investigação e/ou divulgação de informações sobre a vida alheia (Hirata, 2017).

Hirata (2017) destaca que o surgimento desses direitos caracteriza uma reação da teoria estatal, na qual encontra respaldo em documentos considerados universais, cujo propósito é fundamentar os princípios de liberdade, justiça e igualdade no mundo. Como base

[8] DE CUPIS, Adriano. *Il diritto alla riservatezza*. Dott. A Giuffrè – Editore, Milano, 1959.

para os direitos de personalidade, o autor relaciona os seguintes documentos, considerados de amplitude universal:

> [...] a Declaração dos Direitos do Homem e do Cidadão, de 1789, a Declaração Universal dos Direitos do Homem, de 1948 (art. 12), a 9ª Conferência Internacional Americana de 1948 (art. 5º), a Convenção Europeia dos Direitos do Homem de 1950 (art. 8º), a Convenção Panamericana dos Direitos do Homem de 1959, a Conferência Nórdica sobre o Direito à Intimidade, de 1967, além de outros documentos internacionais (Hirata, 2017).

Em 1890, no final do século XIX, Warren e Brandeis, no artigo de renome no campo do direito "The right to privacy", avançaram à análise a respeito do direito à privacidade e suas implicações a partir das transformações políticas, sociais e econômicas. Os autores ainda defenderam a necessidade do reconhecimento de novos direitos para a proteção dos indivíduos acerca de exposições sem o devido consentimento. Vale ressaltar que o sistema judiciário dos países de língua inglesa, baseia-se em decisões anteriores e a jurisprudência, observando os costumes de vivência da sociedade, características atreladas a "*common law*".

Warren e Brandeis (1980, p. 392), observaram que, historicamente, a lei dava remédios para a proteção física e garantias para a não interferência na propriedade (terras e bens), mas que, com o passar do tempo, o escopo dos direitos legais se ampliou de forma gradual. O "direito à vida", por exemplo, expandiu para o direito de gozar a vida, em um nível de liberdade mais intangível, e que também englobava o "direito ser deixado em paz". Enquanto o direito à liberdade passou a assegurar o exercício de amplos privilégios civis e o conceito de "propriedade" passou a abranger outras formas de domínio".

Numa outra perspectiva, o conceito de privacidade estabelece uma relação com o direito de não ser incomodado ou **"direito a estar só"**, conceito esse, que está diretamente ligado à necessidade de proteção do indivíduo a seus assuntos particulares aos quais não desejavam que fossem expostos, sem sua devida permissão. Nesse contexto, Warren e Brandeis (1980, p. 393) avaliavam que a "proteção conferida aos pensamentos, aos sentimentos e às emoções, expressos por meio da escrita ou das artes, na medida em que consiste em impedir a publicação, é apenas uma instância de aplicação do direito mais geral do indivíduo ser deixado em paz".

No Brasil, para a Constituição Federal, o direito à privacidade se configura um direito fundamental, o qual se enquadra nas garantias e direitos fundamentais, de acordo o artigo 5º, o que considera que "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". Embora não defina explicitamente e uma citação direta do termo "privacidade", a Carta Magna determina sobre a inviolabilidade a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação. Além disso, assegura a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, e ainda prevê a garantia do direito de propriedade (Brasil, 1988).

Ademais, a CF/1988 ainda prevê outros direitos, os quais se relacionam com a tutela da privacidade, que devido a sua fluidez e flexibilidade a partir das complexidades do comportamento do humano, configura também nos aspectos dos direitos de personalidade. Ainda no artigo 5º, os incisos XIV e LXXII, respectivamente, conferem a todos os indivíduos o **acesso à informação, e resguarda o sigilo da fonte**, quando necessário ao exercício profissional, e a ***habeas-data***, configura uma ação requerida por um indivíduo que deseja ter acesso a informações relativas a sua pessoa, ou informações que podem estar contidas em registros ou bancos de dados de entidades governamentais ou de caráter público. Além disso, o *habeas-data*, também garante a retificação ou o acréscimo de dados aos registros, "quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" (Brasil, 1997).

A respeito do sigilo e da inviolabilidade, em relação à vida privada e à intimidade, Cancelier (2017, p. 220) aborda o fato de como é possível utilizar qualquer um dos termos para referir a mesma situação. "Ao mesmo tempo, cada um deles poderá assumir – de forma bastante subjetiva – a depender do sujeito da fala, um significado específico", ou seja, os termos podem se adaptar conforme as articulações que forem dadas no discurso de quem a profere. A autora destaca que a privacidade deve ser compreendida antes de tudo como o exercício de uma liberdade da pessoa para configurar uma necessidade humana, uma visão interna do sujeito.

Silva (2020, p. 267), conceituou de forma didática, os direitos fundamentais, a fim de mostrar como os conflitos entre o direito de acesso à informação e a proteção de dados podem ser determinantes em como os documentos arquivísticos devem ser gerados e administrados, sendo possuidores de informações que podem violar os direitos de personalidade. Além disso, o autor reforçou a respeito do compromisso constitucional do arquivista na promoção do acesso, ao mesmo tempo, considerando os direitos de personalidades. O autor destacou que:

> No caso do **direito à intimidade**, ele está relacionado aos traços, às qualidades, às propriedades de intimidade de uma pessoa que não podem ser afetados; não podem ser invadidos sem a devida autorização. No caso do **direito à vida privada**, também está relacionado à propriedade de cada uma dessas pessoas, ou seja, o cidadão não pode ter o seu espaço invadido sem devida autorização. No que tange ao **direito à imagem**, está relacionado com a captação, projeção ou divulgação da imagem de alguém sem o seu consentimento. Em se tratando de imagem, nós temos três tipos: imagem retrato, que permite reconhecer as características físicas; a imagem atributo, que está ligada à nossa reputação, e a imagem científica, que corresponde ao material genético de cada indivíduo. Outro direito é o **direito à honra**, que está relacionado a três tipos de violações: calúnia, difamação e injúria, que, nesse caso, compreende atos como imputar, divulgar, fazer uma afirmação genérica, eticamente degradante, fazer uma agressão, faltar com a verdade ou até um insulto que deprecie a personalidade da pessoa e seus valores (Silva, 2020, p. 267).

A depender das dinâmicas entre os termos **sigilo e inviolabilidade**, em relação **à vida privada e à intimidade**, Cancelier (2017) avalia que:

> [...] é possível fazer uso de qualquer um dos termos para referenciar a mesma situação. Por exemplo, fala-se em vida privada ou vida íntima para tratar do mesmo espaço da vida sobre a qual se fala. Algo secreto, sigiloso ou íntimo pode ser relacionado ao mesmo aspecto que se deseja manter em segredo. O privado pode ser íntimo, o íntimo pode ser secreto, o secreto pode ser privado. [...] Assim, nem sempre o íntimo será secreto ou o assunto sigiloso será privado. O que se quer dizer é que o significado do discurso irá variar conforme quem o profere, possibilitando cada um dos termos aqui apresentados usos variados (Cancelier, 2017, p. 2020).

Para além da oposição ao público, Cancelier (2017) considera que a privacidade seja no aspecto do "estar só" ou numa perspectiva mais contemporânea de controle informacional, da proteção de dados, é necessário manter o vínculo com a pessoa, como uma forma de manifestação da personalidade (Cancelier, 2017, p. 2020).

Por outro lado, Habermas (2014, p. 173) discorre sobre que o 'oposto da privacidade não é a publicidade, mas sim a indiscrição', o que possibilita compreender a privacidade no contexto contemporâneo, onde é possível exercitar a privacidade em público. Conforme Leonardi (2011, p. 367), "[...] proteger a privacidade em público não significa uma tutela absoluta, mas apenas representa a limitação de certas maneiras de usar e revelar algumas informações, pois nem sempre o que foi feito em público [...] é, de fato, público".

2.2 O surgimento do direito à Autodeterminação Informativa

A autodeterminação informativa é um dos fundamentos que disciplina a lei de proteção de dados no Brasil, conforme estabelece o art. 2º, inciso II. Entretanto, a norma brasileira não apresenta a definição do conceito, que teve seu surgimento na Alemanha, a partir da evolução da jurisprudência alemã, e que também influenciou outros ordenamentos estrangeiros, assim como a LGPD.

No que concerne a origem e a evolução, Mendes (2022, p. 13) observou que compreender a origem e sua evolução da autodeterminação informativa é fundamental para entender como terceiros lidam com dados e informações, uma vez que, o conceito está ligado à proteção do direito da personalidade. Além disso, a autora destaca que embora o direito tenha sido reconhecido constitucionalmente em 1983, seu desenvolvimento ocorreu ao longo dos anos por diferentes julgamentos do Tribunal Constitucional da Alemanha, a respeito da proteção de dados.

A jornada pela consolidação da autodeterminação informativa, iniciou a partir do art. 2º, inciso I da Lei fundamental da Alemanha, que "garante que todos têm direito ao livre desenvolvimento de sua personalidade", e evoluindo de acordo com cada ação ou recurso interposto no Tribunal Constitucional (Mendes, 2022, p. 13). Ora pela busca do reconhecimento pela "liberdade geral de ação", utilizando-se como base para o direito de personalidade (1953 - 1957), ora pelo direito ao "respeito à vida privada" (1969 - 1970).

A jurisprudência sobre coleta de informações de caráter pessoal para fins de censo populacional, abordou a questão da privacidade e do uso adequado dos dados. No caso específico da coleta de dados sobre viagens de férias e lazer. A Corte alemã reconheceu que:

> [...] a norma do art. 2°, S1°, da LF abriga não apenas o direito de liberdade geral de ação (caso Elfes), mas também o direito ao respeito à esfera privada. Isso se dá com as decisões do microcenso (BVerfGE 27, 1 (6)) e dos autos de divórcio (BVerfGE 27, 344 (352)), dos anos de 1969 e 1970, respectivamente, que serão apresentadas a seguir. Para que essa evolução jurisprudencial pudesse ocorrer, foi preciso, em primeiro lugar, a percepção de que a liberdade geral de ação não representava um conceito de proteção suficiente contra ameaças da vida moderna à personalidade. Como a liberdade de ação protege exclusivamente o livre comportamento do indivíduo, esse direito é inadequado para proteção do indivíduo contra a ação de terceiros [...] E isso ficou claro tanto no caso do microcenso como no caso dos autos do divórcio, uma vez que em ambos tratou-se de averiguar qual proteção contra ação de terceiros o direito fundamental (Mendes, 2022).

A concepção do tribunal alemão, desenvolvida a partir da jurisprudência, considerou que os direitos fundamentais são vistos como direito de defesa do indivíduo. O entendimento

do tribunal foi que para se investigar a violação à esfera privada é preciso avaliar como ocorreu a coleta e o processamento dessa informação (Mendes, 2022, p. 25). Apesar dos avanços, o direito à esfera privada sofreu críticas nos aspectos da relatividade, conforme apontado:

> À concepção da esfera privada ainda é feita outra crítica, estritamente relacionada ao princípio da relatividade da esfera privada, qual seja, a noção do contexto de aplicação. Ela se refere à ideia de que "a sensibilidade e o conteúdo de significado de informações dependem do respectivo contexto de aplicação"[...]. Assim, a finalidade da coleta [...] e o destinatário da informação são mais decisivos para a avaliação da constitucionalidade do processamento de dados do que a classificação dos dados em privados ou íntimos (Mendes, 2022, p. 26).

A partir do ano de 1973[9], superado os limites a respeito do direito à esfera privada, a Alemanha reconheceu pela primeira vez o direito da personalidade como Direito Constitucional (1980)[10] e aplicação, na prática, da ideia do que venha a se tornar autodeterminação:

> [o] indivíduo deve basicamente [...] poder decidir por si mesmo como ele deseja se apresentar frente a terceiros ou ao público, se e em que medida terceiros podem dispor de sua personalidade; disto também faz especialmente parte da decisão de como ele quer se colocar em evidência com suas próprias palavras (Mendes, 2022, p. 31).

A autora destacou que a evolução referente ao direito de personalidade, ofereceu uma proteção ampliada na sociedade moderna, firmada em um tripé: da proteção abrangente, do conceito de autodeterminação e da abstração, este último diz respeito às novas formas de compreensão de proteção do direito de personalidade.

Nota-se que para o desenvolvimento do conceito da ideia de autodeterminação contribuíram para a sua construção, "as abordagens da relatividade da esfera privada e o contexto de uso de informações como fonte de risco" (Mendes, 2022, p. 32). Conceito esse que por sua vez foi aprofundado e consolidado como um direito fundamental orientado para a

---

[9] Caso "Soraya" trata a respeito da publicação referente a uma entrevista fictícia, o qual violou os direitos de personalidades, cabendo à editora responsável por reparação financeira, uma vez que não foi possível restabelecer a condição anterior ao dano (Mendes, 2022, p. 27).

[10] Caso "Eppler" trata de um recurso submetido ao Tribunal Alemão por considerar ter sido lesado em um discurso eleitoral, em que foram atribuídas palavras que não foram pronunciadas pelo tal (Mendes, 2022, p. 29).

informação, em seguida compreendido sobre critério de processamentos da informação de forma transparente.

A partir da sentença de recenseamento da população, é retomado o conceito de autodeterminação informativa e já não importava se as informações coletadas eram de cunho íntimo, privado ou público. Os riscos relativos à privacidade poderiam surgir a partir do processamento eletrônico dos dados. O tribunal avaliou que:

> [...] o processamento automatizado dos dados ameaçaria o poder do indivíduo de decidir por si mesmo se e como ele desejaria fornecer a terceiros os seus dados pessoais, considerando que o processamento de dados possibilitaria a elaboração de "perfil completo da personalidade" por meio de "sistemas automatizados integrados sem que o interessado pudesse controlar de forma suficiente sua correção e utilização (Mendes, 2022, p. 36).

Assim, o direito à autodeterminação informativa se constituiu a partir da superação da proteção à esfera privada e íntima, cujo qual, se caracterizou tendo como ponto focal o poder de decisão do indivíduo, e ampliou a proteção para todo o tratamento sobre as informações pessoais. Desse modo, na definição do conceito de autodeterminação informativa, ou seja, ao invés de limitar a esfera privada e íntima, "não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados" (Mendes, 2020, p. 11).

No Brasil, o Ministro do Supremo Tribunal Federal, Luiz Fux[11], considera que o direito da autodeterminação informativa, origina-se do princípio constitucional da dignidade da pessoa humana, cuja qual, se desenvolveu a partir da Segunda Guerra Mundial. O Ministro destaca que para "[...] o desenvolvimento tecnológico sustentável, assim como há a liberdade de proliferação dos dados, há a garantia dessa denominada autodeterminação informativa: saber para que fim os dados serão utilizados" (CNJ, 2021).

A autodeterminação informativa está positivada pela Constituição Federal de 1988 e também com previsão de proteção de dados no regulamenta jurídico Carta dos Direitos Fundamentais da União Europeia[12].

---

[11] Discurso realizado em palestra no Congresso Nacional de Registro Civil (Conarci 2021), o presidente do Conselho Nacional de Justiça (CNJ), Ministro do Supremo Tribunal Federal Luiz Fux, discorreu a respeito do direito à autodeterminação informativa. Disponível em: https://www.cnj.jus.br/dignidade-humana-esta-na-origem-da-autodeterminacao-informativa-da-lgpd-afirma-fux/

[12] (2000/C364/01) O artigo 8º da Carta de Direitos Fundamentais da União Europeia garante: "Protecção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter

2.3 As Leis de Privacidade pelo Mundo e impactos no cenário brasileiro

Ao longo dos últimos 50 anos[13], MacNeil (2019, p. 19-27) observou-se uma crescente preocupação dos cidadãos em relação aos potenciais abusos decorrentes do uso de informações pessoais armazenadas em banco de dados e em arquivos. Embora inofensivas em formatos não estruturados, essas informações, quando combinadas pela capacidade tecnológica e no poder cruzamento de diversas fontes, podem levar a uma sociedade menos livre. A autora enfatizou as atuais preocupações acerca da perda de privacidade e, de forma mais contundente, sobre o poder de vigilância, mesmo que alegadamente benigno, exercido pelo governo ou por grandes organizações na coleta de informações dos indivíduos, como exemplo, as escutas telefônicas e o compartilhamento de bases de dados.

A respeito da vigilância informacional, a autora destacou que:

> [...] a perda da privacidade, estão relacionadas, à quantidade de informação conhecida acerca de um indivíduo, e surgiram em resposta a situações criadas pelas práticas de captação de informações, ignoradas nas interpretações tradicionais de invasão de privacidade (MacNeil, 2019, p. 19).

Neste contexto, qual é o limite entre a liberdade individual e a necessidade de dispor de um certo grau da privacidade para que o indivíduo possa usufruir como ser social e contribuir em favor do avanço aos interesses coletivos?

É diante deste cenário, que os Estados se empenharam a discussões[14] sobre o sistema de processamento automatizado de informações e ao desenvolvimento de leis de proteção de dados pelo mundo[15], e buscam "definir as categorias de vida privada em conformidade com as práticas de gestão documental, e a defender esses dados contra invasões arbitrárias" (MacNeil, 2019, p. 19). As práticas de gestão de documentos do governo também são consideradas como potenciais ameaças à privacidade dos cidadãos, e nesse sentido o

---

a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente" (UE, 2000).

[13] Considerou aqui os últimos 50 anos, devidos às referências dos autores que estudaram o tema sobre o desenvolvimento de leis de proteção de dados, e que abrangia o final da década de 1960, como: Arthur Miller 1971; MacNeil 1992.

[14] Bruno Bioni, destacou as discussões em 1973, do grupo de trabalho de aconselhamento sobre os sistemas de processamentos automatizados do *Health, Education, and Welfare* (HEW) definido como germe das normas de proteção de dados pessoais (Bioni, 2022, p. 1).

[15] MacNeil, destacou que nos últimos anos "testemunharam o surgimento, na maioria dos países ocidentais, de legislação de proteção de dados, que incide sobre a coleta, uso e divulgação de informações pessoais, principalmente por agências governamentais" (MacNeil, 2019, p. 44)**.**

desenvolvimento de regulamentos são direcionados às agências governamentais (MacNeil, 2019, p. 19).

Em observação aos avanços das legislações de privacidade e de proteção de dados no cenário mundial, nota-se que, à medida que as relações e atividades comerciais e sociais se estreitam, surge a necessidade de estabelecer critérios para que essas relações aconteçam de forma mais justa e igualitária.

Nesse sentido, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), criada em 1960, tem como missão a promoção do bem-estar econômico e social global, sendo um "fórum e centro de conhecimento único para dados, análises e melhores práticas em políticas públicas". Na prática, os governos dos países integrantes buscam a cooperação para encontrar soluções para problemas comuns, como o livre comércio e o fluxo transfronteiriço de dados.

Nessa mesma direção, e à luz dos desenvolvimentos globais, a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), órgão do sistema das Nações Unidas, fundada na década de 1960, atua para o tratamento integrado de áreas do comércio e seu desenvolvimento, a tecnologia e também para um desenvolvimento mais sustentável. O fórum intergovernamental procura, em seus encontros, estabelecer diálogos sobre temáticas de cooperação técnicas que visam auxiliar países com estratégias para o crescimento, propondo uma integração dos países de forma positiva na economia mundial. A UNCTAD destacou que "sem leis específicas que regulam o mercado da privacidade, a relação de poder entre o proprietário do dado e os interessados em obter dados continuará sendo desleal e benéfica à segunda parte" (Unctad, 2021).

Adicionalmente, a UNCTAD tem entre os seus objetivos realizar o mapeamento global[16], o qual realiza o rastreamento das leis cibernéticas e o estado em que se encontram a legislação referente às leis de privacidade e proteção de dados, a proteção ao consumidor, o comércio eletrônico e transações eletrônicas. Nesse propósito, verifica-se a adoção de crimes cibernéticos dos 194 estados-membros, entre outras demandas necessárias da esfera digital.

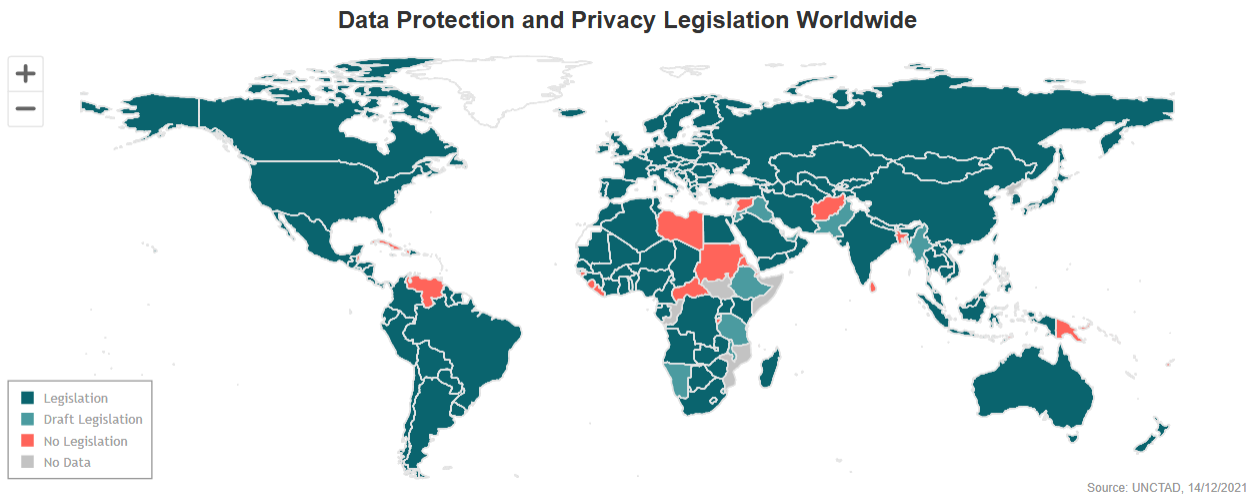
Segundo o portal, em sua última atualização, ocorrida até o ano 2021, os dados revelaram que 137 dos 194 países analisados implementaram legislações para garantir a proteção de dados e privacidade, o equivalente a 71%. Além disso, 9% dos países possuem projetos de lei em tramitação. No entanto, os dados revelaram que 15% de países não constam

---

[16] *UNCTAD Global Cyberlaw Tracker*. Disponível https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide

legislações na área e 5% dos países não constam em nenhum dado que contempla a temática relativa à privacidade e proteção de dados, conforme ilustrado por meios das cores, na figura de n.º 2. Os resultados do rastreamento são disponibilizados na página do site *Data Protection and Privacy Legislation Worldwide*[17].

Figura 2 - Leis de Privacidade no Mundo



Fonte: *Data Protection and Privacy Legislation Worldwide* (2021).

É possível observar que a partir do último rastreamento realizado em 2021, regiões como a África e Ásia que possuíam diferentes níveis de adoção de legislações de proteção de dados e privacidade. Consideramos aqui, que estas são regiões com um número maior de países em suas composições. Por sua vez, a Europa encontra-se em uma posição bem avançada, quase em sua totalidade, sendo 98% legislação implementada e apenas 1% não possui dados disponíveis. Importante ressaltar que qualquer organização que realiza tratamento de dados pessoais nos países europeus, está sujeita ao Regulamento Geral de Proteção de Dados, mesmo que não tenha implementado as diretrizes.

Com relação à participação dos Países Menos Desenvolvidos (PMD) e Pequenos Estados Insulares em Desenvolvimento (PEID), o percentual de implementação das legislações, segundo o rastreamento, é de 48% e 37%, respectivamente. O quadro a seguir detalha o percentual de legislações implementadas, projetos de lei em tramitação, regiões sem legislação ou sem dados disponíveis no cenário mundial:

---

17 *Data Protection and Privacy Legislation Worldwide.* Disponível: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Quadro 1- Legislações de Proteção de Dados e Privacidade em todo o mundo

Região	Legislação	Projeto de Lei	Nenhuma Legislação	Nenhum Dado
África (54 países)	33 (61%)	6 (11%)	10 (19%)	5 (9%)
Américas (35 países)	26 (74%)	4 (12%)	5 (14%)	0 (0%)
Ásia-Pacífico (60 países)	34 (57%)	7 (12%)	15 (25%)	4 (7%)
Europa (45 países)	44 (98%)	0 (0%)	0 (0%)	1 (2%)
Países Menos Desenvolvidos (PMD) (46 países)	22 (48%)	4 (9%)	16 (35%)	4 (9%)
Pequenos Estados Insulares em Desenvolvimento (PEID) (38 países)	14 (37%)	5 (13%)	16 (42%)	3 (8%)

Fonte: Elaborado com base nos dados do rastreamento da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), 2021.

A considerar o impacto da cultura de privacidade e proteção de dados e a atenção voltada para os aspectos dos direitos humanos, torna-se imprescindível que, atualmente, para o desenvolvimento das relações política e econômica, os diferentes Estados busquem uma integração harmônica como favorecimento às relações multilaterais.

Desse modo, o Mercado Comum do Sul (Mercosul), bloco econômico e político formado pelos Países-Membros (Argentina, Brasil, Paraguai, Venezuela[18] e Uruguai), além dos Estados Associados (Chile, Colômbia, Equador, Guiana, Suriname e Peru). Estes últimos são autorizados a participar das reuniões que tratam de temas de interesse comum, em posição de observadores, os quais não serão considerados nesta pesquisa.

Nesta direção, o Mercosul estabeleceu o compromisso de harmonizar suas legislações, nas áreas pertinentes, para obter o fortalecimento do processo de integração[19]. Adicionalmente, fixou para o chamado Grupo Agenda Digital (GDA), o plano de ação para a bienal 2018-2020, a adoção de compromissos em matérias como infraestrutura digital e conectividade; segurança e confiança no ambiente digital; habilidades digitais; governo digital e governo aberto, entre outras matérias.

[18] Atualmente a República Bolivariana da Venezuela se encontra suspensa de todos os direitos e obrigações inerentes à sua condição de Estado Parte do Mercosul, em conformidade com o disposto no segundo parágrafo do artigo 5° do Protocolo de Ushuaia.

[19] De acordo com Tratado de Assunção para a Constituição de um Mercado Comum, os Estados Partes decidiram constituir um Mercado Comum, estabelecido a 31 de dezembro de 1994, denominando como “Mercado Comum do Sul”.

Para alcançar as propostas pelo Mercosul (2017), algumas iniciativas estavam previstas dentro da agenda, as quais possuíam uma relação direta com a proteção dos dados e o acesso à informação, a saber: ações que visavam a obtenção da coerência normativa de políticas nacionais de proteção de dados pessoais; o desenvolvimento de mecanismos conjunto para coordenação de atividades de detecção, prevenção, gestão e resposta a incidentes de segurança digital; a subscrição de um acordo de reconhecimento mútuo de assinaturas digitais; desenvolvimentos de iniciativas conjuntas em matéria de governo aberto, dados abertos, oferta de serviços transfronteiriços por meios digitais e uso de tecnologias emergentes para a otimização dos serviços de governo. Cabe ressaltar que a criação do Grupo Agenda Digital (GAD)[20] para a coordenação da agenda, possibilitou o trabalho de forma integrada, priorizando o desenvolvimento de políticas públicas a respeito de benefícios da transformação digital, bem como, lidar com seus desafios.

Ademais, segundo a Declaração Especial dos Presidentes do Mercosul sobre Democracia e Integridade da Informação em Ambientes Digitais[21], por ocasião da LXIII Cúpula de Presidentes da Mercosul, os representantes dos Estados Membros, apontaram a "importância fundamental do acesso à informação e da liberdade de expressão, opinião, comunicação e manifestação de pensamento, em caráter de princípios e direitos humanos e liberdades fundamentais de sociedades democráticas, particularmente no ambiente digital" (2017). Além disso, foi destacado, que "o amplo e livre fluxo de informações e ideias contribui para fortalecer o acesso à informação de qualidade, que é uma condição necessária para um debate público enriquecedor, livre, pluralista, diversificado, inclusivo e democrático" (Mercosul, 2017). Segundo o documento, foi reiterado que as leis, regulamentos e direitos devem ser aplicáveis e reconhecidos também nos ambientes digitais:

> [...] o compromisso em reconhecer que as mesmas leis, regulamentos e direitos que regem "fora de linha" devem ser aplicáveis também aos ambientes digitais, tais como os direitos à liberdade de expressão, liberdade de imprensa, privacidade e proteção de dados pessoais, não discriminação e direito ao devido processo, com especial atenção aos casos de assédio e difamação, envolvendo também as plataformas digitais nesse propósito (Mercosul, 2017).

[20] Agenda Digital Mercosul, disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital.
[21] A Declaração Especial dos Presidentes do MERCOSUL sobre Democracia e Integridade da Informação em Ambientes Digitais. Disponível em: https://documentos.mercosur.int/public/declaraciones/163.

Os representantes presidenciais concordaram a respeito da urgência de ações que promovam a proteção dos dados e integridade das informações para a garantia dos direitos humanos, sobretudo no fortalecimento da confiança dos cidadãos:

> [...] urgência de promover ações conjuntas, a partir de uma perspectiva de direitos humanos, para a construção da confiança cidadã, a proteção de dados pessoais e a promoção da integridade, exatidão, consistência e confiabilidade das informações circulantes em ambientes digitais, bem como sobre a necessidade de proteger a população contra a disseminação de informações falsas, de discursos de ódio e de outras formas de conteúdo nocivo (Mercosul, 2017).

Além disso, os representantes deliberam que a necessidade de um ambiente que incentive políticas transparentes, no que se refere ao tratamento de dados pessoais e a preservação da privacidade, respeitando as normas vigentes de bloco econômico:

> [...] incentivar políticas transparentes, responsáveis e respeitosas dos direitos humanos por parte das empresas de tecnologia, especialmente com relação à moderação de conteúdo, algoritmos de recomendação e ao tratamento dos dados pessoais, procurando minimizar a proliferação de conteúdos falsos ou ilegais e a defesa dos direitos das pessoas consumidoras desses serviços, inclusive no que tange à preservação da privacidade e à proteção de dados pessoais, em conformidade com os marcos legais e regulatórios vigentes em cada país (Mercosul, 2017).

Anteriormente, a organização havia apresentado orientações a serem observadas pelos países integrantes dos Estados-Membros, disposições relativas à defesa do consumidor e suas relações de consumo, apesar de ainda não dispor de normas específicas sobre a temática proteção de dados. Conforme destacado por Lima (2023, p. 46) as resoluções se referiam à defesa do direito do consumidor, aos princípios fundamentais[22] e a proteção do comércio eletrônico[23].

A Resolução Mercosul/GMC n.º 36/2019, considera "que é importante aprofundar a harmonização de legislações na área de defesa do consumidor no âmbito do Mercosul" e a necessidade do avanço e impulsionamento de ações de proteção do direito do consumidor. Para tal, utilizaram-se dos princípios, como: princípio da ordem pública de proteção; princípio do acesso ao consumo e da transparência dos mercados; princípio de respeito à dignidade da

---

[22] Resolução Mercosul/GMC n. 36/2019, referente a Defesa do Consumidor - Princípios Fundamentais. Disponível em https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/

[23] Resolução Mercosul/GMC n. 37/2019, refere-se a Defesa do Consumidor a Proteção do Comércio Eletrônico. Disponível: https://www.mercosur.int/pt-br/documentos-e-normativa/normativa/

pessoa humana e antidiscriminatório; princípio de prevenção de riscos, princípio da boa-fé e o princípio da informação. Nessa última, recomenda-se que "os fornecedores devem prestar aos consumidores informação clara, verídica e suficiente que lhes permita fazer escolhas adequadas aos seus desejos e necessidades", concordando com os princípios de necessidade, o livre acesso, a qualidade dos dados e a transparência.

Some-se a isto, a Resolução Mercosul/GMC n.º 37/2019, que considerou pertinente a regulação da proteção comércio eletrônico "durante todo o processo da transação, o direito à informação clara, suficiente, verídica e de fácil acesso sobre o fornecedor, o produto e/ou serviço e a transação realizada". O texto ainda recomenda que o fornecedor deve disponibilizar em meios eletrônicos e de fácil localização das informações contratuais, além de "proporcionar um mecanismo de confirmação expressa da decisão de efetuar a transação, de forma que o silêncio do consumidor não seja considerado como consentimento", conforme rege o artigo 5º (Mercosul, 2019).

Segundo Marques, Lima e Reis (2023, p. 46) se propôs a demonstrar o estado da arte a respeito dos principais aspectos (e princípios) relativos à proteção de dados pessoais presentes nos Estados-Membros Argentina, Brasil, Paraguai e Uruguai. Sob a ótica da defesa e o tratamento dos dados dos consumidores, a autora destacou que:

> [...] as características ontológicas das transações que ocorrem por meio do comércio eletrônico e o tratamento de dados pessoais dos consumidores, é quase prosaica a necessidade da asserção de que as garantias ao direito à informação dos consumidores também se refiram à necessidade da garantia pelos Estados-Membros de instrumentos aptos a efetivar o direito à informação nessas transações (Marques; Lima; Reis, 2023).

Nessa direção, o estudo comparativo revelou a existência de harmonia entre as principais normas de proteção de dados da Argentina e do Uruguai, sendo possível observar que as diferenças se davam, sobretudo, em virtude da época de elaboração dessas normas. Tais países estabeleceram disposições normativas, entre 2000 a 2008, anos anteriores aos debates públicos referente ao direito à portabilidade de dados e o comércio eletrônico que iniciaram apenas a partir da década de 2010 (Marques; Lima; Reis, 2023, p. 54).

Outrossim, Marques, Lima e Reis (2023, p. 54), também destacou a carência de discussões relativas às medidas a respeito das boas práticas, da implementação de estruturas de governança em privacidade e proteção de dados pessoais, as avaliações de impacto à proteção de dados pessoais, e ainda, elaboração de normas que estabelecessem critérios específicos para o tratamento de dados pessoais de crianças e adolescentes.

Embora as mencionadas carências, o nível de proteção ao tratamento de dados pessoais e à livre circulação desses dados na Argentina e no Uruguai é considerado adequado, sendo assegurado pela Comissão da União Europeia, nos termos da *Directiva 95/46/CE*, que conferem as decisões de 30 de junho de 2003[24] e 21 de agosto de 2012[25]. Contudo, observou que a Argentina busca atualização do seu regulamento, a partir do projeto de lei que se encontra em tramitação no congresso argentino, desde 2023, tendo em vista, os avanços tecnológicos atuais[26].

Assim como o Brasil, o Paraguai estabeleceu sua norma de proteção de dados pessoais (Lei de Proteção de Dados Pessoais de Crédito) após a implementação do regulamento europeu. Apesar da influência dessa normativa, a legislação paraguaia ainda necessita de consolidação. Conforme o estudo de Marques, Lima e Reis (2023, p. 54), a norma paraguaia omite disposições sobre avaliação de impacto, conceitos de anonimização e pseudonimização, direito à revisão de decisões automatizadas, fluxo transfronteiriço de dados pessoais, e não obriga a designação de um encarregado de dados pessoais. Além disso, também "não dispõe de aspectos relativos ao tratamento de dados pessoais de crianças e de adolescentes e ao tratamento de dados pessoais pelo setor público".

No quadro n.º 2, é possível observar a evolução das principais normas e regulamentos sobre privacidade e proteção de dados nos Países-Membros do Mercosul. Nele, foram destacadas as autoridades fiscalizadoras, responsáveis por garantir o cumprimento das leis e aplicar sanções em caso de descumprimento. A existência dessas autoridades é fundamental para a harmonização legislativa entre os países e para a regulação eficaz do fluxo transfronteiriço de dados pessoais.

---

[24] 2003/490/CE: Decisão da Comissão de 30 de junho de 2003, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à proteção adequada de dados pessoais na Argentina. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003D0490&qid=1741545410045.

[25] 2012/484/UE: Decisão de Execução da Comissão de 21 de agosto de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à proteção adequada de dados pessoais pela República Oriental do Uruguai no que diz respeito ao tratamento automatizado de dados pessoais. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02012D0484-20161217&qid=1741547820632.

[26] 2016/2295 Decisão de Execução da Comissão, em 16 de dezembro de 2016, alterando os termos da Diretiva 95/46/CE Parlamento Europeu e do Conselho relativas ao nível adequado de proteção dos dados pessoais na Argentina, artigos: 3º e 3º -A; Decisão de Execução da Comissão, em 21 de agosto de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à proteção adequada de dados pessoais pela República Oriental do Uruguai no que diz respeito ao tratamento automatizado de dados pessoais. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016D2295.

Quadro 2- Leis de Privacidade dos Países Membros do Mercosul

Países	Legislações sobre Proteção de Dados	Autoridade Fiscalizadora	Considerações
Brasil	Constituição Federal, 1988. Código de Defesa do Consumidor - Lei n° 8.078/1990; Lei do Habeas Data (Lei n° 9.507/1997); Lei de Sigilo Bancário (Lei Complementar n° 105/2001); Lei do Cadastro Positivo (Lei n° 12.414/2011); Lei de Acesso à Informação (Lei n° 12.527/2011 e Decreto n.º 7.724/2012); Marco Civil da Internet (Lei n° 12.965/2014 e Decreto n° 8.771/2016); Resolução n° 2.217/2018 do Conselho Federal de Medicina; Código de Processo Civil - Lei n.º 13.105/2015 (art. 319); Lei Geral de Proteção de Dados Pessoais (LGPD) Lei n.º 13.709, 2018; Resoluções CMN n.° 4.893/2021 e CMN n.° 85/2021 do Banco Central do Brasil; Lei n.º 14.289/2022 (preservação do sigilo sobre a condição de pessoa que vive com infecção pelos vírus HIV e das hepatites crônicas (HBV e HCV) e de pessoas com hanseníase e com tuberculose).	Autoridade Nacional de Proteção de Dados (ANPD)	Apesar da LGPD ter entrado em vigor apenas em 2020, outras leis já abordavam, de forma pontual, os direitos dos indivíduos em relação à privacidade e ao acesso à informação, mesmo sem uma lei específica sobre o tema. A LGPD permite a transferência internacional de dados, desde que os países e organizações proporcionem um grau de proteção de dados pessoais adequado ao previsto na Lei. Além disso, no âmbito das atividades de direito público, a ANPD poderá realizar a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.
Argentina	Reforma Constitucional, 1994 (habeas data) Lei n.º 25.326 de 2000 - Lei de Proteção de Dados Pessoais; Decreto n.º 1.558 de 2001; Decreto n.º 1160 de 2010; Código Penal Nacional da Argentina (art. 117 e 173); Lei n.º 27.078/2014 Lei Digital da Argentina (art.59).	Agência de Acesso à Informação Pública (AAIP)	A Argentina foi um dos primeiros países da América Latina a estabelecer normas para a proteção de dados pessoais, em 2000, seguindo o modelo europeu. Reconhecida em 2003, pela União Europeia como um país que oferece um nível adequado de proteção para dados pessoais. Apesar do reconhecimento, o país criou um projeto de lei para atualização que se encontra em tramitação desde 2023.
Paraguai	Constituição Nacional, 1992 (art.33- O direito à privacidade, art. 135 - Dados de Habeas); Código Penal, 1997 (art. 174 - alteração de dados e art. 175- sabotagem de computadores; Capítulo II Atos puníveis contraprovas documentárias); Lei 1682 de 2001 (revogada); Lei 1.969 de 2002; Lei n.º 4868 de 2013 Comércio Eletrônico (art.6, 7, 10, 23, 36); Lei n.º 5.543 de 2015; Lei n.º 6.534, 2020 (Lei de Proteção de Dados Pessoais de Crédito)	Banco Central do Paraguai; Secretaria de Defesa do Consumidor e do Usuário	A Lei de Proteção de Dados Pessoais de Crédito do Paraguai trata da proteção de dados pessoais de crédito, abrangendo também dados confidenciais. O país possui legislação específica sobre o tema no âmbito das relações comerciais internacionais, no entanto, não possui autoridade autônoma e independente de proteção de dados, além de não possuir obrigatoriedade de nomear o encarregado de dados.

Uruguai	*Constitución de la República Oriental del Uruguay* de 1967 (art.72); *Ley de Protección de Datos Personale* - Lei n.º 18.331 de 2008; Decreto Regulatório n.º 414/009 de 2009 (arts. 47 a 40); *Accountability Act and Balancing of Budget Execution of the Exercise 2017* - Lei n.º 19.670/2018; Lei n.º 19.670 de 2018; Decreto n.º 64/2020 de 2020 (arts. 62 e 63).	*Unidad Reguladora y de Control de Dados Personales (URCDP*)	O Uruguai é um dos países do Mercosul com legislação considerada adequada para a proteção de dados pessoais, juntamente com a Argentina, segundo a Comissão Nacional de Informática e Liberdades (CNIL). O Decreto n. 64/2020 trouxe a figura do "*Delegado de Protección de Datos Personales*" e "*Evaluación de Impacto en la Protección de Datos*"
Venezuela	Constituição da República Bolivariana da Venezuela de 1999 (art. 28, 48, 58, 60); Lei da Criança; Lei da Suprema Corte de Justiça (art. 167).	Não há	Atualmente não há uma lei de proteção de dados propriamente dita, embora haja citações em normas gerais dispersas. O país está suspenso do Mercosul desde 2017.

Fonte: Elaboração própria

Nesta análise das relações econômicas e sociais que influenciam a privacidade e a proteção de dados, o BRICS, formado inicialmente por Brasil, Rússia, Índia, China e África do Sul, merece destaque. Este grupo de países emergentes (não considerado grupo econômico formalmente), com destaque para o crescimento econômico no mercado global, que desempenha um papel importante também para o desenvolvimento humano.

Silva (2023), observou que os países integrantes do grupo se empenham em fomentar o desenvolvimento sustentável e a infraestrutura, os quais abrangem tanto as iniciativas públicas quanto privadas. Nesse cenário, a proteção de dados surge como um elemento crítico para a manutenção da privacidade dos cidadãos e a segurança cibernética diante das diferentes tradições sociais e jurídicas. Além disso, Silva (2023) destacou outros dois fatores, políticos e econômicos, que podem afetar a harmonização entre os países membros.

A respeito das características comuns desses Estados, o autor considera que:

> [...] as políticas de proteção de dados desses Estados apresentam algumas características em comum, mas também diferenças significativas. De modo que manifestam sua similaridade a partir da necessidade de cooperação e colaboração para garantir a segurança e a privacidade dos dados. [...] De sorte que a digitalização massiva e a interconexão de tecnologias tornam esses países alvos de ciberataques, exigindo a implementação de estratégias sólidas e projetos governamentais bem-informados (Silva, 2023).

Quanto aos desafios enfrentados em relação à proteção de dados, devido à complexidade de harmonização e de interoperabilidade entre as legislações dos países

membros, Silva (2023, p. 693-694) destacou a necessidade de “criação de mecanismos de cooperação multissetorial, nos quais os governos do BRICS possam dialogar com acadêmicos, representantes do setor privado e da sociedade civil, abordando as dissemelhanças de cada país”. Essa cooperação é fundamental para enfrentamentos dos desafios comuns, assim como para as aplicações de soluções eficientes.

> [...] os regulamentos de proteção podem garantir a proteção dos direitos humanos e a privacidade dos cidadãos, fortalecendo a democracia e a justiça social. Criar mecanismos de cooperação multissetorial entre os países do BRICS pode promover a troca de conhecimentos e experiências em relação à proteção de dados, fortalecendo a segurança cibernética global (Silva, 2023, p. 697).

Na Rússia, a Lei Federal de 27 de julho de 2006 n.º 152-FZ está em vigor desde 2006, concomitantemente com outras leis que regem a proteção de dados no país. Embora esteja alinhada com o regulamento europeu, a legislação russa tem características próprias. Ademais, a lei tem passado por constantes alterações, um exemplo recente foi a aprovação da Lei Federal n.º 266-FZ, de 14 de julho de 2022. A emenda altera a Lei Federal sobre Dados Pessoais, a qual impõe obrigações mais rigorosas aos operadores, tanto nacionais e estrangeiros, em relação às interações com os titulares, o processamento e a transferência de dados.

No estudo comparativo, Silva (2023, p. 697) destacou que a partir de 2015, a lei passou a obrigar o armazenamento de referências pessoais de cidadãos russos em servidores e conjuntos de arquivos fisicamente localizados no país. No entanto, observou a ausência de clareza no regimento, como a possibilidade de fazer cópias de dados pessoais e o armazenamento fora da Rússia. Ainda reflete a preocupação em relação à criptografia desses dados, como forma a prejudicar a liberdade civis e a privacidade dos indivíduos.

Quanto à China, as normas referentes à proteção de dados que compõem seu arcabouço, fazem parte de uma estrutura complexa e são distribuídas em vários regulamentos, que visam garantir a proteção à privacidade dos cidadãos chineses e além de regulamentar a gestão de dados pessoais no país (DLA Piper[27], 2025). Todavia, “embora a China tenha

[27] DLA Piper, é um escritório de advocacia global que opera por meio de diversas entidades jurídicas. Também é responsável pela ferramenta “Manual de Leis de Proteção de Dados do Mundo” fornece uma visão geral das principais leis de privacidade e proteção de dados no cenário mundial, alcançando mais de 160 jurisdições. Disponível em: https://www.dlapiperdataprotection.com/.

investido em leis e regulamentos [...] a transparência e a monitoração das ações das autoridades persistem há muitos anos" (Silva 2023, p. 698).

Na África do Sul, o direito de privacidade é reconhecido como um direito fundamental pela Declaração de Direitos da Constituição da República da África do Sul e assegurado pela Constituição da República da África do Sul. Estão entre seus objetivos "o direito à privacidade, inclui o direito à proteção contra a coleta, retenção, disseminação e uso ilegais de informações pessoais". Além disso, a legislação prevê que "o Estado deve respeitar, proteger, promover e cumprir os direitos previstos na Declaração de Direitos" regular e harmonizar com as normas internacionais (África do Sul, 2013).

A Lei de Proteção de Informações Pessoais da África do Sul (POPIA), é considerada uma das mais recentes no mundo, em vigor em 2020 e entre suas finalidades, destacam-se:

> Promover a proteção de informações pessoais processadas por órgãos públicos e privados; introduzir certas condições para estabelecer requisitos mínimos para o processamento de informações pessoais; prever o estabelecimento de um Regulador de Informações para exercer certos poderes e desempenhar certos deveres e funções em termos desta Lei e da Lei de Promoção de Acesso à Informação de 2000; prever a emissão de códigos de conduta; prever os direitos das pessoas em relação a comunicações eletrônicas não solicitadas e tomada de decisão automatizada ; regulamentar o fluxo de informações pessoais através das fronteiras da República; e prever questões relacionadas a isso (África do Sul, 2013).

Entre os preâmbulos, a Lei de Proteção de Informações Pessoais da África do Sul tem em mente que deve estar:

> [...] em consonância com os valores constitucionais da democracia e da abertura, a necessidade de progresso económico e social, no quadro da sociedade da informação, exige a remoção de impedimentos desnecessários ao livre fluxo de informação, incluindo informações pessoais (África do Sul, 2013).

Por sua vez, a Índia, após um longo período de debates a respeito da temática, em 2023 foi promulgada a *Digital Personal Data Protection Act (DPDPA*). A lei assim foi modelada a partir do regulamento europeu, e assim como a LGPD não se trata de mera transcrição, possuindo assim características próprias. Ademais, com sua promulgação da legislação indiana substituiu um conjunto de regras na Lei de Tecnologia da Informação

(2000) e nas Regras de Tecnologia da Informação (2011) que orientava de forma superficial a proteção de dados (Conjur, 2023)[28].

Em contraste com a LGPD, a lei indiana de proteção de dados não faz distinção entre dados pessoais e dados pessoais sensíveis. Ambas são consideradas da mesma maneira, e estão sujeitas às mesmas disposições. Além disso, o regulamento trata de forma permissiva e flexível das diretrizes em relação às práticas que dizem respeito à área de tecnologias, numa busca talvez de propor um equilíbrio à economia digital emergente. Outra diferença importante a destacar, são os direitos dos titulares, diferentemente da legislação brasileira, a lei indiana apresenta não apenas os direitos dos titulares, mas também as obrigações a serem desempenhadas pelos titulares de dados, conforme o artigo 15º do regulamento:

> Um Titular de Dados deverá desempenhar as seguintes funções, nomeadamente: (a) cumprir as disposições de todas as leis aplicáveis em vigor no exercício dos direitos ao abrigo das disposições desta Lei; (b) garantir que não se faz passar por outra pessoa ao fornecer os seus dados pessoais para uma finalidade específica; (c) garantir que não suprime qualquer informação material ao fornecer os seus dados pessoais para qualquer documento, identificador único, prova de identidade ou prova de morada emitida pelo Estado ou qualquer dos seus instrumentos; (d) garantir que não registra uma queixa ou queixa falsa ou frívola junto de um Fiduciário de Dados ou do Conselho; e (e) fornecer apenas informações que sejam verificáveis como autênticas, ao exercer o direito à correcção ou ao apagamento ao abrigo das disposições desta Lei ou das regras estabelecidas ao abrigo da mesma (Índia, 2023, tradução nossa).

O quadro a seguir detalha as principais legislações dos países do BRICS, com o foco na existência de autoridade fiscalizadora capaz de interagir com entidades internacionais. Adicionalmente, o levantamento apresenta considerações relevantes sobre o cenário regulatório de cada país.

---

[28] SILVA, Anna Luiza. HAIKAL, Beatriz; BECKER, Daniel. Revista Consultor Jurídico, Era uma vez em Bollywood: nova lei de proteção de dados pessoais da Índia. 26 de novembro de 2023. Disponível em: https://www.conjur.com.br/2023-nov-26/era-uma-vez-em-bollywood-nova-lei-de-protecao-de-dados-pessoais-da-india/. Acesso em 16 de março de 2025.

Quadro 3 - Leis de Privacidade Países Membros do BRICS

Países	Legislações sobre Proteção de Dados	Autoridade Fiscalizadora	Considerações
Rússia	Constituição da Federação Russa (art. 23 e 24) Lei Federal n.º 152 FZ de 27 de julho de 2006 (DPA); Lei Federal n.º 149-FZ de 14 de julho de 2006 (Lei da Informação) Código do Trabalho da Federação Russa; Decreto de 20 de outubro de 2021 n.º 1799 sobre o Credenciamento de Organizações que Possuem Sistemas de Informação que Fornecem Identificação e (ou) Autenticação usando Dados Pessoais Biométricos de Indivíduos (disponível somente em russo aqui) (Decreto n.º 1799) Decreto de 29 de junho de 2021 n.º 1046 sobre Controle Estadual Federal (Supervisão) sobre o Processamento de Dados Pessoais (Decreto n.º 1046); Lei Federal de 14 de julho de 2022 n.º 266-FZ sobre a Emenda à Lei Federal sobre Dados Pessoais (disponível apenas em russo aqui) (a Lei de Emenda).	Serviço Federal de Supervisão de Comunicações, Tecnologias de Informação e Meios de Comunicação de Massa - Roscomnadzor	Lei Federal de 14 de julho de 2022 n.º 266-FZ sobre a Emenda à Lei Federal sobre Dados Pessoais (a Lei de Emenda) foi adotada para impor obrigações mais rigorosas aos operadores de dados nacionais e estrangeiros em termos de como eles interagem com os titulares dos dados, bem como com os processadores, e demonstram sua conformidade geral e especificamente no caso de transferências de dados.
China	Lei de Proteção de Informações Pessoais (PIPL); Lei de Segurança Cibernética (CSL), 12 de setembro 2017; Lei de Segurança de Dados (DSL), 09 de setembro de 2021; Regulamento sobre Facilitação e Regulamentação das Transferências Transfronteiriças de Dados, 22 de março de 2024; Regulamento de Gestão de Segurança de Dados de Rede, 1º de janeiro de 2025.	Administração do Ciberespaço da China (CAC)	A proteção de dados na China reflete o contexto político, sendo também utilizado em favor da segurança nacional.
África da Sul	Constituição da República da África do Sul, 1996; Declaração de Direitos da Constituição da República da África do Sul; Lei de Proteção de Informações Pessoais, (POPIA)	*Information Regulator*	

Índia	Lei de Tecnologia da Informação de 2000 (Lei de TI); Lei de Proteção de Dados Pessoais Digitais de 2023 (Lei DPDP);	não há	A privacidade é um direito fundamental, que está consagrado no Artigo 21 [Direito à Vida e à Liberdade] da Constituição da Índia, em 2017. A Lei DPDP é aplicável apenas a dados pessoais em formato digital e não regulamenta dados não pessoais e não digitais ou digitalizados.

Fonte: Elaboração própria

3 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A proteção dos dados pessoais no cenário brasileiro alcançou destaque sem precedentes a partir do avanço da tecnologia e da transformação digital, em caráter permanente, o qual afetou todas as esferas da vida social, econômica, política e cultural da sociedade. “O seu desenvolvimento histórico se deu a partir de uma série de disposições cuja relação, propósito e alcance foram fornecidos pela leitura da cláusula geral da personalidade e efetivados a partir de estruturas como a defesa do consumidor” (Doneda, 2022, p. 267) antes que pudesse direcionar-se para seu olhar sob a perspectiva da proteção de dados.

A crescente relevância da temática da proteção de dados pessoais ganhava contornos mais nítidos. Doneda (2011, p. 92) já caracterizava a necessidade dessa proteção como um direito fundamental, especialmente diante da expansão do tratamento de dados em processos automatizados, atividade que representa riscos significativos aos indivíduos, conforme destacado pelo autor:

> O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental (Doneda, 2011).

No mesmo estudo (Doneda, 2011, p. 92), o autor argumentava que essas garantias, inicialmente vinculadas à privacidade, deveriam ser compreendidas em um contexto mais amplo. Nesse cenário, outros interesses seriam considerados, e a proteção abrangeria inclusive outras formas de controle possibilitadas pela manipulação de dados pessoais.

A respeito das discussões na esfera do Direito, Sarlet (2022, p. 56) destacou que:

> [...] que tem sido convocado a regular também essa matéria, a despeito de a instituição e subsequente ampliação em termos quantitativos e qualitativos da proteção jurídica de dados pessoais ter iniciado no limiar da Década de 1970, reconhecimento de um direito humano e fundamental à proteção dos dados pessoais, contudo, teve de esperar ainda um tempo considerável para ser incorporado de modo abrangente à gramática jurídico-constitucional (Sarlet, 2022, p. 56).

A Constituição Federal, por sua vez, contemplava o tema da informação e estabelece garantia, por meio como à liberdade de expressão, o direito à informação. Além disso, sob os aspectos da privacidade garante, pauta de forma específicas para os acessos físicos à segurança dos indivíduos, como a proibição da invasão a domicílio ou ainda a violação das correspondências. De forma esparsa, houve um conjunto de disposições que abrangiam a temática da privacidade. No entanto, de forma generalizada, existia uma consciência a respeito da possibilidade de tratar as informações pessoais em categorias amplas e abstratas, como um sistema de permissões e proibições que não considerava os objetivos potenciais desse tratamento. Essa interpretação poderia ampliar a permissividade em relação à utilização indevida (ou seus excessos) das informações pessoais, em um caráter reducionista à proteção dos dados dos indivíduos[29], o que deixava em evidência a complexidade do tratamento dessa matéria. (Doneda, 2022, p. 268-270).

Diante da necessidade de tutela efetiva aos tratamentos sobre os dados pessoais e, ainda, levando em consideração a utilização das novas tecnologias, verificou-se a necessidade de superação desse entendimento para legislar a respeito de uma garantia constitucional autônoma à proteção de dados pessoais. Tal reconhecimento se concretizou a partir da Proposta de Emenda Constitucional n.º 17/2019, que alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, acrescendo ao art. 5º, inciso LXXIX, a informação de que ao indivíduo "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Ao art. 21, inciso XXVI, fixou a obrigação da União de "organizar e fiscalizar a proteção e o tratamento de dados pessoais" e, por fim, incluiu-se ao art. 22, inciso XXX, a competência à União para legislar sobre a temática da proteção e tratamento de dados pessoais, promulgando a Emenda Constitucional n.º 115, em 10 de fevereiro de 2022.

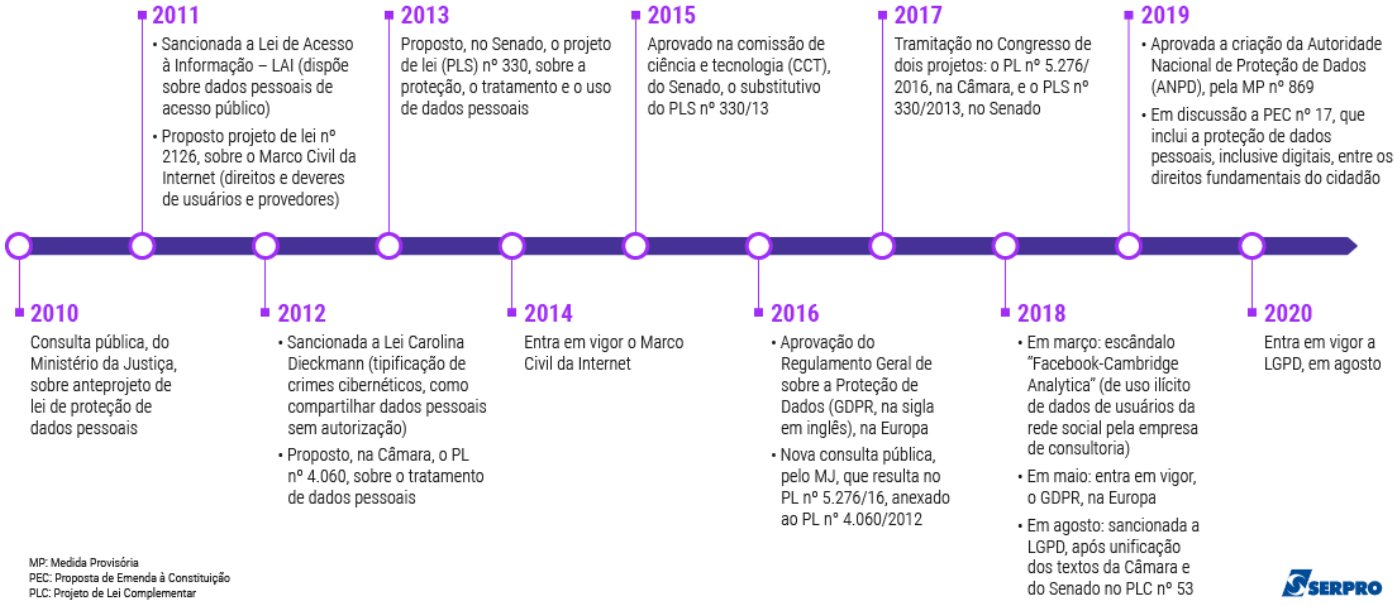
Observa-se que, em quase uma década de discussões acerca da temática da proteção de dados, a "agenda da privacidade e proteção de dados ganhou indiscutível relevância, inclusive em meio aos próprios parlamentares" (Mendonça e Rielli, 2022). Nesse sentido, destacam-se diversas proposições legislativas brasileiras sobre o tema que se enquadraram nesse

[29] O acórdão do Supremo Tribunal Federal, em plenário, no Recurso Extraordinário (RE) 418.416/SC. Rel.: Min. Sepúlveda Pertence. 10/5/2006. Pub. DJ 19 dez. 2006, considerou que "não há violação do art. 5º XII, da Constituição que, conforme se acentuou na sentença, não se aplica no caso, pois não houve quebra de comunicações de dados (interceptação das comunicações), mas sim apreensão de base física [computador] na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". Disponível: https://www.jusbrasil.com.br/jurisprudencia/stf/14732487.

"guarda-chuva", identificado a partir de um estudo que considerou o monitoramento sobre a produção legislativa nas últimas quatro décadas (1980 a 2021), no qual se observou um crescimento expressivo a partir de 2010 e ainda maior entre os anos de 2019 e 2020[30]. Desse modo, a proteção de dados consagrou-se como um direito fundamental, o que colaborou com a diferenciação do direito de privacidade e ampliou a compreensão para o tratamento das informações pessoais e sua relação com a sociedade, possibilitando o exercício da cidadania.

Em relação às fases de evolução e maturação de pautas que tratam de informações pessoais, o SERPRO elaborou uma linha do tempo (Figura n.º 3) que detalha as etapas até a aprovação da LGPD e de outras leis correlatas. É possível observar, nessa linha do tempo, as movimentações mais intensas da última década, com início no final de 2010, desde a abertura da consulta pública do Ministério da Justiça[31] sobre o anteprojeto da lei de proteção de dados pessoais, a sociedade, cujo qual houve outras inserções ao longo do tempo, até sua entrada em vigor em 2020.

Figura 3 - Linha do tempo das fases da LGPD e leis correlatas



Fonte: Serpro, 2020

[30] O estudo foi realizado pela Data Privacy Brasil, na plataforma de monitoramento, resgate e análise sobre os debates em torno do tema de privacidade e proteção de dados. Disponível em: https://observatorioprivacidade.com.br/projetos-em-numeros/.

[31] Não foi localizado para consulta o anteprojeto na internet, no entanto, foi possível verificar a divulgação da notícia pela Folha de São Paulo: https://www1.folha.uol.com.br/fsp/cotidian/ff0112201035.htm

Paralelamente à aprovação da Lei de Acesso à Informação em 2011, o projeto de lei sobre o Marco Civil da Internet (MCI)[32], que regulamenta a Internet, tido antes como um ambiente, onde não havia regulamentação, foi proposto, entrando em vigor em 2014. Essa legislação estabeleceu diretrizes e garantias sobre os direitos e deveres para o uso da internet, abordando a preservação da neutralidade da rede, a liberdade de expressão, a proteção de dados e a privacidade, além de determinar a responsabilização dos agentes conforme suas atividades e as diretrizes para a atuação do Estado.

O cenário brasileiro também testemunhou a sanção da Lei Carolina Dieckmann em 2012. Essa legislação representou um marco ao tipificar crimes cibernéticos, como o compartilhamento indevido de dados pessoais. Entre 2013 e 2017, o Congresso Nacional acompanhou a tramitação simultânea de dois projetos de leis referentes ao tema da proteção e no tratamento de dados pessoais. Esse debate foi impulsionado em 2016, quando a aprovação do Regulamento Geral de Proteção de Dados (GDPR) na Europa ofereceu uma importante base para a subsequente elaboração e sanção da lei de proteção de dados brasileira em 2018.

Outro fato evidenciado na linha do tempo, e que tiveram impactos por todo o mundo, foi o escândalo envolvendo a empresa de consultoria política britânica *Cambridge Analytica* e o *Facebook,* o qual verificou o acesso e uso de dados e informações de usuários de forma indevida para criar perfis psicográficos, além de anúncios personalizados e direcionados a influenciar as decisões de votos de eleitores.

Na perspectiva do zelo e da fiscalização do cumprimento do adequado tratamento dos dados pessoais no Brasil, foi determinada a criação da Autoridade Nacional de Proteção de Dados (ANPD)[33] transformada em seguida em autarquia de natureza especial[34], dotada de autonomia técnica e decisória. Entre seus objetivos estão: zelar, orientar e fiscalizar a proteção de dados no país, podendo, ainda, aplicar sanções administrativas em razão das infrações cometidas às obrigações previstas na LGPD, conforme disposto no artigo 52º:

---

[32] Lei n.º 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[33] Lei n.º 13.853, de 8 de julho de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm

[34] Lei 14.460, de 25 de outubro de 2022. Transformou a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e cargos comissionados; alterou as Leis n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei n.º 13.853, de 8 de julho de 2019. Disponível: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art9

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração;X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Brasil, 2018).

Importante ressaltar a respeito da a criação de um órgão consultivo da ANPD, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), composto por membros da sociedade civil e representantes do poder público, estabelecido no art. 58-A da LGPD. Entre as suas atribuições, destacam-se: propor diretrizes estratégicas que visam fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; a elaboração de relatórios anuais que avaliem a execução das ações da Política Nacional de Proteção de Dados e da Privacidade; sugerir propostas de ações à ANPD; e a elaboração de estudos e debates em audiências públicas que prezam pela disseminação do conhecimento sobre a proteção de dados à população em geral (Brasil, 2024).

3.1 As diretrizes da Lei Geral de Proteção de Dados Pessoais

Antes de começar a refletir sobre as contribuições para a Lei Geral de Proteção de Dados, é necessário avaliar as diretrizes e princípios que regem as atividades realizadas com os dados pessoais e que se configuram nesse novo cenário a utilização das nossas informações pessoais quanto a utilização dos dados pessoais de outras pessoas. Uma vez que, a LGPD afeta desde as ações cotidianas, como o simples acesso a nossas redes sociais ou as ações mais complexas como compras on-line ou a contratação de serviços que envolvem transações bancárias. É fundamental refletir sobre as diretrizes e os princípios estabelecidos pela para a aplicação prática da proteção dos dados pessoais no país. Adicionalmente, vale ressaltar, que neste cenário, trataremos dados pessoais e informações pessoais como sinônimos, uma vez

que no estudo e práticas da Arquivologia não lidamos com dados isolados ou soltos, além da necessidade de que esses dados e informações estejam manifestados em um documento arquivístico com suas devidas características essenciais mantidas em algum suporte.

No seu capítulo inicial, a LGPD apresenta suas disposições preliminares, disciplinando os objetivos norteadores, as relações jurídicas e os sujeitos que se propõe a regular. Além disso, estabelece que, independentemente do meio pelo qual essas informações pessoais circulam, é necessário cumprir os princípios e fundamentos definidos, visando à proteção dos direitos fundamentais de liberdade, de privacidade e ao livre desenvolvimento da personalidade dos indivíduos.

Ao longo dos seus dez capítulos, distribuídos em 65 artigos, a LGPD dispõe sobre os princípios e diretrizes, conforme apresentado na figura 1, na qual propomos uma versão adaptada da figura "A LGPD em um giro" do Serviço Federal de Processamento de Dados (SERPRO), que foi desenvolvida na ocasião para simplificar e ilustrar o entendimento das acerca das diretrizes informadas na lei.

Figura 4 - LGPD - Objetivos e Princípios

Fonte: adaptação do "LGPD em um giro", Serpro (2019)

Nesse contexto, a LGPD disciplina sete fundamentos obrigatórios em seu art. 2º, os quais se referem aos direitos e às garantias fundamentais determinados na Constituição Federal de 1988. A disciplina da proteção de dados pessoais tem como fundamentos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018).

Embora pouco explicado na LGPD, o direito à autodeterminação informativa permite ao titular o controle de seus dados pessoais. Isso inclui a possibilidade de solicitar ao agente controlador dos dados pessoais, ainda que o tratamento seja legítimo, conforme exposto no artigo 18:

> [...] informações de confirmação da existência de tratamento, correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários, portabilidade dos dados a outro fornecedor de serviço ou produto, eliminação dos dados pessoais tratados com o consentimento, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento (Brasil, 2018).

Em continuidade, a Lei 13709/2018, conceitua dado pessoal como informação relacionada a pessoa natural identificada ou identificável, como exemplo podemos citar: nome; data e local de nascimento; RG; CPF; retrato em fotografia; endereço residencial; endereço de e-mail; número de cartão bancário.

A lei também conceitua “dado sensível” como um dado pessoal que necessita de mais atenção devido à sua sensibilidade, e que ao ser revelados podem gerar discriminações ou dano ao titular. Informações como a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico são dados pessoais sensíveis quando vinculado a uma pessoa natural. Nesse sentindo, a LGPD estabeleceu em seu art. 11, hipóteses para o tratamento desses dados sensíveis:

> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a)

> cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Brasil, 2018).

Adicionalmente, a lei apresenta o conceito de tratamento de dados, na qual se aproxima do processamento técnico arquivístico, se formos olhar de uma forma mais geral sem tomar como referência a idade documental. Conforme o expresso no artigo 5º da referida lei:

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Para legitimar essas atividades, os tratamentos de dados pessoais precisam estar alinhados às finalidades informadas ao titular, observando os propósitos legítimos, específicos e explícitos, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. A LGPD dispõe ainda, juntamente com o princípio da boa-fé, de outros noves princípios, que validam as atividades de tratamento dos dados pessoais. Conforme o seu artigo 6º da lei, esses princípios são:

> I - **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância

> e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018. Grifos nossos).

Para além da garantia da utilização correta e o tratamento deve estar compatível com as hipóteses e a finalidade no tratamento dos dados, sendo importante analisar a proporcionalidade e a limitação ao mínimo necessário no uso dos dados pessoais. O tratamento de dados somente poderá ser realizado nas seguintes hipóteses:

> I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n.º 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (Brasil, 2018).

Igualmente importante é a adoção de medidas que garantam o acesso efetivo e transparente às informações tratadas, a prevenção ou a mitigação de riscos aos danos causados pelo uso indevido dos dados pessoais, seja por meio de ações de segurança técnica, administrativa ou organizacionais para a proteção dos dados pessoais.

Cabe ainda observar que, na conjuntura da privacidade e da proteção de dados, é necessária a implementação de um programa de governança[35] para a formulação de regras, procedimentos e aplicação de padrões de boas práticas, previstos no artigo 50º. Em apoio, o Guia de Elaboração de Programa de Governança em Privacidade (2024), desenvolvido pela Administração Pública Federal, orienta sobre uma a construção de uma estrutura mínima para a implementação de uma governança em privacidade. A partir disso pode se estabelecer uma "metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos de impacto à privacidade e melhorias contínuas na maturidade" (MGI, 2024, p.8).

No que diz respeito à abrangência territorial do tratamento dos dados pessoais, a LGPD compreende a sua aplicação em todo o território nacional. No entanto, apresenta no capítulo V da supracitada lei, condições para quando houver a necessidade de transferência ou compartilhamento internacional de dados pessoais para países estrangeiros, ou organismos internacionais, do qual o país seja membro. Além disso, é pertinente a avaliação do nível de proteção de dados do país estrangeiro ou do organismo internacional, que seja condizente com os aspectos legais e a adoção de medidas necessárias para o compartilhamento e a transferência internacional de dados.

Sob outra perspectiva, a abrangência territorial nos leva a resgatar a reflexão sobre o princípio da territorialidade, que, embora discutida de forma indireta e tímida por autores da Arquivologia, se faz necessário compreender o tratamento das informações pessoais nas dinâmicas territoriais e extraterritoriais. Em sua análise, Corrêa (2016, p.13) avalia a questão da "territorialidade para além da delimitação geográfica, uma vez que as ações de influências podem transpor barreiras físicas, e as ações humanas e sociais moldam o território". Nos aspectos da privacidade e da proteção de dados, é importante dar luz para a territorialidade no contexto da guarda e armazenamento em repositórios digitais em nuvens, considerando que esse ambiente ultrapassa as barreiras do físico.

Outro aspecto importante a considerar nesta avaliação da territorialidade são as implicações para a violação da privacidade dos indivíduos. O monitoramento e armazenamento de dados pessoais por meio de tecnologias digitais podem acarretar brechas para uma vigilância digital por partes de empresas que, muitas vezes, não estão alocadas no território brasileiro e têm entre os seus objetivos a coleta de dados pessoais sensíveis para fins

[35] A sexta seção desta pesquisa, trataremos sobre a governança, bem como os princípios da boa governança, suas práticas e mecanismos.

comerciais. Isso pode desviar das finalidades definidas junto ao titular de dados, comprometendo também a ética e a transparência das informações nas organizações.

4 AVALIAÇÃO DAS COMPETÊNCIAS DO ARQUIVISTA NO CONTEXTO DA PROTEÇÃO DE DADOS

No Brasil, a partir da década de 1970, com o aumento da criação de cursos de Arquivologia em universidades públicas, houve também uma evolução na formação do arquivista (Kawabata; Valentim, 2015, p. 88-89).

Bellotto (2014, p. 262)[36] considerava que o arquivista da era da informação, é "senhor do sistema" sob a sua responsabilidade. Devem ter consciência de que a proveniência, a organicidade e a unicidade são meios que colaboram com a garantia da segurança e a autenticidade da informação, independente do suporte dos documentos. Bellotto reforçava que o arquivista deve se integrar ao seu meio de trabalho, compreendendo que o arquivo é mais do que informação registrada, sendo uma entidade integral, completa e indivisível, um instrumento de transmissão. A autora destacava que o arquivista deveria marcar presença na política geral das organizações, atuando e colaborando para além dos conhecimentos técnicos, aproximando as técnicas de gerenciamento de outras técnicas.

Nesse sentido, as competências e responsabilidades do profissional, nota-se que, mesmo após ter se passado mais de 20 anos de sua fala, as considerações de Bellotto permanecem bem atuais. Em análise aos padrões de qualificação que considerava como adequados para a atualização na conduta profissional, partir de alguns teóricos, Bellotto (2004), relacionou em seu estudo que essas qualificações concentram em:

> 1. capacidade de análise e síntese, justamente com uma aptidão particular de esclarecer situações complexas e ir ao essencial; 2. habilidade de formular claramente suas ideias, tanto de forma escrita como verbal; 3. capacidade do julgamento seguro; 4. aptidão para tomar decisões sobre questões ligadas à memória da sociedade; 5. abertura às novas tecnologias da informação; 6. bom senso para tomar resoluções; 7. adaptação à realidade, às condições de seu tempo e lugar. E como se tudo isso ainda pouco, fala-se, também, nas qualidades de adaptabilidade, pragmatismo, curiosidade intelectual, rigor, método, continuidade, capacidade de compressão e escuta relativamente ao produtor, ao pesquisador e ao cidadão (Bellotto, 2004, p. 263).

Na perspectiva da Arquivologia, Schellenberg (2006, p. 165) afirmava que as responsabilidades do arquivista deveriam estar claramente definidas em lei. Além disso, o autor destacava, em seus estudos, os pontos essenciais para a administração de arquivos, entre

---

[36] Publicado originalmente em Cenários Arquivísticos, Brasília, v.1, n1, p.47-52,jan./jul.2002. XIII Congresso Brasileiro de Arquivologia, 2000.

eles a natureza das atividades e de autoridade, na qual considerava que as responsabilidades lhes eram atribuídas dentro das organizações e das estruturas de trabalho a que serviam. Adicionalmente, Schellenberg (2006, p. 165) destacou aspectos importantes sobre a natureza da organização, a qual considerava que o arquivista deveria selecionar e formar cuidadosamente o seu pessoal, planejar o trabalho, definir métodos e diretrizes a serem seguidos para desenvolver uma gestão arquivística eficaz.

No que concerne ao fazer arquivístico, as competências e habilidades profissionais do arquivista, consideradas no cenário atual, foram estabelecidas pelo Ministério da Educação (MEC), por meio da aprovação de diretrizes que orientam sua atuação (2021). Essas competências e habilidades foram divididas em duas categorias, gerais e específicas, e visam preparar o arquivista para enfrentar os desafios inerentes à profissão. As competências e habilidades incluem:

> A) Gerais: identificar as fronteiras que demarcam o respectivo campo de conhecimento; gerar produtos a partir dos conhecimentos adquiridos e divulgá-los; formular e executar políticas institucionais; elaborar, coordenar, executar e avaliar planos, programas e projetos; desenvolver e utilizar novas tecnologias; traduzir as necessidades de indivíduos, grupos e comunidades nas respectivas áreas de atuação; desenvolver as atividades profissionais autônomas, de modo a orientar, dirigir, assessorar, prestar consultoria, realizar perícias e emitir laudos técnicos e pareceres; responder a demandas de informação produzidas pelas transformações que caracterizam o mundo contemporâneo. B) Específicas: compreender o estatuto probatório dos documentos de arquivo; identificar o contexto de produção de documentos no âmbito de instituições públicas e privadas; planejar e elaborar instrumentos de gestão de documentos de arquivo que permitam sua organização, avaliação e utilização; realizar operações de arranjo, descrição e difusão (MEC, 2021).

A respeito do conceito de competência e habilidade, para alguns autores (Freitas; Brandão, 2005), **as competências humanas ou profissionais** são entendidas como:

> Combinações sinérgicas de conhecimentos, habilidades e atitudes, expressas pelo desempenho profissional dentro de determinado contexto organizacional, que agregam valor às pessoas e às organizações (Carbone et al., 2009, p. 34).

Além disso, as competências também podem ser entendidas como “qualidades de quem é capaz de analisar uma situação, apresentar soluções e resolver assuntos ou problemas" (Chiavenato, 2004, p. 4). Por sua vez, o conceito de **habilidade** é compreendido como “a capacidade de transformar conhecimento em ação e que resulta em um desempenho desejado”

(Chiavenato, 2004, p. 4). De acordo com o mesmo autor, (Chiavenato, 2004, p. 3) existem três tipos de habilidades importantes para um desempenho bem-sucedido, a saber: (1) habilidades técnicas, (2) habilidades humanas e (3) habilidades conceituais. Chiavenato (2004, p. 3) considera que as habilidades técnicas envolvem o uso do conhecimento especializado na execução de um trabalho ou dos procedimentos necessários à sua realização, estando relacionadas com o fazer. Envolvem o trabalho com "coisas", números, com material físico e concreto. As habilidades humanas estão relacionadas com a interação entre as pessoas, o relacionamento interpessoal e também grupal. Envolvem a capacidade de comunicar, de motivar, de liderar e a de resolução de conflitos pessoais. As habilidades conceituais estão relacionadas à capacidade de enxergar o todo, bem como a facilidade de trabalhar com conceitos, ideias e abstrações. Além disso, representam as capacidades cognitivas mais sofisticadas do administrador e que lhe permitem planejar o futuro, interpretar a missão, desenvolver a visão e perceber oportunidades onde ninguém enxerga nada" Chiavenato (2004, p. 3).

No que concerne às competências arquivísticas, Bahia (2018, p. 24), buscou definir o conceito ressaltando a importância para as organizações, sabendo que competência pode estar envolvida com a ascensão de níveis. A autora destacou a associação do conceito ao desempenho complexo e à maturidade das pessoas. Também ressaltou que as competências podem ser desenvolvidas, formuladas e efetivadas na sequência de um processo formal ou em resposta a alguma situação. Além disso, a autora, na sua abordagem, enfatizou a sensibilidade do arquivista e a sua capacidade de liderança para identificar as fronteiras que delineiam os respectivos campos de conhecimento. No estudo em questão, Bahia (2018, p. 25) apontou o interesse crescente das empresas e de pesquisadores pela temática das competências e aproximou sua abordagem à de Zarifian (2012, p. 66), que relacionava o conceito de competência ao conceito de qualificação, referindo-se à capacidade de uma pessoa de assumir iniciativas, ser proativa e dominar novas situações no trabalho que surgirem.

> [...] competência é a capacidade de transformar conhecimentos, habilidades e atitudes (CHA) que, quando integrados e utilizados estrategicamente pela pessoa, permitem que ela atinja com sucesso os resultados que deseja (Zarifian, 2012, p. 66).

Por sua vez, Zarifian (2012, p. 66) também relacionava o conceito de competência à capacidade de mudança do comportamento social dos indivíduos em relação ao trabalho e à

sua organização. No âmbito prático, trata-se da capacidade de mobilizar pessoas em torno de objetivos comuns, incentivando-as a atuar como corresponsáveis por suas ações.

4.1 A Normatização da atuação do Arquivista

A profissão do arquivista foi regulamentada pela Lei n.º 6.546 de 4 de julho de 1978, conforme estabelecido no artigo primeiro, que orienta sobre a atuação do arquivista[37].

De imediato, no art. 2º, são estabelecidas 12 atribuições dos arquivistas. Observa-se que uma parcela dessas atribuições, especificamente 8, trata de habilidades e competências que dizem respeito ao planejamento, à organização, à direção e ao controle, conforme demonstrado nas atribuições destacadas abaixo:

> I - **planejamento, organização e direção** de serviços de Arquivo; II - **planejamento, orientação e acompanhamento** do processo documental e informativo; III - **planejamento, orientação e direção** das atividades de identificação das espécies documentais e participação no planejamento de novos documentos e controle de multicópias; IV - **planejamento, organização e direção** de serviços ou centro de documentação e informação constituídos de acervos arquivísticos e mistos; V - **planejamento, organização e direção** de serviços de microfilmagem aplicada aos arquivos; VI - **orientação do planejamento** da automação aplicada aos arquivos; VII - **orientação** quanto à classificação, arranjo e descrição de documentos; VIII - **orientação** da avaliação e seleção de documentos, para fins de preservação; IX - promoção de medidas necessárias à conservação de documentos, X - elaboração de pareceres e trabalhos de complexidade sobre assuntos arquivísticos; XI - assessoramento aos trabalhos de pesquisa científica ou técnico-administrativa; XII - desenvolvimento de estudos sobre documentos culturalmente importantes (Brasil, 1978, grifo nosso).

De acordo com Jardim (2018, p. 32), o arquivista necessita identificar e atuar sobre as mudanças das organizações contemporâneas, observando os impactos nos contextos da sociedade. Neste cenário de transformações, o autor destacou que os modos de produção, acesso e conservação também demandam de inovações, sobretudo, nas práticas de gestão dos serviços e também nas instituições arquivísticas. Neste contexto, Jardim (2018) definiu gestão arquivística como:

---

[37] Ressaltamos que, para esta pesquisa, consideramos exclusivamente as atribuições relacionadas ao trabalho específico do arquivista, conforme definido na lei, ou seja, com formação no país ou no exterior e devidamente provisionados. Excluindo, portanto, a análise das atribuições do técnico de arquivo.

> Conjunto de elementos mobilizados para a gerência de serviços e instituições arquivísticas. Inclui todo o ciclo, da produção à guarda permanente, passando pela gestão de documentos, a preservação, a produção de mecanismos de recuperação da informação, a difusão, o acesso e as demais operações que constituem a missão das instituições e serviços arquivísticos. Envolve também os aspectos gerenciais relacionados a pessoas, infraestrutura física, legal, tecnológica, recursos orçamentários, etc. (Jardim, 2018, p. 32).

O conceito de gestão arquivística definido por Jardim (2018) converge às práticas do gerenciamento arquivístico conforme conceituado por Silva (2024, p. 82) que, inclusive, o apresenta como sinônimo da gestão arquivística. Ademais, podemos também observar que as responsabilidades, que destacamos anteriormente e que integram as atribuições dos arquivistas (art. 2º da Lei 6.546/1978), se concentram no desenvolvimento do gerenciamento arquivístico, que de acordo com Silva (2020, p. 133), fazem parte do escopo de competências essenciais para a atuação do bacharel em Arquivologia e que consistem em planejar, organizar, dirigir e controlar os seguintes elementos:

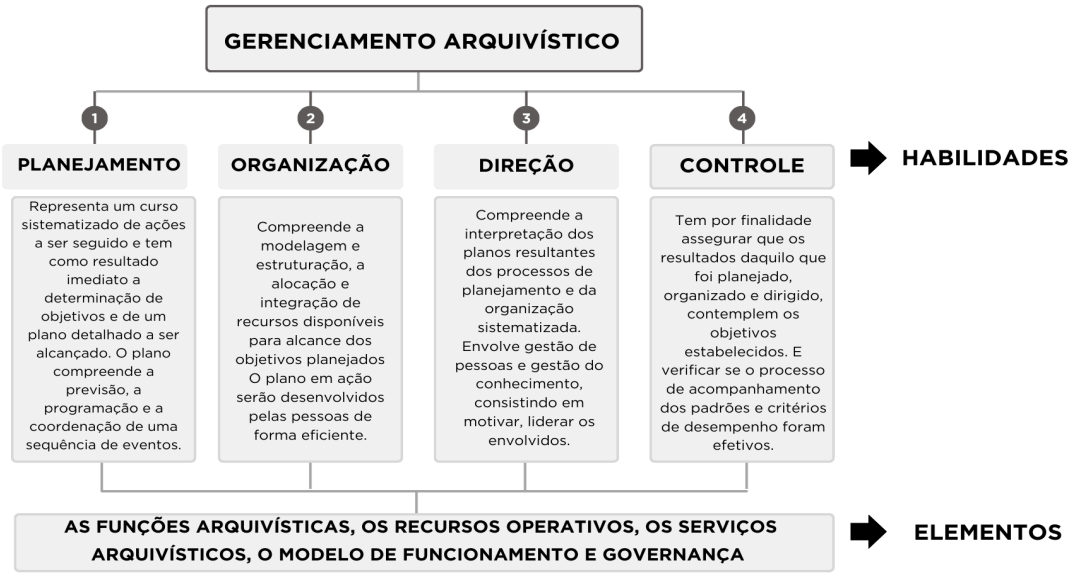
> Das funções e atividades técnicas arquivísticas, incluindo desde a regulamentação dos processos e procedimentos decorrentes até os métodos e diretrizes a serem seguidos e os seus instrumentos arquivísticos que precisam ser elaborados; dos recursos operativos necessários, como espaços físicos e digitais, recursos materiais e tecnológicos, equipes técnicas e seus respectivos custos; dos serviços arquivísticos (unidades administrativas técnicas e/ou destinadas aos usuários internos e/ou externos) nos quais as funções arquivísticas serão executadas e os recursos operativos serão alocados; do modelo de funcionamento e governança (redes ou sistemas) de uma ou mais estrutura orgânica (instituição arquivística ou não) encarregada(s) dos serviços e funções arquivísticas em ambiente a ser considerado (Silva, 2024, p. 80).

Importante ressaltar que a abordagem de Silva (2020, p. 133) rompe com os rótulos burocráticos e tecnicistas imaginados por boa parte da sociedade e também praticada por alguns arquivistas. O autor propõe uma nova postura profissional à qual os arquivistas devem se apropriar.

Considerando que **as funções arquivísticas, os recursos operativos, os serviços arquivísticos e o modelo de funcionamento e governança**, mencionados por Silva (2024, p. 80), são elementos essenciais para o funcionamento eficiente de uma instituição, apresentamos, na Figura 5, uma representação das características das competências e habilidades arquivísticas associadas a esses elementos. Essa representação ilustra como as competências e habilidades relacionadas ao planejamento, organização, direção e controle,

orientações dispostas no art. 2º da Lei n.º 6.546/1978, se articulam no âmbito do gerenciamento arquivístico.

Figura 5 - Competências e Habilidades para o Gerenciamento Arquivístico



Fonte: Elaboração própria, com base em Silva (2024).

Em diálogo com os estudos realizados por Jardim (2018) e Silva (2020; 2024), podemos observar o teor gerencial das responsabilidades e habilidades arquivísticas em consonância com as abordagens desenvolvidas por Chiavenato (2000) quando aborda a tarefa da Administração:

> A tarefa da Administração é a de interpretar os objetivos propostos pela organização e transformá-los em ação organizacional por meio do planejamento, organização, direção e controle de todos os esforços realizados em todas as áreas e em todos os níveis da organização, a fim de alcançar tais objetivos da maneira mais adequada à situação. Assim, a Administração é o processo de planejar, organizar, dirigir e controlar o uso de recursos a fim de alcançar objetivos (Chiavenato, 2000, p. 7).

Prosseguindo com a análise das atribuições dispostas no art. 2º, a Lei n.º 6.546/1978 apresenta outras quatro responsabilidades na qual se referem aos incisos: IX a XII. No que diz respeito à elaboração de pareceres técnicos, observa-se que o arquivista é o profissional capacitado para analisar e realizar diagnósticos, além de propor alterações e medidas com base em critérios arquivísticos. Destaca-se que Bahia (2018, p. 198) descreve uma grande

incidência de busca por essa competência. A autora reafirma que essa é uma habilidade que requer do profissional outros conhecimentos envolvidos.

> Esta prática requer conhecimento da estrutura da segurança do trabalho, das relações interpessoais e do bem-estar no ambiente do trabalho, mobilizando assim recursos humanos, capacitação no universo digital, gestão documental, gerenciamento, manuseio, uso e acesso, catástrofes e desastres naturais, edifício, acervo e plano de emergência (Bahia, 2018, p. 198).

Bellotto (2004, p. 301), por sua vez, em estudos anteriores, evidenciou a respeito da "capacidade [do arquivista] de análise e síntese juntamente com uma aptidão particular para esclarecer situações complexas" e emitir julgamentos seguros. A título de esclarecimento, considera-se relevante apresentar, aqui, o significado do termo "parecer" para uma compreensão mais precisa dessa atribuição, mencionada no inciso X do art. 2º. Por exemplo, Bellotto (2004, p. 101) definiu o termo como uma "opinião técnica ou científica sobre um ato que serve de base à tomada de decisão" e comparou o termo a "consulta".

A Lei 6.546/1978 também regulamenta a competência de assessoramento aos trabalhos de pesquisas científicas e técnico-administrativas. Os dados apresentados por Bahia (2018, p. 179), em sua pesquisa realizada no Portal Catho, indicaram uma incidência que evidenciou a importância dessa competência como um diferencial competitivo para o destaque no mercado de trabalho, conforme destacado pela autora:

> O profissional arquivista é o gestor de processos documentais e está apto a trabalhar com soluções de tratamento funcional da documentação arquivista (sic), atendendo às demandas administrativas e técnico-científicas da sociedade (Bahia, 2018. p. 191).

No tocante à atuação do arquivista no apoio ao desenvolvimento tanto para a pesquisa científica quanto técnico-administrativa, Jardim (1998) avalia as potenciais transformações emergentes da produção, uso e transferência da informação. E ainda, as interseções entre o arquivo, o arquivista e a Arquivologia, que configuram novas dimensões para a pesquisa no campo arquivístico. Nesse contexto, o autor visualiza o arquivista como sujeito também no papel de produtor de conhecimento e pressupõe um exercício de reflexão quanto ao estado da arte no campo, considerando o papel da informação e da ciência no mundo contemporâneo.

Como última atribuição do profissional, mencionada no artigo 2º, Lei n.º 6.546/1978, refere-se ao desenvolvimento de estudos sobre documentos culturalmente importantes. Uma vez que existem várias possibilidades de analisar essa atribuição, propomos a abordagem

dessa análise sob o aspecto da responsabilidade social do arquivista — governo, cidadão e sociedade —, destacando a sua contribuição para a garantia democrática de direitos dos indivíduos, como o acesso à informação e o direito à proteção de dados.

Para proceder com a aplicação da lei para a profissão de arquivista, foi promulgado o Decreto n.º 82.590, em 6 novembro de 1978, que estabelece que o exercício das profissões de Arquivista depende de registro na Delegacia Regional do Trabalho do Ministério do Trabalho. O Decreto em questão aborda as atribuições nos mesmos moldes da Lei 6546/1978.

Em complemento, a Classificação Brasileira de Ocupações (CBO), instituída pela Portaria n.º 397 em 2002, tem por objetivo identificar e atualizar as ocupações profissionais, incluindo atualizações constantes a respeito das atividades profissionais. A partir da busca pelo termo "arquivista" no site do Ministério do Trabalho e Emprego, foram encontrados os seguintes títulos listados no quadro 4.

Quadro 4 - Classificação Brasileira de Ocupações de Arquivista

Códigos	Títulos	Tipo
2613-05	Arquivista	Ocupação
4151-05	Arquivista de documentos	Ocupação
2611-05	Arquivista pesquisador (jornalismo)	Ocupação
2613	Arquivista e museólogos	Família

Fonte: Ministério do Trabalho e Emprego (2010).

Consoante as competências pessoais identificadas nesta análise, a CBO considera que o arquivista deve demonstrar habilidade para o trabalho em equipe de forma interdisciplinar, atuando com ética, flexibilidade e criatividade. Espera-se que o arquivista desenvolva raciocínio lógico e abstrato, acuidade espacial, senso de organização, além de possuir bom conhecimento em legislação e participar de conselhos profissionais (Brasil, 2010). Em relação à descrição sumária da ocupação, a CBO considera que os arquivistas:

> Organizam documentação de arquivos institucionais e pessoais, criam projetos de museus e exposições, organizam acervos museológicos públicos e privados. Dão acesso à informação, conservam acervos. Preparam ações educativas ou culturais, planejam e realizam atividades técnico-administrativas, orientam a implantação das atividades técnicas. Participam da política de criação e implantação de museus e instituições arquivísticas (Brasil, 2010).

A respeito das áreas mapeadas para atuação do arquivista, a CBO considera as seguintes atividades: organizar documentação de arquivos institucionais e pessoais; criar

projetos e exposições; garantir o acesso à informação; conservar acervos; preparar ações educativas e/ou culturais; planejar atividades técnico-administrativas; orientar a implantação de atividades técnicas; participar da política de criação e implantação de instituições arquivísticas; realizar atividades técnico-administrativas; administrar atividades patrocinadas; e comunicar-se.

4.2 A função do encarregado pelo tratamento de dados pessoais

A LGPD traz em seu ordenamento a figura do encarregado pelo tratamento de dados e o define como: "A pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (Brasil, 2018).

No contexto europeu, esse profissional é denominado como *Data Protection Officer* (DPO), uma nomenclatura bem aceita no Brasil. O termo foi introduzido a partir da aprovação do *General Data Protection Regulation* (GDPR).

No Brasil, por ocasião da criação da ANPD[38], também foi proposta a alteração na redação da LGPD, redefinindo a função do encarregado pelo tratamento de dados, na qual passou a permitir o desempenho das atividades por pessoas jurídicas, e não apenas por pessoas físicas. Além disso, passou também a exigir[39] a indicação do encarregado pelo agente operador de dados.

Segundo a LGPD, em seu artigo 41º, o controlador deverá indicar o encarregado pelo tratamento de dados pessoais, divulgando sua identidade e as informações publicamente de forma clara e objetiva. As atividades relacionadas às responsabilidades 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 (Brasil, 2018).

[38] A Lei n.º 13853, de 8 de julho de 2019, determina a criação da Autoridade Nacional de Proteção de Dados e alterou a definição do encarregado pelo tratamento de dados na Lei n.º 13.709, de 14 de agosto de 2018.

[39] Observa-se que a Resolução n.º 18, retoma o texto inicial da LGPD e passa a considerar a indicação do encarregado para operador como facultativa, sendo considerada política de boas práticas de governança para fins do disposto no art. 52, § 1º, inciso IX, da Lei n.º 13.709, de 14 de agosto de 2018, e no art. 13, inciso II, do anexo da Resolução CD/ANPD n.º 4, de 24 de fevereiro de 2023.

Apesar de definir as atribuições do encarregado de forma sucinta, o regulamento prevê a possibilidade de estabelecer normas complementares sobre a indicação ou até a dispensa do encarregado, levando em conta a natureza, o porte e volume de operações de tratamento de dados, conforme disposto no inciso 3º deste mesmo artigo (Brasil, 2018).

Considerando que cabe ao encarregado fazer a interface entre o titular de dados, o agente de tratamento e a ANPD, observa-se que a função configura uma posição central no direcionamento da implementação da LGPD, atuando como mediador para orientar quanto às melhores práticas de proteção de dados dentro das organizações. Observa-se ainda que o papel do encarregado vai muito além do canal de comunicação, desempenhando uma função de assistência e orientação sobre as demandas da implementação de melhores práticas para a proteção de dados e garantia do cumprimento do direito fundamental no Brasil.

Diante da necessidade de maior detalhamento sobre o papel do encarregado pelo tratamento de dados, a ANPD aprovou, em 16 de julho de 2024, a Resolução CD/ANPD n.º 18, que especifica de forma mais clara suas atribuições. Além disso, a resolução oferece maior segurança jurídica em relação a possíveis conflitos de interesse e reforça a autonomia técnica do encarregado de dados para a execução das atividades, livre de interferências indevidas.

No segundo capítulo, a norma determina a indicação do encarregado por ato formal, do qual devem constar as atribuições e atividades a serem desempenhadas, além de informar um suplente para a função. Essa ação demonstra a adoção de políticas de boas práticas e governança, conforme disposto na LGPD, no art. 52, bem como a previsão da continuidade das atividades em caso de ausência ou vacância, conforme destaca o terceiro artigo:

> A indicação do encarregado deve ser realizada por ato formal do agente de tratamento, do qual constem as formas de atuação e as atividades a serem desempenhadas.§ 1º Entende-se por ato formal o documento escrito, datado e assinado, que, de maneira clara e inequívoca, demonstre a intenção do agente de tratamento em designar como encarregado uma pessoa natural ou uma pessoa jurídica.§ 2° O documento referido no caput deverá ser apresentado à ANPD, quando solicitado (Brasil, 2024).

A resolução aborda em seu artigo 7º a respeito das qualificações necessárias para o desempenho das atribuições e considera os conhecimentos sobre legislação de proteção de dados pessoais e seus contextos, o volume e os riscos envolvidos nas operações de tratamentos. Além disso, aborda as obrigações dos agentes de tratamento; contudo, é possível identificar algumas responsabilidades associadas diretamente ao papel do encarregado pelo tratamento de dados. Compete ao encarregado prestar assistência e orientação ao agente de

tratamento na realização de atividades e ainda para a tomada de decisões estratégicas referentes ao tratamento de dados pessoais. Além disso, o encarregado tem garantido o acesso direto às pessoas de maior nível hierárquico dentro da organização, que tomam as decisões estratégicas que afetam ou envolvem o tratamento de dados pessoais (Brasil, 2024).

Em relação às características e atribuições do encarregado pelo tratamento de dados, a norma estabelece que para o exercício da atividade: "não pressupõe a inscrição em qualquer entidade nem qualquer certificação ou formação profissional específica" (Brasil, 2024). No entanto, é importante considerar que uma pessoa que ocupa essa função deve possuir conhecimentos e habilidades sobre a área de proteção de dados. Além disso, é fundamental que o encarregado adote uma inteligência de aprendizado contínuo.

No que se refere às atribuições e responsabilidades do encarregado, a resolução considera:

> Art. 15. I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis; II - receber comunicações da ANPD e adotar providências; III - orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares. Parágrafo único [...] I - encaminhar internamente a demanda para as unidades competentes; II - fornecer a orientação e a assistência necessárias ao agente de tratamento; e III - indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado. Art. 16 [...] I - registro e comunicação de incidente de segurança; II - registro das operações de tratamento de dados pessoais; III - relatório de impacto à proteção de dados pessoais; IV - mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais; V - medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito; VI - processos e políticas internas que assegurem o cumprimento da Lei n.º 13.709, de 14 de agosto de 2018, e dos regulamentos e orientações da ANPD; VII - instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais; VIII - transferências internacionais de dados; IX - regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei n.º 13.709, de 14 de agosto de 2018; X - produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e XI - outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais (Brasil, 2024).

Embora a norma atribui diversas responsabilidades ao encarregado pelo tratamento de dados, ela não confere a responsabilidade perante a ANPD. Cabe ao controlador a responsabilidade pela garantia da conformidade das operações de tratamentos dos dados pessoais.

Quanto à criação e registro da ocupação do Encarregado pelo Tratamento de Dados Pessoais, conforme prevista na LGPD, observa-se que era algo esperado por profissionais que já atuavam e ocupavam essa função[40]. O novo termo foi oficialmente incluído na Classificação Brasileira de Ocupações, em 2022, como Oficial de Proteção de Dados Pessoais (DPO). Além disso, o título está inserido na família n.º 1421, que corresponde ao grupo de Gerentes administrativos, financeiros, de riscos e afins.

No que se refere à categoria de riscos, é interessante destacar o papel do encarregado para o gerenciamento de riscos, no qual ele deve atuar na mitigação. Por exemplo, prestar assistência e orientação na elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)[41]. Este relatório é obrigatório para o controlador em situações de tratamento que possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais, bem como às liberdades civis e aos direitos fundamentais do titular de dados. Além disso, o relatório deve ainda incluir medidas, salvaguardas e mecanismos de mitigação de riscos (Brasil, 2018).

Abaixo, apresentamos a descrição sumária relativa à ocupação do Oficial de Proteção de Dados Pessoais:

> Planejam processos administrativos, financeiros, de compliance, de riscos e de proteção de dados pessoais e privacidade e de facilities management. Gerenciam equipes, prestação de serviços terceirizados, rotinas administrativas e financeiras. Administram riscos, recursos materiais e canal de denúncia. Participam da implementação do programa de compliance e/ou de governança em privacidade. Planejam e implementam atividades de manutenção e conservação do ambiente construído. Monitoram e avaliam o cumprimento das políticas do programa, normativas, código de ética, procedimentos internos e parceiros de negócios. Participam da identificação de situações de riscos e propõem ações para mitigação dos mesmos. Prestam atendimento ao cliente e/ou cooperado e/ou titular de dados pessoais (CBO, 2022).

---

[40] Conforme artigo publicado pelo blog Migalhas, em 25 de março de 2022. Disponível: https://www.migalhas.com.br/depeso/362444/dpo-atividade-inscrita-no-cbo-pelo-ministerio-do-trabalho

[41] RIPD: Relatório de impacto à proteção de dados pessoais: 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.

A respeito das competências pessoais para essa ocupação, a CBO considera importante que o encarregado possua uma visão global organizacional e uma capacidade de observação analítica. Ele deve demonstrar capacidade investigativa e habilidade para tomada de decisões. Além disso, é fundamental que o profissional tenha flexibilidade e saiba trabalhar em equipe. É importante que o profissional tenha habilidade em lidar em cenários que exijam administração de conflitos e foco na resolução de problemas. A competência em comunicação também é essencial, permitindo que ele transmita informações de forma clara e objetiva.

4.3 Análise comparativa dos regulamentos das funções do Arquivista e do Encarregado pelo tratamento de dados

Com base nas análises realizadas sobre as competências, habilidades e atribuições relativas à profissão de arquivista e à função de encarregado pelo tratamento de dados, fundamentadas em suas legislações — a Lei n.º 6.546/1978 e a Resolução CD/ANPD n.º 18/2024 —, este capítulo busca identificar as convergências, entendidas como a direção comum para um mesmo ponto. E as semelhanças, observadas como a relação entre coisas ou ideias que apresentam elementos análogos entre si.

Para melhor visualizar no quadro 5, foram dispostas as atribuições das suas funções e categorizadas a partir das convergências e semelhanças identificadas nas duas legislações. A partir dessas análises, foi possível identificar proximidades no desempenho do arquivista na condução de ações sistematizadas de planejamento, organização, orientação e acompanhamento de serviços arquivísticos e da execução das funções arquivísticas, em favor da função de encarregado pelo tratamento de dados.

A título de exemplo, podemos destacar, na segunda linha do quadro 5, a semelhança da atribuição para o cumprimento do atendimento às solicitações ou reclamações dos titulares de dados, com a obrigatoriedade da garantia do direito de acesso às informações pessoais, conforme determinado pela LGPD. Além disso, observamos também a convergência com práticas do gerenciamento arquivístico e da governança organizacional.

Quadro 5 - Semelhanças e convergências entre as atribuições do Arquivista e do Encarregado

Arquivista	Encarregado de Dados	Categorias	Comentários
Planejamento, organização e direção de serviços de Arquivo.	Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis.	Semelhança e Convergência	Relaciona-se com o acesso à informação e à transparência, atendendo aos direitos do titular/cidadão; Convergência com práticas do gerenciamento arquivístico e da governança organizacional
	Recebimento de comunicações da ANPD e adoção de providências.	Convergência	Relaciona-se com a prestação de contas e a responsabilização.
	Encaminhamento das demandas para as unidades competentes.	Convergência	
Planejamento, orientação e acompanhamento do processo documental e informativo/orientação quanto à classificação, arranjo e descrição de documentos; avaliação e seleção de documentos, para fins de preservação.	Registro das operações de tratamento de dados pessoais; assistência e orientação para a transferências internacionais de dados.	Semelhança	Assemelha-se às práticas arquivísticas desde a produção até a destinação final e as operações de tratamento de dados.
	Orientação aos funcionários e aos contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.	Convergência	Relaciona as orientações a respeito das práticas desde a produção, a destinação final e as operações de tratamento de dados;
Elaboração de pareceres e trabalhos de complexidade sobre assuntos arquivísticos.	Assistência e orientação para a elaboração do Relatório de impacto à proteção de dados pessoais.	Convergência e semelhança	Elaboração do RIPD pelo arquivista em conjunto com outras áreas, interações das convergências e semelhanças.
	Assistência e orientação na elaboração e implementação de processos e políticas internas que assegurem o cumprimento da LGPD e dos regulamentos e orientações da ANPD.	Convergência	Convergência com práticas do gerenciamento arquivístico e da governança organizacional. (Implementação de programa de governança em privacidade).
	Implementação ou definição dos mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais.	Semelhança	Relaciona-se com implementação das boas práticas (normas ISO's e normas arquivísticas) e o gerenciamento de riscos.
Promoção de medidas necessárias à conservação de documentos.	Implementação de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.	Semelhança	Relaciona-se com implementação das boas práticas (normas *ISO*'s e normas arquivísticas) e o gerenciamento de riscos.

	Assistência e orientação para a definição e implementação das regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da LGPD.		
Assessoramento aos trabalhos de pesquisa científica ou técnico-administrativa.	Assistência e orientação na elaboração de instrumentos contratuais que disciplinam questões relacionadas ao tratamento de dados pessoais.	Convergência	Contribuições para elaboração de cláusulas para termos de privacidade e proteção de dados, para o correto tratamento de dados, informações e documentos.

Fonte: Elaboração própria.

Podemos também considerar a responsabilidade arquivística em relação à assistência e orientação para a elaboração políticas internas ou para a implementação de regras de boas práticas que asseguram o cumprimento da LGPD e de outros regulamentos da ANPD. Segundo Iacovino (2016, p. 289) ao arquivista são delegadas diversas responsabilidades que vão além de uma gestão de documentos de qualidade, mas também a orientação por meio de normas de boas práticas. Na visão da autora, há um consenso de que o arquivista deve se posicionar mesmo que estas estejam além de suas responsabilidades perante ao empregador. Além disso, Hurley (2005, p. 237-242, *apud* Iacovino, 2016, p. 288) define as responsabilidades do arquivista, algumas não executadas simultaneamente, como:

> 1. Estabelecer instruções específicas; 2. Definir normas; 3. Facilitar a implementação de requisitos; 4. Oferecer serviços profissionais; 5. Criar condições para as obrigações relacionadas ao processamento arquivístico; 6. Monitorar processamento; 7. Tomar medidas regulatórias no caso de desvios de conduta; 8. Garantir obediência às normas; 9. Fiscalizar o uso de avaliações de performance (Iacovino, 2016. p. 289).

A responsabilidade arquivística também pode ser interpretada sob a perspectiva da gestão de riscos e da prestação de contas, na medida que o arquivista colabora para a implementação de medidas, sejam elas técnicas, administrativas ou de segurança, para a prevenção de acessos não autorizados, bem como de situações acidentais ou ilícita de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado das informações pessoais.

Silva (2017, p. 347) destaca que “não se pode jamais esquecer que o objetivo final dos arquivos e dos arquivistas é a promoção responsável de um acesso pleno e de qualidade aos documentos arquivísticos e suas informações”. Além disso, é relevante também considerar,

que “naturalmente, um volume considerável de informações recolhidas, produzidas e recebidas pelo poder público é registrado em documentos arquivísticos, independente do suporte” (Silva, 2017, p.13).

A respeito da responsabilidade e interesse do poder público para o acesso e a transparência dos documentos e informações, Silva (2017, p. 20) destaca que:

> Os órgãos públicos brasileiros, enquanto detentores de parte da soberania do Estado e executores de funções estatais, devem divulgar e promover o acesso de informações de interesse público e fomentar o desenvolvimento da cultura de transparência e do controle social da administração pública, mas também precisam proteger as informações consideradas sigilosas e pessoais com eficiência e eficácia (Silva, 2017).

No entanto, é fundamental refletir que parte dessas informações possuem um caráter pessoal, sendo necessário garantir que seu acesso não comprometa outros direitos assegurados por outros ordenamentos.

Nesta análise comparativa revelou-se ambas as funções possuem semelhanças e convergências importantes, especialmente no que tange ao planejamento, organização, orientação e direção dos serviços arquivísticos para a proteção de dados no que diz respeito às informações. Todavia, vale ressaltar que o Quadro 5 não é exaustivo, permitindo que outras análises possam ser feitas e que outras semelhanças e convergências possam ser identificadas ou visualizadas.

5 ANÁLISE E APRESENTAÇÃO DOS RESULTADOS

Nesta seção apresentaremos como foi delineada a coleta de dados, a seleção da população referente aos arquivistas, os recursos e ferramentas utilizadas para o alcance desses profissionais e a contextualização das perguntas para então proceder com a apresentação e análise dos resultados. Buscou-se que dessa forma a amostra fosse representativa, considerando os critérios e os eixos descritos na metodologia deste trabalho, que diz respeito à proteção e integridade dos conteúdos dos documentos, à responsabilidade arquivística, à gestão de riscos e à prestação de contas em relação à transparência.

5.1 Seleção da população e amostra

Considerou-se para esta pesquisa a população de arquivistas graduados, conforme a Lei 6.546/1978. Objetivando alcançar todos esses profissionais e amplificar essa pesquisa na comunidade arquivística, recorremos ao apoio às associações de profissionais arquivistas que abrangem 12 estados[42] pelo Brasil. Além disso, solicitamos o apoio para a divulgação do questionário, ao Fórum Nacional das Associações de Arquivologia do Brasil (FNArq), responsável pela aproximação entre as associações de arquivistas, existentes no Brasil, bem como o seu fortalecimento da classe ao nível nacional.

Adicionalmente, o questionário foi enviado para os colegiados das universidades federais e estaduais[43], para que estes fossem direcionados aos egressos do curso de Arquivologia, e ainda, aos pós-graduandos na área.

Além disso, o questionário foi divulgado em outras plataformas, como também o envio realizados de forma individual a profissionais arquivistas conhecidos no meio

---

[42] O questionário foi enviado as seguintes associações: Associação dos Arquivistas da Bahia (AABA), Associação de Arquivologia do Estado de Goiás (AAG), Associação de Arquivistas do Estado do Ceará (ARQUIVE-CE), Associação dos Arquivistas do Estado do Espírito Santo (AARQES), Associação de Arquivistas da Paraíba (AAPB), Associação dos Arquivistas do Estado do Rio Grande do Sul (AARS), Associação de Arquivistas de São Paulo (ARQ-SP), Associação dos Arquivistas do Estado do Rio de Janeiro (AAERJ), Associação de Arquivistas do Estado de Santa Catarina (AAESC), Associação Mineira de Arquivistas (AMArq), Associação dos Arquivistas do Estado do Pará (AAEPA), Associação Paranaense de Arquivistas (APA)

[43] Universidade Federal de Minas Gerais, Universidade Federal do Estado do Rio de Janeiro, Universidade Federal Fluminense, Universidade Federal de Santa Maria, Universidade de Brasília, Universidade Federal da Bahia, Universidade Estadual de Londrina, Universidade Federal do Espírito Santo, Universidade Federal do Rio Grande do Sul, Universidade Estadual Paulista, Universidade Estadual da Paraíba, Universidade Federal da Paraíba, Universidade Federal do Rio Grande, Universidade Federal de Santa Catarina, Universidade Federal do Amazonas, Universidade Federal do Pará.

acadêmico como já atuantes na área de privacidade e proteção de dados. Pelo *WhatsApp*[44] a abordagem ocorreu a partir de envios em grupos de profissionais atuantes na área de gestão de documentos, de ex-alunos do curso de Arquivologia UFMG e de grupos criados para os eventos nacionais da área, totalizando o alcance de 645 pessoas. No *Instagram* a publicação do questionário obteve o total de 2895 visualizações, a qual geraram paralelamente outros 28 compartilhamentos a partir dessa mesma publicação. E ainda, o questionário foi enviado pontualmente para outros 21 profissionais arquivistas que possuíam perfis no *LinkedIn,* os quais foram devidamente analisados e aqueles que se enquadraram nos critérios propostos, receberam o questionário. A procura pelos profissionais ocorreu a partir da busca pelos termos 'arquivista e data protection officer', 'arquivista e encarregado de dados'.

5.2 Análise da coleta e apresentação dos resultados

Durante o planejamento do questionário definiu-se que para a etapa inicial seria necessário realizar um filtro entre os profissionais arquivistas a fim de qualificá-los para o próximo estágio, utilizando a amostragem por etapas:

> Esse tipo de amostragem pode ser utilizado quando a população se compõe de unidades que podem ser distribuídas em diversos estágios. Torna-se muito útil quando se deseja pesquisar uma população cujos elementos se encontram dispersos numa grande área, como um estado ou um país (Gil, 2024, p. 105).

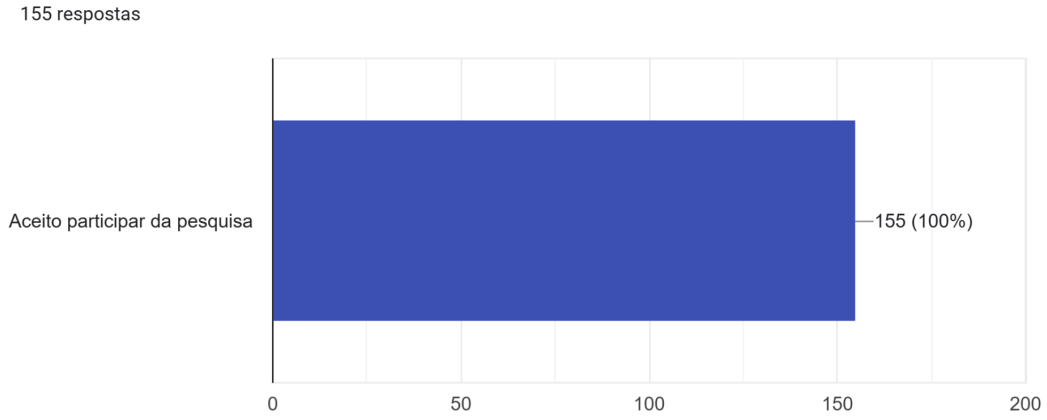
A aplicação do questionário ocorreu a todos os arquivistas que aceitaram participar de forma voluntária à pesquisa, observando os filtros para as perguntas iniciais, que tinha o objetivo principal de selecionar os profissionais que atuam ou atuaram na implementação da LGPD, a partir da sua data de vigência.

Importante ressaltar que, para observarmos a necessidade de incluir os profissionais que atuaram na área da proteção de dados, mas que não estavam em atividade no momento da aplicação do questionário. Diante disso, o recorte temporal foi ajustado abrangendo o período de entrada em vigor da LGPD. Assim, o foco não se restringiu apenas aos arquivistas envolvidos atualmente na implementação, mas contemplando todos os arquivistas que em algum momento estiveram envolvidos em comitês de governança em privacidade e proteção de dados ou na função de encarregado pelo tratamento de dados.

[44] Os grupos de WhatsApp foram: Gestão Documental na veia, Ex-alunos Arquivologia UFMG; Canal de Comunicação Associação Mineira de Arquivista (AMARQ); IX CNA que se referem ao Congresso Nacional de Arquivologia.

A divulgação do questionário foi iniciada no dia 17 de julho de 2024, com o término previsto e efetivado no dia 17 de agosto de 2024, com abrangência nacional. Dos envios realizados, foram efetivados a participação de 155 profissionais, conforme demonstrado abaixo no gráfico n.º 1

Gráfico 1- Aceite dos profissionais ao questionário

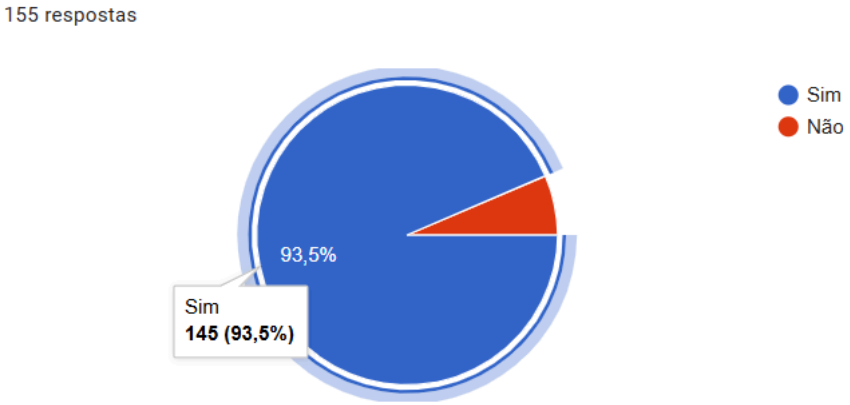


Fonte: Elaboração própria, 2024

A partir do aceite para participação e com base nas respostas afirmativas às **questões de n.º 1 e n.º 2**, conforme a proposta do questionário, os arquivistas voluntários prosseguiram respondendo às questões subsequentes, que compreendiam as perguntas de números 3 a 18.

A primeira pergunta teve como objetivo verificar se o profissional possuía formação superior no curso de Arquivologia, conforme disposto nos incisos I e II, do art. 1º da Lei 6.546/1978. Em resposta, 93,5% dos participantes, correspondendo a um total de 145 arquivistas, conforme se observa abaixo no gráfico n.º 2:

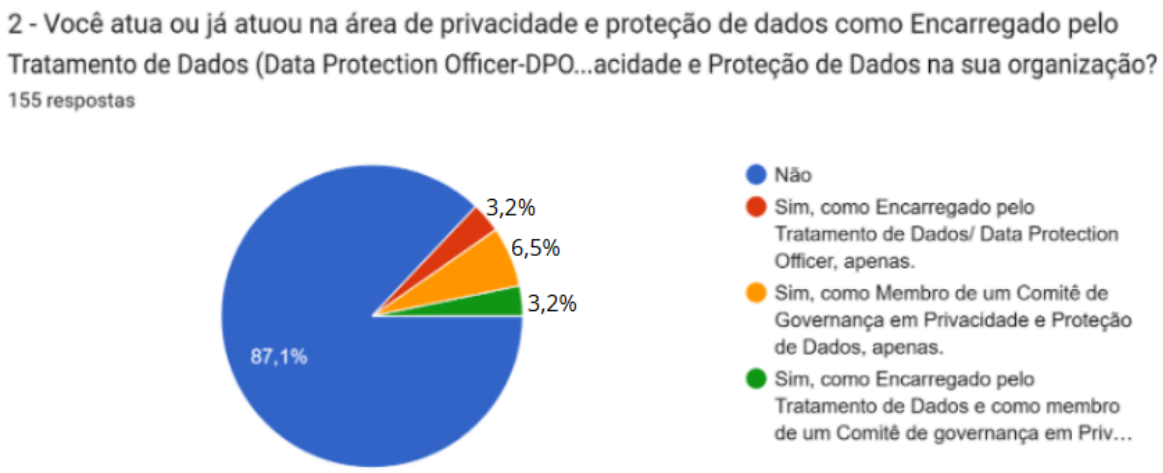
Gráfico 2 - Questão 01 do Questionário



Fonte: elaboração própria, 2024.

A **questão de n.º 2**, buscou-se identificar se os arquivistas atuam ou atuaram com a temática privacidade e proteção de dados, especificamente em relação às funções de Encarregado pelo Tratamento de Dados e/ou membro do comitê de governança em privacidade e proteção de dados, podendo ainda ter atuado nas duas funções em algum determinado momento. Os resultados indicaram que a maioria dos profissionais participantes da pesquisa, sendo um porcentual de 87,1%, (totalizando 135 indivíduos) não tiveram atuação direta na área de proteção de dados ou em funções correlatas. Em contrapartida, **20 arquivistas** relataram atuação na área, a saber: 5 profissionais (3,2% do total de respondentes e 25% dos arquivistas atuantes) desempenharam o papel de encarregado pelo tratamento de dados. Adicionalmente, 10 profissionais (6,5% do total de respondentes) integraram comitês de governança em privacidade e proteção de dados. Observou-se que 5 arquivistas (3,2% do total de respondentes) acumularam ambas as responsabilidades, atuando em algum momento nas duas funções, conforme ilustrado no gráfico a seguir.

Gráfico 3 - Questão 02 do Questionário

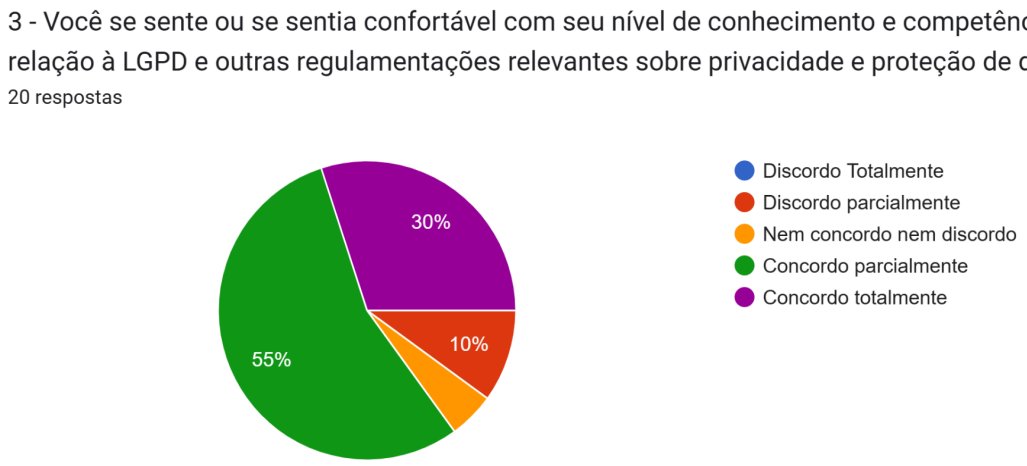


Fonte: elaboração própria, 2024.

O terceiro bloco de perguntas do questionário buscou compreender a atuação dos 20 arquivistas atuantes na área de proteção de dados, observando os quatro eixos principais: **a proteção de documentos arquivísticos** no desenvolvimento das rotinas e procedimentos que envolvem a produção, o uso e a destinação; a **responsabilidade no gerenciamento arquivístico,** que compreende o planejamento, organização, direção e o controle; **a gestão de riscos** que abrange a identificação, avaliação a fim de mitigá-los, controle e monitoramento de incidentes; e **a prestação de contas e a responsabilidade** no desenvolvimento de políticas de acesso e privacidade.

Nessa direção, passou-se para a **questão n.º 3** cujo objetivo era avaliar o grau de conforto dos arquivistas em relação ao seu conhecimento e competências sobre a Lei Geral de Proteção de Dados e outras normativas de privacidade e proteção de dados. A questão de n.º 3 revelou o seguinte panorama: uma parcela de 30% dos profissionais atuantes (6 arquivistas) demonstrou total confiança em sua capacidade de atuação nessa área. A maioria dos profissionais atuantes, representando 55% (11 arquivistas), expressou concordância parcial com a questão. Em contrapartida, 10% dos profissionais atuantes (2 arquivistas) discordaram parcialmente, enquanto um único profissional (5%) adotou uma postura neutra diante da questão, conforme o gráfico n.º 4.

Gráfico 4 - Questão 03 do Questionário



Fonte: elaboração própria, 2024.

A análise desse cenário revela-se um cenário favorável, visto que 85% dos profissionais atuantes (17 arquivistas) demonstraram, em alguma medida, segurança para a atuação em relação aos regulamentos de proteção de dados. Este resultado sugere um empenho desses profissionais na busca contínua por atualização e aprimoramento de seus conhecimentos. Como analisada na seção 4 desta dissertação sobre as competências e responsabilidades do arquivista, percebe-se a atualidade das reflexões de Bellotto (2004, p. 263), sobretudo a necessária a adaptação do profissional à realidade e as às condições de seu tempo e lugar.

Em prosseguimento, a **questão de n.º 4** buscou investigar se a experiência profissional dos arquivistas poderia influenciar seu desempenho e capacitação para os desafios decorrentes da Lei Geral de Proteção de Dados. Tendo em vista que a atuação se baseia na procedimentação e a aplicação da lei, tem em seus fundamentos as bases jurídicas, necessitando que os profissionais tenham alguma compreensão na área. Ademais, convém destacar que a construção do regulamento levou em conta os debates e discussões acerca das práticas informacionais justas e também os aspectos das boas práticas internacionais. Por conseguinte, também considerou as preocupações ao desenvolvimento da livre formação da personalidade do indivíduo e outros direitos fundamentais, cujos quais compreende as garantias expressas na Constituição Federal de 1988.

A respeito da capacidade do arquivista, cabe salientar, conforme analisado na seção 4 desta dissertação, sobre a propriedade desse profissional de realizar análise e síntese, juntamente com uma aptidão para situações complexas, para a emissão de julgamentos seguros. Além disso, Bellotto (2006, p. 301) salientou outras qualidades que se espera desse

profissional, como a habilidade de formular claramente suas ideias, tanto na forma escrita quanto na verbal; aptidão para tomar decisões sobre questões ligadas à memória da sociedade; abertura às novas tecnologias; bom senso para tomar resoluções; adaptação à realidade e as condições. Adicionalmente, a autora também destacou Bellotto (2006, p. 301) qualidades de "adaptabilidade, pragmatismo, curiosidade intelectual, rigor, método, continuidade, capacidade de compreensão e escuta relativamente ao produtor, ao pesquisador e ao cidadão". A vivência profissional exige que o arquivista o desafio o esforço de "comunicação, de aperfeiçoamento, de reciclagem, paralelamente ao entendimento da evolução das práticas profissionais, das técnicas que não cessam de se renovar, dos conhecimentos" (Bellotto, 2006, p. 301).

Os resultados para a questão n.º 4 indicaram que 40% dos arquivistas (8 profissionais) concordam totalmente que sua experiência profissional contribuiu significativamente para lidar com os desafios na área de proteção de dados. Uma parcela de 50% (10 arquivistas) concorda parcialmente com essa afirmação, enquanto os restantes 10% (2 arquivistas) discordam parcialmente quanto à influência da experiência profissional no enfrentamento desses desafios, conforme o apresentado no gráfico n.º 5.

Gráfico 5 - Questão 04 do Questionário

Fonte: elaboração própria, 2024.

Diante disso, observa-se que 90% dos atuantes (18 arquivistas, somando quais concordaram total e parcialmente) reconhecem em maior ou menor grau que a vivência e experiência é um fator relevante para enfrentar os desafios advindos da Lei Geral de Proteção

de Dados. Isso sugere que o conhecimento adquirido ao longo da carreira em Arquivologia forneceu bases para lidar com as demandas próprias da área.

Além disso, ao avaliar os profissionais que concordaram parcialmente (50%, total de 10 arquivistas atuantes), pode-se inferir que, embora a experiência seja útil, outros fatores, como a formação específica na área de proteção de dados, as atualizações constantes sobre as legislações, além do apoio institucional, são fundamentais para o bom desempenho da função. Ao passo que, conforme destacado por Bellotto (2006, p. 304), o arquivista avança vertical e horizontalmente, ou seja, "atinge níveis mais altos de especialização e conhecimento na arquivística, quando se expande para as áreas vizinhas".

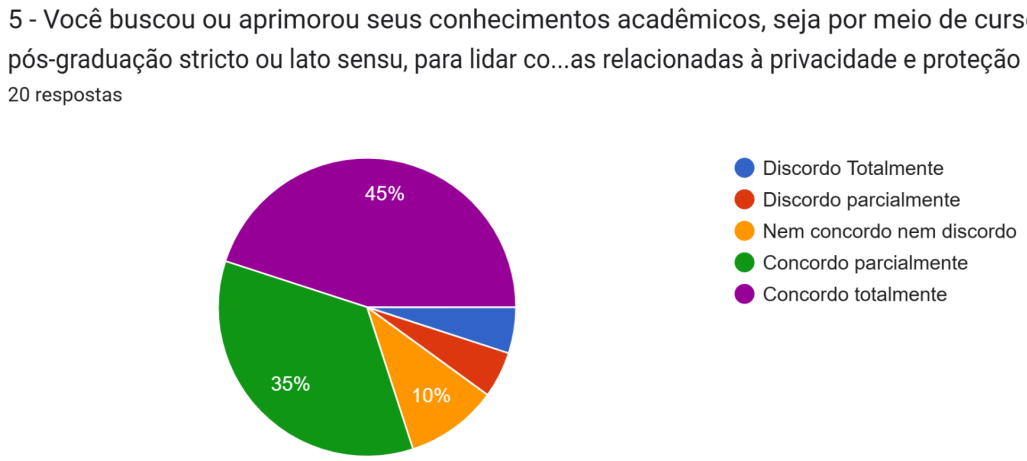
Em relação aos resultados da minoria de 10% (2 arquivistas atuantes) que discordam parcialmente, infere-se que esses profissionais podem ter vivenciado situações em que a experiência tradicional não tenha se mostrado aplicável frente aos desafios impostos pela LGPD. Por exemplo, podemos considerar nos aspectos que necessitam de diálogo e interações mais aprofundadas em áreas de tecnologia ou jurídicas, inclusive a própria cultura da organização, pode se tornar um dificultador. Além disso, podemos inferir a partir desses resultados que, mesmo com experiência profissional, pode haver a necessidade de formação complementar ou atualizações contínuas.

Em resumo, observa-se que a experiência profissional é considerada valiosa para a atuação da proteção de dados, mas enfatizam-se as inferências quanto à combinação de experiências e à busca pelo aprendizado contínuo.

A **questão de n.º 5**, buscou-se compreender, para além das experiências práticas nas organizações, se os arquivistas buscaram aprimorar seus conhecimentos acadêmicos por meio de cursos de pós-graduação (stricto ou lato sensu e) para responder às demandas de privacidade e proteção de dados. O objetivo era verificar a proatividade dos profissionais em adquirir qualificações – entendidas como a capacidade de propor iniciativas e dominar novas situações no trabalho – e em desenvolver novas competências, tanto humana quanto profissionais, que o ambiente acadêmico pode proporcionar, mesmo em períodos de curta duração. Os resultados revelaram que uma parcela significativa dos arquivistas demonstrou proatividade na busca por aprimoramento profissional: 45% (9 arquivistas) concordam totalmente que investiram em cursos de pós-graduação para aprofundar seus conhecimentos. Outros 35% (7 arquivistas) concordam parcialmente com essa questão. Em contrapartida, uma pequena parcela de 5% (1 arquivista) discordou parcialmente e outros 5% (1 arquivista) discordaram totalmente a respeito da busca pelo aprimoramento em pós-graduação para lidar

com as demandas de proteção de dados. Adicionalmente, 10% dos entrevistados (2 arquivistas) adotaram uma postura neutra em relação à questão, conforme revela o gráfico n.º 6 a seguir:

Gráfico 6 - Questão 05 do Questionário



Fonte: elaboração própria, 2024.

Compreende-se, a partir do desenvolvimento desta pesquisa, que competências resultam da combinação de conhecimentos, habilidades e atitudes, manifestadas no desempenho profissional em um contexto organizacional específico.

A **questão de n.º 6**, teve como objetivo avaliar o grau de concordância dos arquivistas participantes sobre a responsabilidade arquivística e a sua relevância para a governança arquivística da organização. Para melhor compreensão, resgatamos o conceito de governança arquivística, cujas funções básicas abrangem as ações de avaliação, a direção e o monitoramento do gerenciamento arquivístico. Implica na interação e o diálogo com outras áreas, processos, produtos, com os atores e as partes interessadas (interna e externa) que, embora nem sempre estão diretamente ligadas a arquivísticas, suas ações interferem direta ou indiretamente.

Adicionalmente, é importante reconhecer que a governança arquivística ultrapassa as paredes da organização, interagindo com as áreas do governo e da sociedade, e se alinha às normas e regulamentos do ordenamento jurídico brasileiros. Como mecanismo da governança, a responsabilidade (arquivística) pode manifestar sua abordagem de diferentes, a depender de cada país, no entanto, é possível concordar que não pode ser tratada por apenas

por meio de legislação. De acordo com as análises de Iacovino (2016, p. 261), “a profissão do arquivista é mecanismo essencial para a responsabilidade pública”, pois é por meio dos arquivos que se torna possível detectar ações ilícitas e desvios éticos.

Os resultados evidenciaram um consenso entre os participantes: a responsabilidade arquivística transcende a mera gestão documental. Especificamente, 90% dos arquivistas (18 profissionais) concordaram totalmente com essa afirmação, enquanto os 10% restantes (2 profissionais) demonstraram concordância parcial, conforme demonstrado no gráfico de n.º 7:

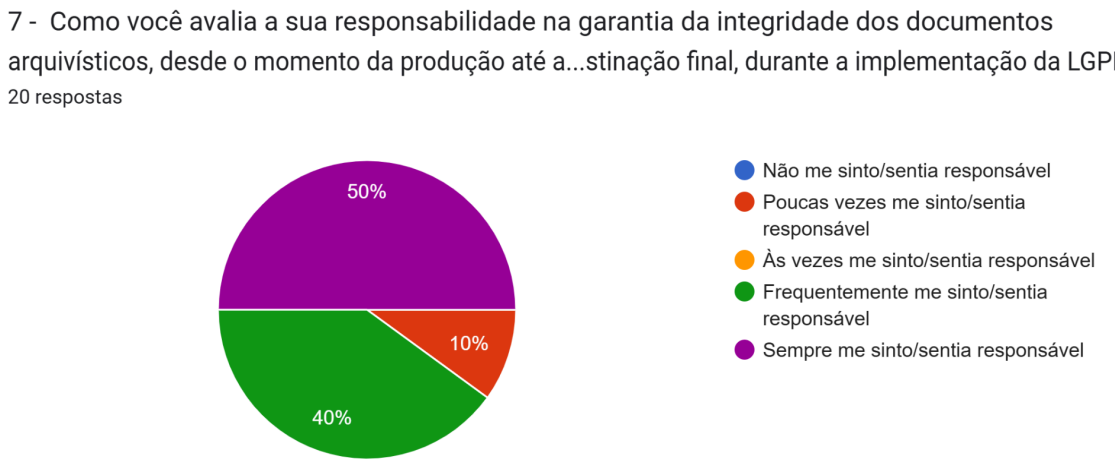
Gráfico 7 - Questão 06 do Questionário

Fonte: elaboração própria, 2024.

A **questão de n.º 7**, pretendia compreender como o arquivista avaliava sua responsabilidade a respeito de sua atuação para a garantia da integridade dos documentos arquivísticos, considerando o fluxo desde a produção até a destinação final, em favor da adequação da Lei Geral de Proteção de Dados e a implementação nos programas de governança em privacidade e proteção de dados. Como explicação sobre o conceito de “integridade” utilizou-se do Glossário de Documentos Arquivísticos Digitais (Conarq, 2016, p. 29) que descreveu como o “estado dos documentos que se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada”. O glossário também tratou de definir a “integridade arquivística” que decorre do princípio da proveniência. Além disso, a partir desta pesquisa buscou dissertar a respeito da contribuição da área da segurança da informação, que tem a integridade como um dos pilares, e caracteriza-se como propriedade de precisão e completeza.

Os resultados evidenciaram novamente forte senso de responsabilidade entre os profissionais: 90% de respostas foram positivas, com 50% (10 arquivistas) afirmando sentir-se sempre responsáveis pela integralidade dos documentos arquivísticos, e outros 40% (8 arquivistas) indicando que frequentemente se sentem responsáveis pela integridade dos documentos arquivísticos. Em contraste, apenas 10% (2 arquivistas) afirmaram poucas vezes que se sentiam responsáveis pela integridade dos documentos arquivísticos, conforme demonstrado no gráfico de n.º 8:

Gráfico 8 - Questão 07 do Questionário



Fonte: elaboração própria, 2024.

Merece destaque a diferença de percepção nos resultados entre a questão anterior (n.º 6), que investigou o nível de concordância, em relação à questão n.º 7. Observou-se que, enquanto houve consenso entre os profissionais quanto à responsabilidade arquivística englobar o gerenciamento e a governança, a avaliação sobre como eles percebiam seu próprio envolvimento na responsabilidade pelo processamento arquivístico revelou nuances menos positivas.

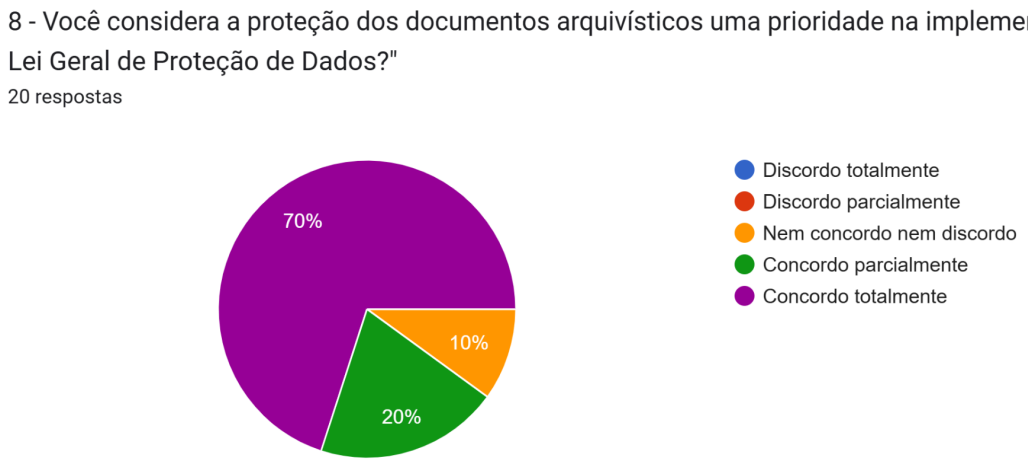
A **questão de n.º 8**, buscou compreender como o arquivista considera a proteção dos documentos arquivísticos como uma prioridade na implementação LGPD em programa de privacidade e proteção de dados. Nesse sentido, destaca que os documentos arquivísticos (um ativo de informação), "[...] são testemunhos inequívocos da vida das instituições. Estão registrados nos arquivos as informações sobre o estabelecimento, a competência, as atribuições, as funções, as operações e as atuações levadas a efeito, por uma entidade" (Bellotto, 2022, p. 306). Outro ponto importante a considerar sobre os documentos

arquivísticos é a sua interligação com a sociedade, a qual passa também pela relação arquivos e governo, arquivos e cidadania, seja por meio de atos dispositivos que orientam, sejam os documentos comprobatórios que servem como prova, seja os registros informativos que podem ser utilizados para acionar ou movimentar (Bellotto, 2022, p. 306).

Considerado por Bellotto como a rede das relações entre o Estado e o cidadão, sejam essas relações de ordem administrativa, jurídica, política, social e econômica (Bellotto, 2022, p. 307-310). Em vista disso, a priorização da proteção dos documentos arquivísticos encontra respaldo também nas análises de Schellenberg (2006, p. 30) que elencou as razões para a instituição de arquivos, destacando como uma prática necessária para aumentar a eficiência governamental, configurando como sendo a principal fonte de informação nesse cenário. Ademais, Schellenberg salientou que os documentos integram instrumentos administrativos fundamentais para a execução dos trabalhos. Eles servem como provas de operações financeiras, legais, demandando, portanto, proteção. Segundo o autor, os documentos arquivísticos "englobam o grande capital da experiência oficial de que o governo necessita para dar continuidade e consistência às suas ações, tomar determinações, tratar de problemas sociais e econômicos, bem como de problemas de organização e métodos" (Schellenberg 2006, p. 33).

A partir disso, a análise dos resultados da questão de n.º 8, revelou um cenário positivo: 70% (14 arquivistas) demonstraram total concordância quanto à prioridade dos documentos arquivísticos na implementação da LGPD. Outros 20% (4 arquivistas) aderiram parcialmente a essa visão, enquanto uma pequena parcela de 10% (2 arquivistas) manteve uma postura neutra em relação à questão, logo, dentro da população selecionada nenhum dos participantes discordou da prioridade na proteção de documentos arquivísticos.

Gráfico 9 - Questão 08 do Questionário



Fonte: elaboração própria, 2024.

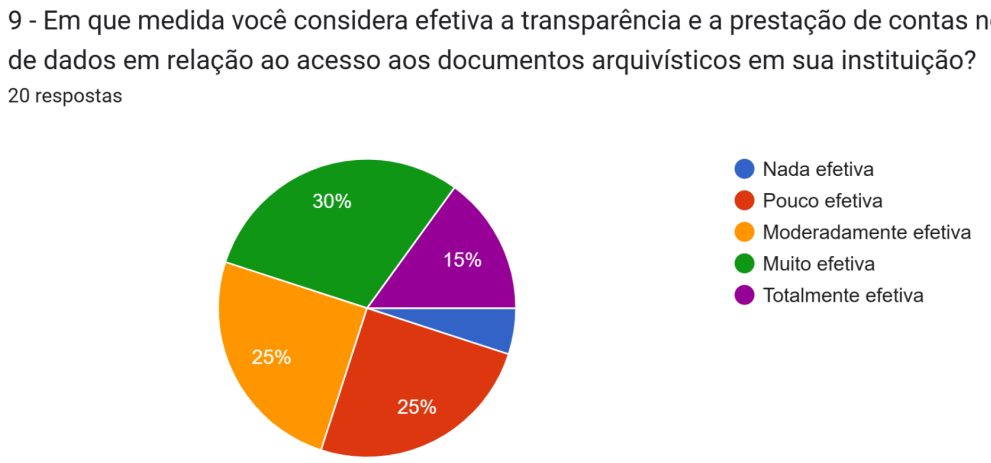
A partir desse resultado, observa que um grupo atuante que corresponde a 30% (6 arquivistas) considera a prioridade parcialmente ou se manteve numa posição neutra. Diante dessa constatação, podemos inferir que esses profissionais priorizam outros aspectos da implementação da LGPD? Ou ainda, esses dados podem indicar que, apesar de reconhecerem a importância dos documentos arquivísticos, esses profissionais enfrentam desafios ou prioridades concorrentes na implementação da LGPD?

A **questão de n.º 9**, buscou analisar em que medida os participantes consideram efetiva a transparência e a prestação de contas no tratamento de dados em relação aos acessos aos documentos arquivísticos nas instituições em que esses profissionais atuavam. Como contextualização abordamos na seção 5 desta pesquisa (5.1.2) a conceituação dos princípios de transparência e prestação de contas, observando suas práticas para contribuição ao acesso às informações a partir das operações, estruturas, processos decisórios e seus resultados, numa concepção de transparência ativa, em que executa as ações de forma oportuna e proativa se a necessidade de solicitação da sociedade.

Em consonância com os princípios da transparência e da prestação de contas para o acesso à informação e divulgação, a Lei de Acesso à Informação atribui aos órgãos e entidades públicas a responsabilidade pela aplicação dos procedimentos estabelecidos. Isso implica o dever de garantir a gestão transparente da informação, possibilitando o amplo acesso e a prestação de contas sobre seu uso; a proteção dos documentos e seu conteúdo, assegurando a segurança da informação (disponibilidade, autenticidade e integridade) e a proteção às informações de caráter pessoal, observando as restrições legais de acesso.

A análise dos resultados revelou uma distribuição nas percepções dos arquivistas quanto à efetividade dos princípios de transparência e prestação de contas no acesso aos documentos arquivísticos em suas instituições. Uma parcela de 15% (3 arquivistas) a considerou totalmente efetiva, e 30% (6 arquivistas) a avaliaram como muito efetiva. Em contrapartida, opiniões mais moderadas foram expressas por 25% (5 arquivistas), que a julgaram moderadamente efetiva, enquanto outros 25% (5 arquivistas) apontaram para uma baixa efetividade da transparência e da prestação de contas, conforme evidenciado no gráfico de n.º 10:

Gráfico 10 - Questão 09 do Questionário



Fonte: elaboração própria, 2024.

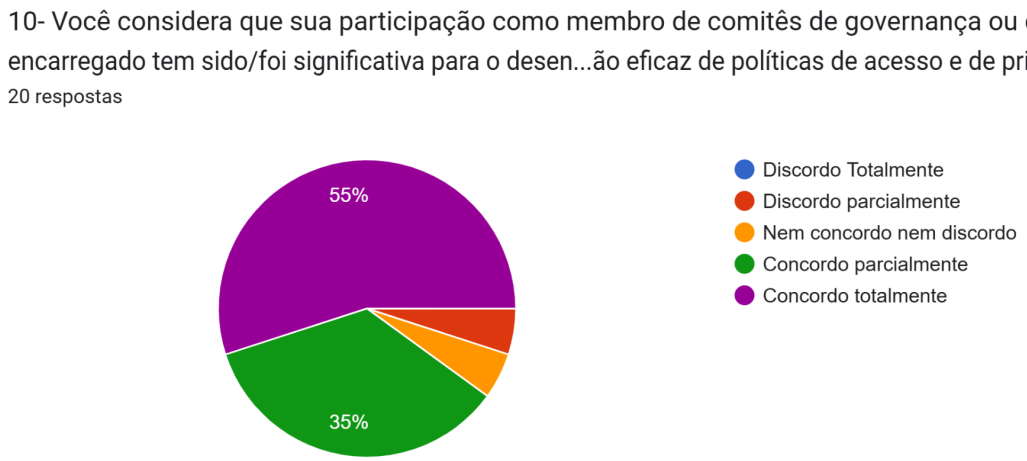
A **questão n.º 10**, objetiva a compreensão em como os arquivistas participantes da pesquisa consideravam suas atuações como membros de comitês de governança em privacidade e proteção de dados ou encarregados pelo tratamento de dados, nas instituições em que trabalhavam. O objetivo principal da pergunta era entender se essa atuação foi significativa no desenvolvimento e implementação de procedimentos que visavam equilibrar o direito ao acesso e o direito à privacidade.

A seção 4 desta dissertação, a fim de exemplificar a atuação, propôs-se a avaliar as competências dos arquivistas no âmbito da proteção de dados, cuja qual aprofundou a compreensão dessas competências a partir de seus regulamentos específicos. A partir disso, constatou-se uma proximidade no desempenho do arquivista em relação à função de encarregado pelo tratamento de dados, notadamente em: semelhança e convergência com o acesso à informação e à transparência, atendendo aos direitos do titular/cidadão; convergência das funções com práticas de gerenciamento arquivístico e governança organizacional;

convergência com os princípios da prestação de contas e *accountability*; e as semelhanças das funções para a implementação de boas práticas (normas *ISO's* e normas arquivísticas) para o gerenciamento de riscos.

Os resultados mostraram que a maioria dos participantes considerou eficaz sua atuação como membros de comitês ou encarregados no desenvolvimento de ações para programas de privacidade e proteção de dados. Especificamente, 55% (11 arquivistas) concordaram totalmente, e outros 35% (7 arquivistas) concordaram parcialmente. Uma pequena parcela de 5% (1 arquivista) se manteve neutra, enquanto outros 5% (1 arquivista) discordaram parcialmente em relação ao desenvolvimento e à implementação eficaz de políticas de acesso e privacidade.

Gráfico 11 - Questão 10 do Questionário



Fonte: elaboração própria, 2024.

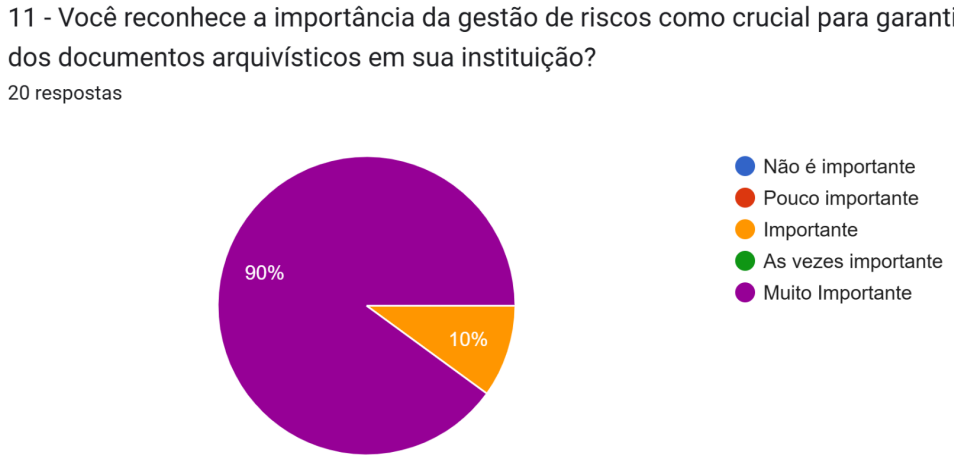
O que podemos inferir é que a grande maioria dos arquivistas participantes da pesquisa (18 arquivistas) percebe que a sua participação em comitês de governança ou como encarregados pelo tratamento de dados como eficaz no desenvolvimento de ações para programas de privacidade e proteção de dados e reconhecem o impacto das suas habilidades e competência no desempenho dessas funções.

A **questão de n.º 11** teve como objetivo compreender se os profissionais arquivistas reconheciam a importância da gestão de riscos como mecanismo de monitoramento e controle para a garantia dos documentos arquivísticos nas organizações em que atuavam. Aqui, é importante destacar que a LGPD tem na sua essência a mitigação de riscos, a qual avalia a proporcionalidade e o balanceamento da legitimidade do uso de determinados dados ou

registros. Outra ação que configura o gerenciamento de risco é a elaboração de relatórios de impacto à proteção de dados pessoais, que visam o registro da identificação e avaliação dos riscos, bem como as medidas para mitigá-los. A lei dispõe ainda de um capítulo para tratar da segurança e de regras de boas práticas e destaca que o "controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular" (Brasil, 2018).

O resultado demonstrou um reconhecimento unânime da importância da gestão de riscos para a segurança dos documentos arquivísticos entre os profissionais da área (100%). A maioria expressiva, correspondente a 90% (18 arquivistas), avaliou essa importância como muito alta, enquanto os restantes 10% (2 arquivistas) a consideraram importante, conforme ilustrado no gráfico abaixo.

Gráfico 12 - Questão 11 do Questionário



Fonte: elaboração própria, 2024.

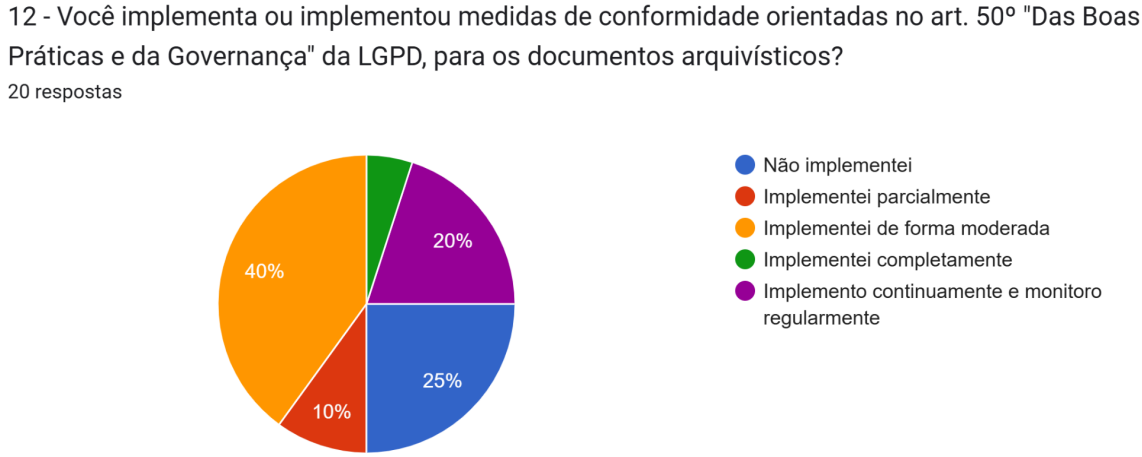
Podemos inferir, a partir do resultado da questão n.º 11, que os arquivistas percebem a segurança dos documentos não apenas como uma tarefa operacional, mas sim como uma questão estratégica que requer uma abordagem proativa a favor do gerenciamento de riscos. A alta porcentagem dos que consideram a gestão de riscos "muito importante" na implementação de programa de governança em privacidade reforça essa percepção.

A **questão n.º 12** teve uma abordagem complementar à pergunta anterior e buscou verificar se os profissionais tiveram a oportunidade de implementar alguma medida de conformidade com a Lei Geral de Proteção de Dados (LGPD), orientada pelo art. 50, que dispõe da aplicação de "boas práticas". Essas práticas incluem normas de segurança, padrões

técnicos, ações de conscientização e treinamentos (educativas), além de mecanismos internos de supervisão e mitigação de riscos, que também demonstram adesão às boas práticas. Em contraste com a questão anterior, que focava no reconhecimento da importância e teve um retorno positivo em sua totalidade, esta revelou diferentes níveis de implementação das boas práticas por parte dos arquivistas, o que de certa forma nos permite inferir que a implementação de medidas organizacionais, técnicas ou de segurança, não depende necessariamente de uma única área.

Nesse sentido, observou-se que 20% (4 arquivistas) implementam e monitoram continuamente as boas práticas, um percentual maior de 40% (8 arquivistas) realizou uma implementação moderada, 10% (2 arquivistas) implementaram apenas parcialmente, uma pequena parcela de 5% (1 arquivista) implementou completamente, e 25% dos participantes (5 arquivistas) não implementou medidas de conformidade, conforme mostra o gráfico abaixo:

Gráfico 13 - Questão 12 do Questionário



Fonte: elaboração própria, 2024.

Na **questão de n.º 13**, foi planejada de forma aberta e não obrigatória, cuja qual buscamos coletar exemplos práticos dos participantes sobre a implementação de medidas de boas práticas e governança em seus trabalhos com programas de privacidade e proteção de dados. Recebemos retornos, alguns bem detalhados, de 14 participantes, com uma variedade de implementações relatadas. Para facilitar a visualização, construímos um quadro que apresenta os temas centrais de cada resposta, a frequência de citações por tema. Desse modo, a partir dos levantamentos dos temas, foi possível relacioná-los com boas práticas dos guias

de implementação e *frameworks* como as normas *ISO's 27701* (extensão da ISO 27001 e controles 27002) que fornece diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Informação de Privacidade. O quadro n.º 6 detalha essas contribuições a seguir:

Quadro 6 - Exemplos de implementação de boas práticas - questão n.º 13

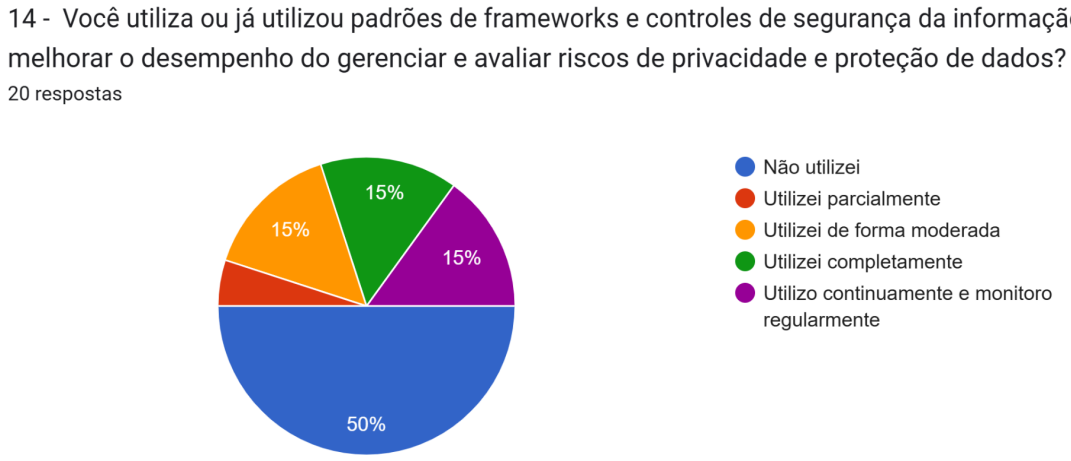
Implementação de Boas Práticas	**n.º de citações**	**Possível Referência**
Desenvolvimento de normas, políticas, padrões técnicos para produção de documentos e outros regulamentos	7	Conformidade com políticas, regras e normas para a segurança das informações (5.36 - *ISO* 27002);
Mecanismos de controle de acesso (Privilégios de acesso; restrições de acesso)	6	Segregação de funções (5.3, ISO 27002); Classificação das informações (5.12. *ISO 27002*); Controle de Acesso (5.15 - *ISO 27002*); Restrição de Acesso (8.3 - *ISO 27002*;
Conscientização e treinamentos sobre cultura de privacidade	5	Conscientização, educação e treinamento em segurança da informação (6.3 - *ISO* 27002);
Mapeamento de dados e fluxo das informações (manutenção de registros de operações de tratamento)	1	Documentação dos procedimentos de operações (5.37 - *ISO* 27002);
Implementação de gestão de documentos	1	Documentação dos procedimentos de operações (5.37 - *ISO 27002*); Controle tecnológicos - Restrição de acesso (8.1 - *ISO 27002*); Prevenção de vazamento de dados (8.12- *ISO 27002*); Coleta de evidência (5.28 - *ISO 27002*); Proteção de registros (5.33 - *ISO 27002*)
Implementar sistemas de informação (Tecnologia)	3	Controle tecnológicos (8; 8.1; - *ISO 27002*); Gestão de vulnerabilidades técnicas (8.8 - *ISO 27002*); Prevenção de vazamento de dados (8.12- *ISO 27002*); *Privacy by design e Privacy by Default* (B.8.4 - *ISO* 27701);
Direito dos titulares (acesso à informação)	1	A.7.3.2 Determinando as informações para os titulares de Dados Pessoais (*ISO 27701*); A.7.3.3 Fornecendo informações aos titulares de Dados Pessoais (*ISO 27701*); A.7.3.1 Determinando e cumprindo as obrigações para os titulares de DP (*ISO 27701*); A.7.3.6 Acesso, correção e/ou exclusão (*ISO 27701*).
Auditorias internas	1	Segurança de serviços em redes (8.22 - *ISO 27002*); Atividade de monitoramento (8.16 -

		ISO 27002); Auditoria Interna (9.2.2 - *ISO 27001*).

Fonte: elaboração própria, com base nas respostas dos arquivistas ao questionário, 2024

A **questão de n.º 14**, teve o propósito de compreender se os participantes haviam utilizado *frameworks* de privacidade e segurança da informação que visam a melhoria do desempenho e o gerenciamento dos riscos de privacidade nos programas de privacidade e proteção de dados em que atuavam. Considera-se aqui o termo como uma estrutura sólida, que fornece a base para construir um software ou sistema, a partir de um conjunto de ferramentas e diretrizes que facilitam o desenvolvimento (um modelo pronto). Os resultados indicam que uma parcela significativa de 50% (10 arquivistas atuantes na área de proteção de dados) não implementou *frameworks* de privacidade e segurança da informação em suas funções relacionadas à governança de privacidade e proteção de dados. Por outro lado, 15% (3 arquivistas atuantes) os empregaram ativamente na adequação, manutenção e monitoramento de riscos do programa. Observou-se também que 15% (3 arquivistas atuantes) fizeram uso moderado, e outros 15% (3 arquivistas atuantes) utilizaram parcialmente esses controles. Uma minoria de 5% (1 arquivista atuante) afirmou não ter utilizado *frameworks* para a implementação dos programas, conforme ilustrado a seguir:

Gráfico 14 - Questão 14 do Questionário



Fonte: elaboração própria, 2024.

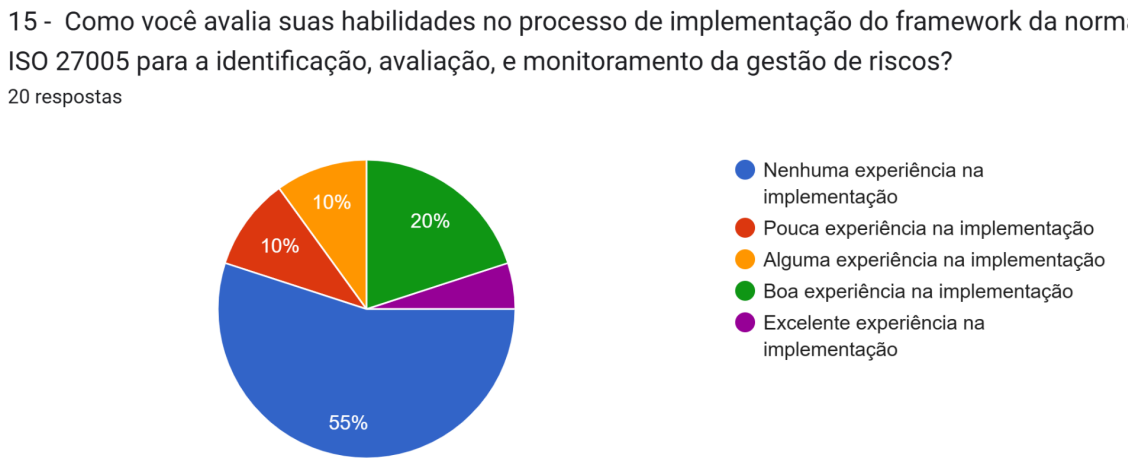
A partir dos resultados desta questão, observou-se que, embora os profissionais utilizem em seu cotidiano os controles para a mitigação de riscos à privacidade e à proteção de dados, nem todos têm ciência da sua participação para o uso e a aplicabilidade. Essa

constatação se alinha às respostas da questão anterior (n.º 12), tendo em vista que obtivemos um total de 14 arquivistas atuantes na área de proteção de dados (70% dos arquivistas atuantes) responderam que fazem uso da aplicação de boas práticas tanto em Arquivos (setores e documentos) quanto no ambiente organizacional.

A **questão de n.º 15**, se propôs a avaliar as habilidades dos participantes nos processos em que houveram implementação da Norma *ISO 27005*. Considerando a identificação, avaliação e monitoramento no gerenciamento de riscos. Essa norma faz parte da família ISO 27000, sendo a ABNT, é o órgão responsável pela tradução no Brasil. Importante também contextualizar que os documentos técnicos, assim como as Normas Internacionais (ISO e IEC), são voluntários e não incluem requisitos contratuais, legais ou estatutários [...] os documentos não substituem leis, decretos ou regulamentos, aos quais os usuários devem atender, tendo precedência sobre qualquer documento técnico ABNT (2023). A norma *ISO 27005,* especificamente, fornece orientações acerca das atividades de gestão de riscos de segurança da informação, em relação à avaliação e seu tratamento de riscos. Essas informações foram apresentadas após a pergunta, como contexto a que se refere a norma 27005.

A partir desse contexto, passamos para a análise da questão, na qual obtivemos o resultado de que 55% (11 arquivistas atuantes) informaram não ter nenhuma experiência e habilidade com a utilização da norma. Enquanto 20% (4 arquivistas atuantes) apresentaram boa experiência e habilidade na aplicação da norma de gestão de riscos. Outros 10% (2 profissionais) apresentaram certa experiência, e outros 10% (2 arquivistas atuantes) responderam ter pouca experiência na implementação, conforme podemos observar no gráfico abaixo:

Gráfico 15 - Questão 15 do questionário



Fonte: elaboração própria, 2024

Em observação, a maioria significativa dos arquivistas (55%, 11 arquivistas atuantes) que não possui experiência ou habilidade com a norma de gestão de riscos. Indica-se uma demanda por treinamento e desenvolvimento sobre o tema, considerando que o arquivista pode atuar na promoção de medidas necessárias ao gerenciamento e à governança arquivísticos, e ainda na elaboração de pareceres e trabalhos de complexidade sobre assuntos arquivísticos. Além disso, o arquivista também deve fazer uso de outros *frameworks* que visam oferecer segurança e controle dos documentos arquivísticos. A título de exemplo podemos citar o e-ARQ Brasil, que estabelece requisitos mínimos para o desenvolvimento de Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), independentemente da plataforma tecnológica em que for desenvolvido e/ou implantado.

A **questão de n.º 16**, optou-se novamente por deixá-la em aberto e de forma não obrigatória, para que os participantes pudessem compartilhar como exemplos as medidas implementadas ou que contribuíram para a implementação em ações relacionadas ao direcionamento, avaliação e o monitoramento na gestão de riscos. Tivemos o retorno de 10 participantes, que destacaram suas contribuições em ações como: implantação de controle de acesso por meio de biometria facial (dados biométricos); mapeamento de fluxos de processos; procedimentos para o controle de acesso; avaliação de riscos utilizando a metodologia *Matriz*

Swot[45] e o método *5W2H*[46]; elaboração de "Relatório de Impacto de Proteção de Dados (RIPD)"; gestão de riscos; monitoramento da implementação das políticas de proteção de dados; conscientização e treinamentos sobre risco no tratamento dos dados e documentos; auditorias internas para avaliar as informações e o monitoramento do setor; criação de normas, políticas e padrões para atendimento da LGPD.

Com base nos exemplos citados pelos arquivistas participantes da pesquisa, o quadro a seguir apresenta uma análise da aplicação das medidas para o gerenciamento de riscos nas organizações.

Quadro 7 - Exemplos de implementação na gestão de riscos - Questão n.º 16 do questionário

Práticas citados por arquivistas	**Análise da abordagem**
Implementação de controles de acesso (biometria, procedimentos)	Controle de segurança física para restringir acesso a informações e áreas sensíveis como medida preventiva de riscos.
Mapeamento de fluxos de processos	Foco na manutenção dos registros das atividades organizacionais, essencial avaliar a maturidade, identificar potenciais vulnerabilidades
Utilização de metodologias de análise de riscos (SWOT, 5W2H)	Adoção metodologias estruturadas para identificação, análise e priorização de riscos, buscando uma abordagem mais sistemática na gestão.
Elaboração relatórios e políticas (RIPD, normas, manuais)	Conformidade com a LGPD, demonstrando ações relacionadas aos princípios de governança
Monitoramento e avaliação (auditorias, análises contínuas)	Implementação de gestão de riscos, com acompanhamento e avaliação da efetividade das medidas implementadas.
Padronização da Gestão de riscos	Padronização de procedimentos para identificação e tratamento de riscos, por meio de metodologias de análise.
Implementação de Cultura de Privacidade Proteção de Dados	Conscientização e treinamento dos colaboradores de várias áreas e níveis, como medida de prevenção e mitigação de riscos, buscando construir uma cultura de segurança.

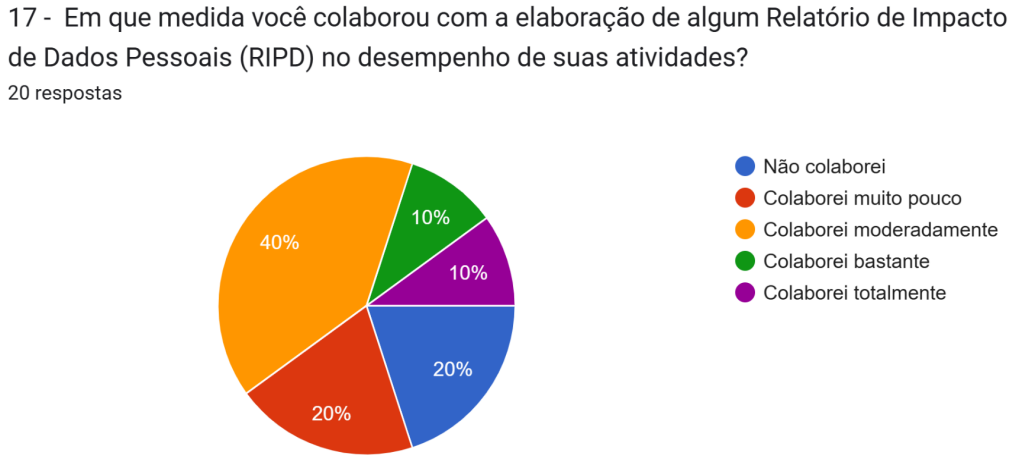
Fonte: elaboração própria

A **questão de n.º 17**, buscou compreender em que medidas os arquivistas participantes colaboraram para a elaboração de relatórios de impacto à proteção de dados. Como abordado

[45] *Matriz Swot* é um acrônimo formado pelas palavras inglesas: *Strengths (forças), Weaknesses (fraquezas), Opportunities (oportunidades) e Threats (ameaças)*.
[46] Método *5w2H*: *"What" (O quê?), "Why" (Por que?), "Who" (Quem?), "Where" (Onde?), "When" (Quando?), "How" (Como?) e "How Much" (Quanto?).*

anteriormente, esse relatório representa um documento obrigatório que mantém a descrição dos processos de tratamento de dados pessoais e que podem gerar riscos às liberdades civis e aos direitos fundamentais dos indivíduos. Ele deve apresentar medidas, salvaguardas e mecanismos para a mitigação de riscos, ou seja, é um instrumento essencial para o gerenciamento dos riscos. Os resultados da questão revelaram diferentes níveis de participação dos arquivistas na elaboração do Relatório de Impacto à Proteção de Dados (RIPD). A maioria dos arquivistas, representando 40% (8 arquivistas atuantes), indicou uma contribuição moderada no processo. Uma parcela menor, de 10% (2 arquivistas atuantes), reportou uma colaboração total, enquanto outros 10% (2 arquivistas atuantes) tiveram uma colaboração considerada significativa. Em contraste, 20% (4 arquivistas atuantes) mencionaram uma colaboração muito baixa, e outros 20% (4 arquivistas atuantes) afirmaram não ter colaborado na elaboração do RIPD, conforme demonstrado no gráfico a seguir:

Gráfico 16 - Questão 17 do Questionário



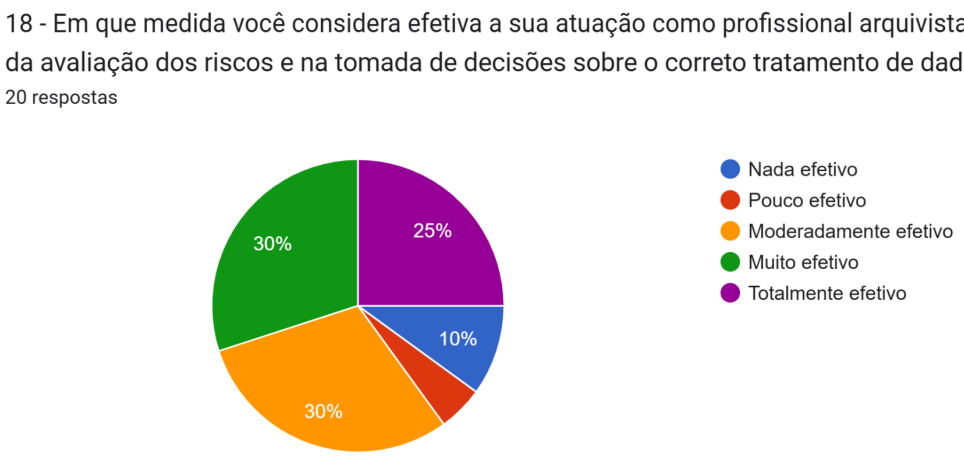
Fonte: elaboração própria, 2024

Diante desses resultados, alguns questionamentos surgiram a partir das análises, como quais fatores contribuíram para que alguns arquivistas tivessem uma colaboração significativa, enquanto outros tiveram uma baixa contribuição para a elaboração de relatórios de impactos à proteção de dados? Será que a proporção da contribuição na confecção desse documento pode estar relacionada ao nível de conhecimento do arquivista? Ou ainda, podemos inferir que a parcela considerável de 40% (20% não colaborou + 20% colaborou muito pouco = totalizando 8 arquivistas atuantes) que tiveram uma colaboração baixa ou

inexistente, é um fator de atenção considerando que esse é um documento essencial para o gerenciamento dos riscos no contexto dos arquivos?

A **questão de n.º 18**, utilizada para encerrar o questionário, buscou avaliar a percepção dos arquivistas sobre a efetividade de sua atuação na condução da avaliação de riscos e na tomada de decisões relacionadas ao tratamento adequado de dados pessoais. Os resultados indicaram que uma parcela significativa dos profissionais avaliou positivamente sua contribuição: 25% (5 arquivistas) consideraram sua atuação totalmente efetiva, e outros 30% (6 arquivistas) a julgaram muito efetiva. Um grupo também expressivo, representando 30% (6 arquivistas), percebeu sua atuação como moderadamente efetiva. Em contraste, uma minoria dos respondentes avaliou sua atuação com menor impacto, sendo 5% (1 arquivista) considerando-a pouco efetiva e 10% (2 arquivistas) como nada efetiva. Conforme demonstrado no gráfico que se segue:

Gráfico 17 - Questão 18 do Questionário



Fonte: elaboração própria, 2024

A partir desse resultado sobre a percepção da efetividade da atuação dos arquivistas no gerenciamento dos riscos de dados pessoais, podemos inferir que uma boa parcela desses profissionais possuem uma percepção positiva (25% dos arquivistas atuantes consideram sua atuação totalmente efetiva + 30% consideram muito efetiva = 55%, totalizando 11 arquivistas), o que nos leva a compreender que esses também reconhecem e confiam em suas habilidades e competências para atuação na área da proteção de dados. Por outro lado, observa também que uma parte significativa considera como moderadamente efetiva (30%, 6

arquivistas), pouco efetiva (5%, 1 arquivista) ou nada efetiva (10%, 2 arquivistas), pode nos apontar a necessidade de aprimoramento e capacitação das habilidades e competências.

Ainda tivemos mais contribuições no espaço aberto dedicado às considerações dos arquivistas atuantes sobre assuntos que não foram abordados no questionário. Um participante contribuiu com o relato de que também atuou de forma indireta, uma vez que suas funções perpassam por atividades que estavam sendo desenvolvidas no momento da implementação da LGPD, como a definição de requisitos para sistemas, a elaboração de manual de redação oficial e a definição de requisitos para o acesso a documentos arquivísticos de caráter permanente. O participante também relatou que houve questionamentos sobre as condições de acesso dos documentos, em relação às tensões entre a LGPD e a LAI, o que foi alinhado a partir de debates técnicos, destacando que o assunto é retomado com frequência.

Outro participante contribuiu com o relato sobre as confusões a respeito do tratamento de dados no âmbito da administração pública, sobre principalmente as informações que envolvem dados pessoais dos servidores, o que torna a rotina de trabalho e a tomadas de decisões morosas. Outra participante destacou a respeito do tratamento dos dados sensíveis, e avaliou que os procedimentos precisam de melhor definição para o acesso aos dados.

Enquanto outro participante destacou que na organização em que trabalha, no âmbito federal, a implementação da LGPD tem sido conduzida desde o início pela equipe de arquivistas, e que o processo ocorreu de forma natural, uma vez que já existia a preocupação com a proteção de dados em suas atividades. Além disso, o participante ressaltou o desinteresse de outras áreas da organização pelo tema.

Outro participante destacou que uma boa parte das adequações já estavam implementadas pela área de gestão de documentos, uma vez que estava no plano de metas do setor de Arquivos. Corroborando com a decisão de colocar o setor de arquivo como unidade responsável pelo apoio à implementação da LGPD. Nessa mesma direção, outro participante ressaltou que os arquivistas são os profissionais cuja responsabilidade é definir acerca da preservação dos documentos arquivísticos, e salientou que o profissional possui amparo legal para o desempenho dessa atividade. Além disso, observou que os arquivistas precisam tomar coragem para assumir seu papel.

Diante dessas contribuições, é fundamental revisitar as análises comparativas apresentadas na seção 4 deste estudo, que detalham as semelhanças e convergências entre as atribuições de arquivistas e encarregados de dados (conforme o quadro n.º 5). As experiências de arquivistas mostram, por exemplo, que a atribuição de "planejamento, organização e

direção de serviços de Arquivo" se alinha com as responsabilidades do encarregado de dados em relação aos direitos de acesso dos titulares e ao recebimento e encaminhamento de demandas das autoridades. Essas atribuições compartilham similaridades e convergências significativas, especialmente no que tange ao acesso à informação, à transparência, à prestação de contas e à responsabilização.

Além disso, foi possível associar o desenvolvimento das habilidades do arquivista às boas práticas das normas ISO/IEC 27701, que complementam a família ISO/IEC 27000. Essa relação ficou evidente ao compararmos as orientações do Quadro 6, na seção 4, com os exemplos de implementação citados pelos arquivistas atuantes na área de privacidade e proteção de dados.

Nesse sentido, a análise corrobora os exemplos práticos citados pelos arquivistas participantes da pesquisa quanto as discussões aqui levantadas sobre a importância de o profissional desenvolver suas competências humanas e profissionais. Isso inclui o aprimoramento de habilidades técnicas, humanas e conceituais, conforme destacado por Bahia (2018, p. 24-25).

6 OS PRINCÍPIOS DE GOVERNANÇA EM RELAÇÃO À PROTEÇÃO DE DADOS A FAVOR DE UMA GOVERNANÇA ARQUIVÍSTICA

A análise da contribuição da governança arquivística para a proteção de dados, requer um retorno aos conceitos da governança, institucional e corporativa, observando seus princípios e diretrizes, bem como a sua relevância para a avaliação da maturidade organizacional. Diante disso, esta seção objetivou investigar como a governança se manifesta em relação aos **princípios de integridade, da transparência, da prestação de contas e da responsabilidade** em consonância às diretrizes estabelecidas pela LGPD.

Cumpre salientar que, embora o princípio da equidade não seja tratado em seção específica, este reside no fato de sua natureza subjacente às práticas arquivísticas, permeando-as de maneira implícita, conforme demonstrado no decorrer desta dissertação. Tal princípio encontra respaldo no Código de Ética do Conselho Internacional de Arquivos (ICA), que estabelece diretrizes de conduta para o arquivista, como evidenciado nos princípios 6 e 7, que diz: "os arquivistas facilitam o acesso aos arquivos ao maior número possível de usuários, oferecendo seus serviços a todos com imparcialidade" e "os arquivistas visam encontrar o justo equilíbrio, no quadro da legislação em vigor, entre o direito ao conhecimento e o respeito à vida privada" (ICA,1996).

A temática da governança ganhou relevância no Brasil a partir de 1995[47] e obteve ainda maior destaque com a publicação do "Código das Melhores Práticas de Governança Corporativa", cuja qual, abordava os princípios considerados básicos de transparência, equidade, prestação de contas (*accountability*) e responsabilidade corporativa (IBGC, 2015). Em 2023 os princípios foram atualizados, sendo acrescidos outros dois: a **integridade** e a sustentabilidade (IBGC, 2023).

Atento às evoluções e observando a "interdependência entre as organizações, bem como a realidade econômica, social e ambiental em que elas estão inseridas", o IBGC atualizou a sua definição de governança corporativa:

> [...] é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em

[47] O Instituto Brasileiro de Governança Corporativa (IBGC), anteriormente nomeado como Instituto Brasileiro de Conselheiros de Administração (IBCA), é uma organização sem fins lucrativos que teve por objetivo de gerar e disseminar o conhecimento das melhores práticas em governança corporativa em diversos setores organizacionais.

> geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente (IBGC, 2023, p. 17).

No contexto do setor público, a discussão acerca da governança enfatiza propostas as relacionadas à transparência, integridade e à prestação de contas (IFAC, 2001)[48]. Além desses, alguns *frameworks,*[49] como a proposta da ANAO[50] (2003), acrescentaram outros três princípios importantes, são eles: liderança, compromisso e integração, os quais, se alinham aos objetivos de eficiência e a eficácia (CIPFA, 2004)[51].

O Tribunal de Contas da União, destacou que para garantia de uma boa governança depende de vários aspectos para alcance dos potenciais benefícios desta abordagem. A título de exemplos foram destacados: a garantia de um comportamento ético, o comprometimento transparente da liderança, a aderência das organizações às regulamentações, a adesão aos códigos, normas e padrões, o balanceamento dos interesses e o envolvimento efetivo dos cidadãos e usuários (TCU, 2020, p. 29).

No cenário brasileiro, a publicação do Referencial Básico de Governança (RBG), compreende um documento que reúne e organiza as boas práticas de governança pública e, quando são aplicadas, pode contribuir para o desempenho de órgãos e entidades públicas. Além desses, o RBG também destacou outros potenciais benefícios da governança, a saber:

> a) garantir a entrega de benefícios econômicos, sociais e ambientais para os cidadãos; b) garantir que a organização seja, e pareça, responsável para com os cidadãos; c) ter clareza acerca de quais são os produtos e serviços efetivamente prestados para cidadãos e usuários, e manter o foco nesse propósito; d) ser transparente, mantendo a sociedade informada acerca das decisões tomadas e dos riscos envolvidos; e) possuir e utilizar informações de qualidade e mecanismos robustos de apoio às tomadas de decisão; f) dialogar com a sociedade e a ela prestar contas; g) garantir a qualidade e a efetividade dos serviços prestados aos cidadãos; h) promover o desenvolvimento contínuo da liderança e dos colaboradores; i) definir claramente processos, papéis, responsabilidades e limites de poder e de autoridade; j) institucionalizar estruturas adequadas de governança; k) selecionar a liderança tendo por base aspectos como conhecimento, habilidades e atitudes (competências individuais); l) avaliar o desempenho e a conformidade da organização e da liderança, mantendo um balanceamento

[48] *Council of the International Federation of Accountants* (IFAC, 2001).
[49] *Framework* é uma estrutura sólida, que fornece a base para construir um software ou sistema, a partir de um conjunto de ferramentas e diretrizes que facilitam o desenvolvimento.
[50] *Australian National Audit Office. Public sector governance: better practice guide. Framework, processes and practices, 2003* (ANAO, 2003).
[51] *The Good Governance Standard for Public Services* (CIPFA, 2004), se trata de um guia para auxiliar a aplicação dos princípios da boa governança nos serviços públicos.

> adequado entre eles; m) garantir a existência de um sistema efetivo de gestão de riscos; n) utilizar-se de controles internos para manter os riscos em níveis adequados e aceitáveis; o) controlar as finanças de forma atenta, robusta e responsável; e p) prover aos cidadãos dados e informações de qualidade (confiáveis, tempestivas, relevantes e compreensíveis) (TCU, 2020, p. 30).

No que diz respeito ao alinhamento de normas e regulamentos do ordenamento jurídico, e que também podem amparar a estruturação da boa governança corporativa e pública do país[52], interessa aqui, dar destaque à Lei de Acesso à Informação (Lei 12.527/2011), que garante o direito fundamental de acesso à informação pública, e ainda facilita o controle e o monitoramento dos atos administrativos e da conduta de agentes públicos (TCU, 2011, p. 31).

O conceito de governança pública, é definido pelo Decreto n.º 9.203/2017 e pelo TCU (2020) de forma semelhante, 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".

De acordo com o Decreto n.º 9.203/2017, estão entre os seus princípios:

> **Capacidade de resposta**: capacidade que a administração tem para manifestar-se de forma clara, eficiente e eficaz às demandas apresentadas pelas partes interessadas; integridade: atuação focada na priorização do interesse público, pautando-se em valores morais e conduta ética; **confiabilidade**: capacidade de minimizar incertezas, garantindo um grau de segurança e credibilidade ao cidadão; **melhoria regulatória**: medidas sistemáticas para ampliar a qualidade da regulação com base em evidências e apoiadas em opiniões dos cidadãos e partes interessadas; **prestação de contas e responsabilidade (*accountability*)**: mecanismo para a prestação de contas, o controle social e a responsabilização pelo desempenho e resultados

[52] Regulamentos e normativos que contribuem para a boa governança nas instituições no Brasil: Código de Ética Profissional do Servidor Público Civil do Poder Executivo federal (Decreto 1.171/1994), que estabelece padrões éticos e morais para o comportamento da liderança no serviço público (Brasil, 1994); Lei de responsabilidade Fiscal (Lei Complementar 101/2000), que estabelece parâmetros de responsabilidade e transparência financeira e orçamentária (Brasil, 2000); Decreto de Gestão da Ética (Decreto 6.029/2007) (Brasil, 2007); Lei de Conflito de Interesses (Lei 12.813/ 2013), que trata do tema no exercício de cargo ou emprego do Poder Executivo federal (Brasil, 2013); Lei das Estatais (Lei 13.303/2016), que estabelece requisitos de governança para empresas públicas e de economia mista (Brasil, 2016); Instrução Normativa Conjunta MP/CGU 1/2016, que trata de controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal (Brasil, 2016); Lei de Defesa do Usuário de Serviços Públicos (Lei 13.460/2017), e sua regulamentação pelo Decreto 9.094/2017 (Brasil, 2017), que tratam sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos (Brasil, 2017); Decreto da Política de Governança da administração pública federal direta, autárquica e fundacional e Governança Pública (Decreto 9.203/2017), além de leis ou decretos, e outros normativos afins, editados pelos órgãos do poder executivo, legislativo e judiciário de estados e municípios, inspirados no decreto federal (Brasil, 2017) (TCU, 2020, p. 32).

> das ações na gestão pública; **transparência:** garantia de acesso às informações legítimas e fidedignas aos cidadãos (Brasil, 2020, grifo nosso).

Adicionalmente o Decreto n.º 9.203/2017, estabelece as diretrizes para desenvolvimento da governança pública, para o desempenho das organizações governamentais com foco nos seguintes aspectos: trazer resultados para a sociedade; a modernização e simplificação dos processos de gestão pública; o monitoramento do desempenho e avaliação das políticas e ações governamentais implementadas; a coordenação e articulação de processos para fortalecer a integração entre os diferentes níveis e esferas, gerando valor público (Brasil, 2017).

A gestão de riscos também se encontra entre as diretrizes deste regulamento e propõe a implementação de controles internos fundamentais para ações estratégicas preventivas. Enquanto a avaliação das políticas públicas, analisa propostas de criação e expansão, avaliando a economicidade. Além disso, a manutenção e a orientação no processo decisório, que se baseiam a partir de evidências para a conformidade legal, também são diretrizes para o bom desempenho das organizações governamentais. Outrossim, a qualidade normativa, pautada pelas boas práticas regulatórias, pela legitimidade e coerência do ordenamento jurídico, é igualmente estabelecida. E finalmente, a orientação pela transparência das atividades e resultados da organização, juntamente com a comunicação aberta à sociedade, que visam fortalecer o acesso público à informação (Brasil, 2017).

A respeito dos mecanismos para o alcance da boa governança, ou seja, referindo-se ao conjunto de ações ou operações necessárias para alcançar um determinado objetivo, esse mesmo Decreto determina o seguinte:

> I - **liderança,** que compreende conjunto de práticas de natureza humana ou comportamental exercida nos principais cargos das organizações, para assegurar a existência das condições mínimas para o exercício da boa governança, quais sejam: a) integridade; b) competência; c) responsabilidade; e d) motivação; II - **estratégia**, que compreende a definição de diretrizes, objetivos, planos e ações, além de critérios de priorização e alinhamento entre organizações e partes interessadas, para que os serviços e produtos de responsabilidade da organização alcancem o resultado pretendido; e III - **controle**, que compreende processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos (Brasil, 2017, grifo nosso).

Importante salientar que os mecanismos de governança, a liderança, estratégia e controle, bem como as suas práticas, irão depender das características da organização e suas necessidades, às exigências legais e os resultados pretendidos para a mitigação dos potenciais riscos.

Na abordagem para uma noção de governança estabelecida por Jardim (2018b. p. 32), o autor buscou traçar um esboço da governança arquivística a partir dos elementos fundamentais da gestão arquivística. Utilizando-se dos aspectos teóricos da governança e o cenário atual arquivístico brasileiro, teve por objetivo ilustrar uma a proposta em vários níveis governamentais, sobretudo no setor público.

Embora, é evidente que apesar dos avanços das instituições arquivísticas desde a redemocratização do país, a crescente demandas sociais por transparências do Estado, a busca pelo direito à memória, (Jardim 2018b, p. 34) e ainda notória observância pela necessidade de harmonia entre o direito de acesso e do direito à privacidade. É de se saber que as fragilidades ainda persistem, carecendo de mais investigações para equilibrar a balança entre a gestão e a governança na área.

Nesse contexto, Jardim (2018, p. 12) propõe uma reflexão sobre os redesenhos da teoria e das práticas arquivísticas nas últimas décadas. Tais transformações são impulsionadas pelos desdobramentos das realidades sociais e da influência de fatores como as "tecnologias da informação, da emergência de novos modelos organizacionais, dos princípios do governo aberto e das crescentes demandas sociais pelo direito à informação, à memória e à privacidade". A partir disso, o desenvolvimento em relação à governança arquivística pode favorecer sua concepção, bem como a implementação de novos modelos.

Em relação à definição do conceito de governança arquivística, Jardim considera que:

> [...] envolve um conjunto de diálogos, processos e produtos relacionados a vários atores e agências no Estado e da sociedade. Inclui não apenas aqueles segmentos diretamente relacionados a dimensões especificamente arquivísticas, mas também os atores, cujas ações perpassam, direta ou indiretamente, as políticas e práticas dos serviços e instituições arquivísticas. É o caso, entre outros, de políticas e ações relacionadas a Governo Aberto, Dados Abertos, Proteção de Dados Pessoais, Programas de Digitalização das Administrações Públicas, Patrimônio Cultural, Ciência e Tecnologia, Acesso à Informação Governamental, Controle Social, Educação, Bibliotecas, Museus, etc. (Jardim 2018, p.14).

É considerado como uma marca fundamental da governança arquivística a capacidade de atuação para além de uma gestão verticalizada, como agindo com ações transversais ao

contexto arquivístico. O autor destaca que a forma dinâmica e relacional "com outras agências, políticas e programas no campo da informação estatal, bem como com setores diversos da sociedade". Além disso, é atribuída a governança arquivística a capacidade do diálogo com outros ambientes informacionais (Jardim, 2018a, p. 40).

Por sua vez, Maluf (2023, p. 114) e Silva e Maluf (2025, p. 442) propuseram funções básicas para a governança arquivística, as quais se referiram às ações de **avaliar**, **dirigir** e **monitorar** o gerenciamento arquivístico, de forma semelhante às três atividades básicas da governança pública. Contudo, os autores ressaltaram a necessidade de adequação e maturação considerando a realidade organizacional e as especificidades de cada instituição, sobretudo, tendo em vista o escopo aplicável da governança no contexto dos arquivos (Silva e Maluf, 2025, p. 444).

Com base nas reflexões sobre a governança e sua função direcionadora, bem como as contribuições para a construção do conceito de governança arquivística, para essa seção, considerou-se relevante analisar como a governança em privacidade e proteção de dados atua sob a perspectiva dos arquivos. Parte-se do pressuposto que a governança arquivística interage e opera em conjunto a outros ambientes informacionais, todavia, mantendo o foco em seu objeto. Compreende-se que esta análise abrange a estrutura organizacional, os processos e os princípios norteadores para a garantia da proteção de dados, sem perder de vista os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

6.1 Os princípios de integridade, transparência, prestação de contas, responsabilidade no contexto dos arquivos

A governança corporativa, assim como a governança pública, compartilha em suas bases os princípios que orientam as aplicações nas organizações e instituições, até mesmo em situações que não foram previstas ou que não sejam de alguma forma aplicáveis, devido às especificidades de cada organização. Nesse sentido, buscou-se analisar brevemente esses elementos no contexto arquivístico, considerando sua natureza administrativa, jurídica, informacional, probatória, orgânica e cumulativa, conforme destacado por Bellotto (2002, p. 19). Essa complexidade, aliada a outras características, confere aos arquivos um caráter único e indivisível.

6.1.1 O Princípio da integridade

No âmbito da gestão de riscos e da segurança da informação, para implementação das boas práticas focadas na garantia da proteção dos dados e da mitigação dos riscos de uma instituição, considera a integridade como um dos pilares da segurança da informação e figura como propriedade característica de exatidão e completude (ISO/IEC 27000, 2018, p. 5)[53]. Paralelamente, a 'confidencialidade' e a 'disponibilidade' são os outros dois conceitos que integram os pilares da segurança da informação, em que confidencialidade se refere a propriedade de que as informações não sejam disponibilizadas ou divulgadas, enquanto disponibilidade está relacionada à garantia da informação (e também sistemas) esteja acessível e utilizável para as pessoas ou entidades autorizadas.

De acordo com o Tribunal de Contas da União, o termo de integridade no contexto das ações organizacionais e do comportamento do agente público, refere-se à adesão e ao alinhamento consistente aos valores, princípios e normas éticas comuns com vistas na priorização do interesse público sobre os interesses privados. Sugere-se a adoção de políticas de integridade baseadas em contexto da organização, de evidências e dos riscos. Além disso, recomenda-se a adesão a programas com menor rigidez para que não se tornem impeditivos ao comportamento ético. A utilização do princípio como estratégia se baseia em pilares que visam implementar um sistema de integridade amplo e coerente; o desenvolvimento de uma cultura de integridade pública; possibilitar a prestação de contas, a responsabilização e a transparência (TCU, 2020, p. 45).

A publicação do Decreto n.º 9.203 em 22 de novembro de 2017 também estabeleceu a obrigatoriedade de instituir programas de integridade, visando impulsionar iniciativas e práticas, desenvolver políticas e implementar mecanismos para a promoção da integridade no setor público. Por conseguinte, no âmbito do Poder Executivo Federal, a promoção da integridade pública ocorre de forma sistêmica e coordenada por meio do Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal (SITAI), instituído pelo Decreto n.º 11.529, de 16 de maio de 2023. Este decreto define termos como programa de integridade, plano de integridade e funções de integridade, conforme detalhado a seguir:

---

[53] Definição dos conceitos em inglês, segundo a norma *ISO 27000* (2018): ***Integrity****: property of accuracy and completeness;* ***Confidentiality****: property that information is not made available or disclosed to unauthorized individuals, entities, or processes;* ***Availability****: property of being accessible and usable on demand by an authorized entity.*

> I - **programa de integridade** - conjunto de princípios, normas, procedimentos e mecanismos de prevenção, detecção e remediação de práticas de corrupção e fraude, de irregularidades, ilícitos e outros desvios éticos e de conduta, de violação ou desrespeito a direitos, valores e princípios que impactem a confiança, a credibilidade e a reputação institucional; II - **plano de integridade** - plano que organiza as medidas de integridade a serem adotadas em determinado período, elaborado por unidade setorial do Sitai e aprovado pela autoridade máxima do órgão ou da entidade; e III - **funções de integridade** - funções constantes nos sistemas de corregedoria, ouvidoria, controle interno, gestão da ética, transparência e outras essenciais ao funcionamento do programa de integridade (Brasil, 2023).

A Controladoria-Geral da União (CGU), atua como órgão central e pela harmonização das funções de integridade, que possui entre as suas atribuições nos sistemas de corregedoria, controle interno, ouvidoria, gestão da ética, transparência e outras essenciais ao bom funcionamento do programa de integridade. Nesse sentido, a CGU avançou na consolidação da "gestão da integridade pública como um pilar estratégico nos órgãos e entidades do Poder Executivo federal, com o lançamento do "Modelo de Maturidade em Integridade Pública" (MMIP) (Brasil, 2023)". Trata-se de uma ferramenta para orientar esforços de uma organização na direção de uma melhor gestão, desempenho e efetividade de um Programa e Plano de Integridade.

Nesse sentido o MMIP é um modelo de diagnóstico e avaliação da maturidade em integridade pública organizacional, oferece os seguintes mecanismos: (1) realização de um diagnóstico; (2) a avaliação da maturidade em integridade pública em comparação com os padrões almejados; (3) a determinação dos requisitos de maturidade em integridade pública desejados, de acordo com a natureza, complexidade e riscos associados às suas operações; (4) a possibilidade de estabelecer um plano de ação para a superação de lacunas identificadas e para a consolidação do nível almejado de maturidade (Brasil, 2023, p. 9). Além disso, o modelo de diagnóstico e maturidade em integridade, possibilita:

> • **Comunicação**: apresenta os parâmetros do que configura uma atuação efetiva da gestão da integridade, de como ela se insere na estrutura de governança da organização, dos principais serviços prestados e do valor agregado à instituição. É, portanto, um valioso instrumento de interlocução e tomada de decisão estratégica no âmbito da organização. • **Avaliação**: estabelece metodologia para a avaliação da maturidade em integridade pública dos órgãos e entidades do Poder Executivo federal, seja na forma de autoavaliação (a própria organização conduz a avaliação), ou por meio de avaliação externa (a avaliação é executada, ou validada, por outra organização) • **Desenvolvimento**: oferece um roteiro para o aprimoramento estruturado da atuação da unidade setorial de integridade, indicando as etapas que a organização deve galgar para estabelecer, consolidar e ampliar a sua maturidade em integridade pública (Brasil, 2023, p. 9).

A *General Data Protection Regulation* também aborda o princípio da integridade (art. 5º) juntamente com ao princípio da confidencialidade, e os relacionam à segurança da informação, devendo a organização assegurar a proteção adequada dos dados, incluindo a "proteção contra o processamento não autorizado ou ilegal e contra perda acidental, destruição ou danificação, utilizando medidas técnicas ou organizacionais adequadas (Europa, 2016). O princípio também é abordado em outros artigos da *GDPR*, como o art. 32º que trata a respeito a segurança do processamento, e que consideram a "estado da técnica, os custos de implementação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas" (Europa, 2016).

Em análise dos Considerandos da *GDPR,* que são declarações introdutórias aos artigos do regulamento, nota-se que eles fornecem o contexto, a justificativa e os princípios que fundamentam as disposições legais, sendo cruciais para a interpretação e aplicação da norma. Especificamente, o Considerando n.º 49[54] aborda a integridade como um elemento essencial para garantir a segurança da rede e da informação. A declaração estabelece que o tratamento de dados pessoais, desde que estritamente necessário para essa finalidade, constitui um interesse legítimo do controlador de dados. Por outro lado, o Considerando n.º 121[55], detalha

---

[54] Considerando n.º 49 da GDPR: Segurança de Redes e Informações como Interesse Legítimo Prevalece: O processamento de dados pessoais na medida estritamente necessária e proporcional para fins de garantir a segurança da rede e da informação, ou seja, a capacidade de uma rede ou sistema de informação de resistir, em um determinado nível de confiança, a eventos acidentais ou ações ilegais ou maliciosas que comprometam a disponibilidade, autenticidade, integridade e confidencialidade dos dados pessoais armazenados ou transmitidos, e a segurança dos serviços relacionados oferecidos por, ou acessíveis por meio dessas redes e sistemas, por autoridades públicas, por equipes de resposta a emergências de computadores (*CERTs*), equipes de resposta a incidentes de segurança de computadores (*CSIRTs*), por provedores de redes e serviços de comunicações eletrônicas e por provedores de tecnologias e serviços de segurança, constitui um interesse legítimo do controlador de dados em questão. Isso pode incluir, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrônicas e a distribuição de código malicioso e interromper ataques de "negação de serviço" e danos a sistemas de comunicação eletrônica e de computadores. Disponível em: https://gdpr-info.eu/recitals/no-49/.

[55] Considerando n.º 121: Independência das Autoridades de Supervisão: 1 As condições gerais para o membro ou membros da autoridade de supervisão devem ser estabelecidas por lei em cada Estado-Membro e devem, em particular, prever que esses membros sejam nomeados, por meio de um procedimento transparente, pelo parlamento, pelo governo ou pelo chefe de Estado do Estado-Membro, com base em uma proposta do governo, de um membro do governo, do parlamento ou de uma câmara do parlamento, ou por um órgão independente incumbido pela legislação do Estado-Membro. 2 A fim de garantir a independência da autoridade de supervisão, o membro ou membros devem agir com integridade, abster-se de qualquer ação incompatível com suas funções e não devem, durante seu mandato, exercer qualquer ocupação incompatível, remunerada ou não. 3 A autoridade de supervisão deve ter seu próprio pessoal, escolhido pela autoridade de supervisão ou por um órgão independente estabelecido pela legislação do Estado-Membro, que deve estar sujeito à

as condições para a nomeação e o funcionamento das autoridades de supervisão do regulamento, órgãos responsáveis por monitorar e aplicar o regulamento, destaca o princípio da integridade no comportamento dos membros dessas autoridades, exigindo que suas ações sejam realizadas de forma transparente, atuando de forma independente e abster de qualquer outra função a qual vincula de forma incompatível.

No contexto dos arquivos, em nosso entendimento, a **integridade arquivística** decorre do "princípio da proveniência que consiste em resguardar um fundo de misturas com outros, de parcelamentos e de eliminações indiscriminadas" (Arquivo Nacional, 2005, p. 108). Por sua vez, Bellotto (2002, p. 21) considera que a integridade arquivística preserva as características de indivisibilidade, significando que os fundos de arquivo devem ser preservados sem dispersão, mutilação, alienação, destruição não autorizada ou adição indevida.

Nesse sentido, compreendemos também, que existem duas situações em que o princípio da integridade tem relação com a Arquivologia, podemos assim dizer que se trata de duas dimensões: (1) a primeira dimensão está relacionada na aplicação do princípio da proveniência tendo em vista os seus dois graus de aplicação o respeito aos fundos e o respeito a ordem original, quando se evita a dispersão dos fundos e mantêm-se as relações orgânicas entre os documentos e entre eles e o produtor e suas funções; (2) a segunda dimensão, de acordo com o nosso entendimento, o princípio de integridade está apoiado na garantia da acurácia e a autenticidade do documento, com foco na manutenção e preservação da completude do documento, mantendo íntegro, configurando a este, a presunção de fidedignidade e a confiabilidade.

Adicionalmente, a integridade arquivística, aproxima do conceito exposto pela Lei de Acesso à Informação, em seu art. 4º, que considera integridade à qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino.

6.1.2 O princípio da transparência

Segundo o Referencial Básico de Governança (2020, p. 45), o princípio da transparência diz respeito à permissão para que a sociedade obtenha informações atualizadas

---

direção exclusiva do membro ou membros da autoridade de supervisão. Disponível: https://gdpr-info.eu/recitals/no-121/

sobre as “operações, estruturas, processos decisórios, resultados e desempenho do setor público” (Brasil, 2020, p. 45). Consiste em:

> [...] disponibilizar, inclusive na forma de dados abertos, para as partes interessadas, as informações que sejam de seu interesse (arts. 3º, I e II, 5º, 8º e 10 da Lei 12.527/2011) e não apenas aquelas impostas por disposições de leis ou regulamentos. Caracteriza-se pela possibilidade de acesso a todas as informações relativas à organização pública, em uma linguagem cidadã, sendo um dos requisitos de controle do Estado pela sociedade civil (Brasil, 2020, p. 45).

O “Referencial Básico de Governança”, considera que o princípio da transparência aplicado de forma adequada proporciona um clima de confiança nas relações interna e externas, e que além das solicitações dos indivíduos, que são necessárias ao cumprimento obrigatório, as organizações devem praticar a transparência de forma oportuna à divulgação relevantes à sociedade, inclusive, em relação à situação financeira, à gestão de desempenho e da governança. Ademais, segundo o mesmo documento, o princípio da transparência “abrange várias iniciativas, como: acesso à informação, divulgação de natureza obrigatória; divulgação de natureza proativa e voluntária, incluindo dados abertos do governo; e transparência fiscal e orçamentária” (TCU, 2020, p. 45).

A aplicação deste princípio na esfera do Estado é vista como um novo instrumento da cidadania e resgata os aspectos da redemocratização do país, que teve como objetivo legítimo a ampliação do processo de acesso à informação. Processo este que buscou facilitar a vida das pessoas, a redução de tempo e custos, o aumento da eficiência a favor da conquista pela credibilidade governamental.

Na perspectiva de ofertar à sociedade o direito de acesso à informação, a transparência foi regulamentada por uma legislação específica e que também podemos considerar como uma legislação arquivística. A Lei n.º 12.527, de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação (LAI), regula o acesso às informações previsto na Constituição Federal de 1988, o qual está vinculado aos direitos e garantias fundamentais, destacados como direitos individuais e coletivos, conforme previsto no inciso XXXIII do art. 5º:

> [...] todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (Brasil, 1988).

Nesse sentido, a Lei de Acesso à Informação é direcionada aos órgãos públicos integrantes da administração direta, às autarquias, às fundações públicas, às empresas públicas, às sociedades de economia mista e demais entidades controladas direta ou indiretamente. A lei também se destina às entidades privadas sem fins lucrativos, que realizam ações de interesse público e que recebem recursos públicos para estes fins.

Além de assegurar o direito fundamental de acesso à informação, os procedimentos previstos na Lei devem ser executados em consonância com os princípios básicos da administração pública, em uma abordagem complementar ao princípio da publicidade. O artigo 3º da LAI estabelece as seguintes diretrizes:

> I - observância da publicidade como preceito geral e do sigilo como exceção; II - divulgação de informações de interesse público, independentemente de solicitações; III - utilização de meios de comunicação viabilizados pela tecnologia da informação; IV - fomento ao desenvolvimento da cultura de transparência na administração pública; V - desenvolvimento do controle social da administração pública.

Em consonância com os preceitos de acesso à informação e divulgação, o art. 6º atribui aos órgãos e entidades públicas a responsabilidade pela aplicação dos procedimentos estabelecidos. Sendo dos órgãos a responsabilidade de assegurar: a gestão transparente da informação, de modo a favorecer o amplo acesso; à proteção da informação, com foco nos pilares da segurança da informação (disponibilidade, autenticidade e integridade); e a proteção da informação sigilosa e pessoal, observando sua integridade e as restrições de acesso legalmente definidas (Brasil, 2011).

Para o atendimento ao princípio da transparência e a garantia ao acesso das informações, o art. 7º da lei compreende ao indivíduo o direito de obter:

> I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada; II - **informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades,** recolhidos ou não a arquivos públicos; III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado; **IV - informação primária, íntegra, autêntica e atualizada**; V - **informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços**; VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e VII - informação relativa: a) **à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos**; b)

> **ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores** (Brasil, 2011, grifos nossos).

Os grifos acima visam dar destaque a alguns direitos elencados no art. 7º da LAI, que visam evidenciar a relação direta com outros princípios da governança. Além da transparência, é possível perceber o princípio da prestação de contas, da integridade dos registros e de seu conteúdo. De igual maneira, infere-se que o artigo em questão aborda intrinsecamente os aspectos da responsabilização. Esta pode ser entendida como o processo contínuo de exigir a prestação de contas pelas ações (ou omissões) e pelos resultados das atividades sob a responsabilidade de um órgão ou área.

A Lei de Acesso à Informação também estabelece as obrigações para que o tratamento de informações pessoais ocorra de forma transparente. Contudo, o art. 31 alerta sobre os excessos, exigindo que esse tratamento seja realizado com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais (Brasil, 2011).

No contexto da proteção de informações, MacNeil, em seu estudo de 1992, analisou criticamente o equilíbrio entre os interesses público e privado. A autora avaliou a possibilidade do surgimento de conflitos entre o acesso e a privacidade no âmbito da discricionariedade administrativa. Ela destacou que:

> [...] o acesso aos documentos contendo informações pessoais é negado como uma questão de direito; em vez disso, uma arbitrariedade para divulgar tal informação é conferida aos agentes públicos. Esse poder discricionário é compelido a criar desigualdades no acesso. Quanto a divulgação pessoal pode expor uma agência do governo ou seus funcionários à crítica pública ou embaraço, o chefe da agência estará, claramente, em conflito de interesse em determinar se deve ou não liberar tal informação. Nessas circunstâncias, "o escudo da privacidade (pode ser) utilizado para proteger abusos (...) que não são de forma alguma [de caráter] pessoal". Por outro lado, os funcionários do governo também podem usar seu poder discricionário para divulgar informação que nitidamente invade a privacidade individual para promover os interesses de uma agência" (MacNeil, 2019, p. 94).

MacNeil (2019) indagou sobre os limites das ações dos profissionais arquivistas ao assumirem a responsabilidade de administrar o acesso a documentos contendo informações pessoais e, muitas vezes, informações pessoais sensíveis. Considerando os potenciais conflitos em relação aos dois valores sociais – a necessidade do indivíduo à privacidade e a necessidade de compreensão da sociedade sobre si própria –, a autora observou que, por um

lado, os arquivistas precisam “proteger a integridade dos interesses da privacidade representados neles; por outro, como comunicadores da memória documental da sociedade, são obrigados a promover o acesso aos documentos na maior extensão possível” (MacNeil, 2019, p. 126). A autora também refletiu a respeito da abrangência da proteção da privacidade somente às pessoas vivas e sobre a complexidade da noção das pessoas sobre si mesmas, que pode se estender além dos limites físicos. Indagou, então, se a informação sobre a família de um indivíduo pode ser considerada sobre ele próprio (MacNeil, 2019, p. 128). Diante dessas informações, cabe perguntar: como o arquivista, enquanto mediador, pode buscar equilíbrio entre o acesso e a privacidade?

No que diz respeito às restrições de acesso à informação, a Lei de Acesso à Informação determina, de acordo com o art. 21, que o acesso não poderá ser negado à informação necessária à tutela judicial ou administrativa de direitos fundamentais. Também determina que “as informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso” (Brasil, 2011).

Quanto à divulgação de informações sigilosas produzidas na administração pública, a LAI, determina que deverá assegurar a sua proteção, destacando em seu art. 25:

> [...] § 1° O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei.§ 2° O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.§ 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados (Brasil, 2011)**.**

Quanto ao tratamento das informações pessoais, a Lei de Acesso à Informação (LAI) estabelece que ele deve ser realizado de forma transparente, sempre respeitando a intimidade, a vida privada, a honra e a imagem das pessoas, bem como suas liberdades e garantias individuais. De forma mais criteriosa, o artigo 31 da LAI destaca outros critérios importantes, sobretudo para tratamento de informações pessoais com restrições, a saber:

> [...] § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada

> sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3° O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante.§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância (Brasil, 2011).

O Conselho Internacional de Arquivos (ICA, 2012, p. 6), que há muito tem se preocupado com a questão do acesso aos arquivos e, observando as mudanças políticas no cenário internacional, propôs-se a sublinhar a importância do acesso e da transparência como elementos necessários à prática arquivística. Como forma de incentivo para o "uso mais amplo possível dos arquivos, baseado no conjunto de leis, regulações e acordos com os quais atuam os arquivos [...], estimulam os arquivistas a serem proativos e a informar o público sobre a disponibilidade dos documentos para uso" (ICA, 2014, p. 4).

Em favor desse movimento, o Comitê de Boas Práticas e Normas (2010-2011), juntamente com arquivistas que, na ocasião, representaram diversas tradições arquivísticas, inclusive o Brasil, desenvolveu o esboço da declaração de "Princípios de acesso aos arquivos" para a adoção de um conjunto de dez princípios que tratavam do acesso aos arquivos. Os princípios propostos na declaração pelo comitê visavam o fortalecimento das instituições nos processos existentes em relação ao acesso aos arquivos, contribuindo como reforço nos procedimentos e na autoavaliação das práticas profissionais. Além disso, ofereceram diretrizes para a revisão dos procedimentos de acesso que apresentassem fragilidades e contestações (ICA, 2012, p. 8).

Na abertura da publicação, ressaltou-se a importância da preservação dos documentos arquivísticos para uso das gerações atuais, bem como para as futuras. Adicionalmente, destacou-se a respeito dos serviços de acesso para a conexão entre os arquivos públicos, o fornecimento de informações aos usuários e a consolidação da confiança depositada nas instituições em virtude dos serviços prestados (ICA, 2012, p. 9).

No que concerne ao papel dos arquivistas na adesão aos "Princípios de Acesso a Arquivos" em prol da transparência, o documento destacou que:

> Os arquivistas apoiam uma cultura de abertura, mas aceitam restrições conforme exigido pela legislação e outras autoridades, pela ética, ou por exigência dos doadores. Quando as restrições são inevitáveis, devem ser claras e limitadas em abrangência e duração. Os arquivistas encorajam as partes responsáveis a formular claramente mandatos e regras consistentes para acesso aos documentos, mas, na ausência de orientações inequívocas, viabilizam o acesso apropriado, considerando a ética profissional, a equidade, a justiça e os requisitos legais. Os arquivistas garantem que as restrições sejam aplicadas justa e razoavelmente, e proporcionam o uso mais amplo possível dos documentos por meio do monitoramento das restrições e da imediata revogação daquelas que não se justificam mais (ICA, 2012).

Reconhecidos internacionalmente como referência para avaliar práticas e políticas de acesso e como guia para o desenvolvimento (ou modificação) de normas de acesso, os dez princípios abrangem tanto os direitos de acesso do público quanto a responsabilidade dos arquivistas em facilitar o acesso aos arquivos e às informações, a saber:

> 1. O público tem o direito de acesso aos arquivos de órgãos públicos. Entidades públicas e privadas devem abrir seus arquivos o mais amplamente possível; 2. Instituições custodiadoras de arquivos tornam pública a existência dos arquivos, inclusive a de documentos fechados ao acesso, e divulgam as restrições que afetam os arquivos; 3. Instituições custodiadoras de arquivos adotam uma abordagem proativa para acesso; 4. Instituições custodiadoras asseguram que restrições de acesso sejam claras e de duração determinada, baseadas em legislação pertinente, reconhecem o direito de privacidade de acordo com as normas culturais e respeitam os direitos dos proprietários de documentos privados; 5. Arquivos são disponibilizados em condições de acesso igualitárias e justas; 6. Instituições custodiadoras de arquivos garantem que vítimas de crimes graves segundo as leis internacionais tenham acesso a documentos que proporcionam a evidência necessária à afirmação de seus direitos humanos e à prova de sua violação, mesmo se esses documentos estiverem fechados ao público em geral; 7. Usuários têm o direito de apelar de uma negação de acesso; 8. Instituições custodiadoras de arquivos garantem que as restrições operacionais não impeçam o acesso aos arquivos; 9. Arquivistas têm acesso a todos os arquivos fechados e neles realizam o trabalho arquivístico necessário; 10. Arquivistas participam do processo de tomada de decisão sobre acesso (ICA, 2012).

Os “Princípios de acesso aos arquivos” são de aplicação geral, sendo utilizados como um guia de referência para o contexto amplo. Contudo, reconhecem a existência de documentos que necessitam ser retirados do acesso público por períodos determinados. Diante disso, o Comitê de Boas Práticas e Normas publicou uma orientação técnica que busca auxiliar a gestão de arquivos com restrições, compondo, assim, uma segunda declaração referente ao “Princípio de acesso aos arquivos".

É nesse sentido que os arquivistas atuam como mediadores e "precisam assegurar tanto à comunidade usuária quanto às entidades que impõem restrições que essas são adequadamente aplicadas" (ICA, 2014, p. 4). No documento, foram destacadas as seguintes orientações sobre procedimentos que trazem considerações em relação às restrições:

1. Assegurar ao público informações sobre os arquivos;
2. O desenvolvimento de políticas de acesso que se baseia na presunção da abertura, se atentando às restrições a informações devidamente escritas de modo que o público compreenda;
3. Acordos de restrições acerca do acesso na ocasião da transferência, assegurando também o direito de privacidade;
4. O controle ao acesso físico aos documentos sob restrição;
5. A permissão da equipe acesso aos documentos sob restrição para realização do trabalho arquivístico;
6. Descrever documentos sob restrição;
7. Responder a pedidos de acesso a documentos sob restrição, considerando as condições de acesso de forma justa e igualitária, todavia é necessário se atender as exceções à restrição;
8. A tomada de decisão sobre acesso, na qual, o arquivista participa do processo de seleção e revisão a fim de determinar a aplicação ou não de restrições.
9. A implementar restrições de acesso;
10. Registro e controle das decisões acerca da tomada de decisão;
11. Revisão das restrições de acesso, garantindo ao usuário o recurso de revisão;
12. Liberação de documentos anteriormente restritos.

A fim de ilustrar, o quadro que se segue relaciona os itens previamente mencionados e, subsequentemente, as orientações técnicas para a implementação do princípio da transparência como prática integrante da boa governança, com vistas à avaliação, ao direcionamento e ao monitoramento do gerenciamento arquivístico em favor da proteção de dados. Nesse sentido, considera-se como parte da análise para a compreensão do equilíbrio entre a garantia do direito de acesso às informações em poder das instituições públicas e o dever de garantir a privacidade dos indivíduos, como mencionados pelas autoras Rodrigues (2019, p. 9) e MacNeil (2019, p. 19).

Quadro 8: Princípios de Acesso a Arquivos: orientações para arquivos com restrições

Restrições	Orientações de Boas Práticas
1. Informações ao público sobre os arquivos	É essencial que as entidades públicas e privadas disponibilizem **informações de forma ampla e acessíveis ao público** sobre seus acervos e políticas de acesso e de aquisição, promovendo transparência.
2. Desenvolvimento de políticas de acesso	Os instrumentos que **governam as políticas de acesso** devem ser aprovados pelo alto escalão da instituição ou da instância administrativa. As políticas devem ser redigidas com a premissa baseada na presunção de abertura, porém se houver documentos que necessitam estar em restrição (gerais e específicas), estes devem estar descritos de forma transparente para compreensão do público, detalhando as exceções. "A política de acesso refere-se a quaisquer leis, regulações, decretos e decisões judiciais, políticas e regras internas e acordos de doação que se aplicam aos arquivos" (ICA, 2014, p. 7).
3. Acordos de restrição para a transferência	Orienta-se que para a transferência documentos para custódia, é necessário definir restrições de forma clara, com prazos determinados, **garantindo a privacidade**. Além disso, considera-se também respeitar a legislação arquivística e ainda as restrições de segurança nacional ou de decisões judiciais que atentem contra a privacidade de alguém. Quaisquer restrições específicas devem ser listadas no documento de transferência (ICA, 2014, p. 9).
4. Controle de acesso físico aos documentos sob restrição	Orienta-se a respeito do controle para áreas de armazenamento de documentos a fim de **garantir a proteção dos documentos e informações** a fim de **reduzir os riscos** de acesso indevidos.
5. Permissão de acesso à equipe arquivística	Orienta-se que os arquivistas deverão ter o direito de acesso todos os arquivos fechados (documentos restritos) para a **execução das suas funções, em cumprimento das finalidades** do tratamento arquivístico (ICA, 2014, p. 10)
6. Descrição de documentos sob restrição	Orienta-se que as instituições custodiadoras devem tornar pública a existência de arquivos, mesmo documentos com acesso restrito devem ser descritos, **respeitando a confidencialidade e garantindo ao usuário o direito de revisão** da decisão da restrição.
7. Resposta a pedidos de acesso a documentos sob restrição	A orientação do **direito ao acesso de forma justa e igualitária**. Ao receber um pedido, o arquivista deve verificar se o material é aberto para uso público, caso não esteja aberto, avaliar se o solicitante é legível, observando as exceções estabelecidas previamente e justificadas em políticas de acesso. (ICA, 2014, p. 11-12).

8. Tomada de decisão sobre acesso	Orienta-se que o arquivista participe ativamente do processo de avaliação e revisão do acesso, aplicando critérios técnicos. Pode utilizar-se de **metodologias para o gerenciamento dos riscos** ao processo de seleção: "a proveniência dos documentos, o assunto do dossiê/processo, e a data e o formato dos documentos podem indicar onde informações restritas são suscetíveis de serem encontradas e se o exame detalhado dos documentos é necessário" (ICA, 2014, p. 13). A revisão de documentos fechados também inclui análise de leis e regulamentos, despachos e decisões judiciais, políticas internas.
9. Implementação de restrições ao acesso	Orienta-se que as instituições que não desejam restringir o acesso aos documentos, devem implementar medidas para o controle sobre o uso final da informação, como assinaturas de compromisso de não divulgação (**análise e mitigação de riscos**); técnicas físicas para restrição de informações em documentos de papel, digitais ou audiovisuais (**medidas de segurança a informação**) (ICA, 2014, p. 14)
10. Registro das decisões sobre o acesso	Orienta-se que para cada decisão de restrição de acesso deve ser documentada e disponibilizada aos membros da equipe, permitindo a **rastreabilidade e prestação de contas** das ações (ICA, 2014, p. 16).
11. Revisão das restrições de acesso	Orienta-se que para atender o direito do usuário recorrer das restrições aplicadas, o procedimento de recursos baseado na legislação e normas internas. Como aplicação de **boas práticas** cabe o fornecimento de um calendário para recursos e respostas da instituição, estabelecendo **mecanismos para revisões e monitoramento periódicos**, que visam a garantia do "acesso aberto" (ICA, 2014, p. 17)
12. Liberação de documentos anteriormente restritos	Orienta-se que os documentos que deixarem de ter necessidade de restrição devem ser liberados ao público nos mesmos termos e condições, ampliando o acesso integral à informação. A revisão deverá ser documentada para o controle da instituição contendo informações que tratam da restrição, utilizando também a prerrogativa do interesse público. "A legislação de proteção de dados pode proibir a inclusão da identidade do usuário cujo pedido levou à liberação das informações. O dossiê de controle deve **manter a evidência de que os documentos** eram restritos no passado e ser conservado permanentemente" (ICA, 2014, p. 18).

Fonte: elaboração própria (baseado em ICA, 2014)

Em relação à Lei Geral de Proteção de Dados, conforme mencionado na seção 3, o princípio da transparência é um dos dez pilares obrigatórios, exigindo que as informações sobre o tratamento de dados sejam claras, precisas e facilmente acessíveis. Além disso, a lei obriga o controlador à adoção de medidas que garantem a transparência do tratamento de

dados quando houver utilização dos dados com base em seu legítimo interesse, conforme destacado no art. 10º. Com isso, os direitos do titular também são assegurados, garantindo-se o acesso facilitado ao tratamento das informações pessoais, conforme destacado no art.17:

> Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição.

A respeito de como o princípio da transparência figura no regulamento europeu, o termo garante seu lugar nos princípios basilares, assim como na LGPD – informação que era de se esperar, uma vez que a norma brasileira foi inspirada na GDPR. Segundo a *General Data Protection Regulation*, os dados pessoais deverão ser "processados de forma lícita, leal e transparente em relação ao titular dos dados ('licitude, lealdade e transparência')" (Europa, 2016)

De forma mais abrangente, o regulamento aborda o princípio da transparência nos capítulos dedicados aos Direitos do Titular (artigos 12 a 23) e, especificamente, nas declarações dos Considerandos n.º 58[56] e n.º 60[57], detalhando este último a obrigação da informação.

---

[56] Considerando n.º 58: O Princípio da Transparência: 1. O princípio da transparência exige que qualquer informação dirigida ao público ou ao titular dos dados seja concisa, facilmente acessível e fácil de entender, e seja utilizada linguagem clara e simples e, adicionalmente, quando apropriado, visualização. 2. Essas informações podem ser fornecidas em formato eletrônico, por exemplo, quando dirigidas ao público, por meio de um site. 3. Isso é de particular relevância em situações em que a proliferação de atores e a complexidade tecnológica da prática tornam difícil para o titular dos dados saber e entender se, por quem e para qual finalidade os dados pessoais relacionados a ele ou ela estão sendo coletados, como no caso de publicidade online. 4. Dado que as crianças merecem proteção específica, qualquer informação e comunicação, quando o processamento for dirigido a uma criança, deve ser feita em linguagem clara e simples que a criança possa entender facilmente.

[57] Considerando 60: Obrigação de Informação: 1. Os princípios do tratamento justo e transparente exigem que o titular dos dados seja informado da existência da operação de tratamento e das suas finalidades. 2. O responsável pelo tratamento deverá fornecer ao titular dos dados quaisquer informações adicionais necessárias para garantir um tratamento justo e transparente, tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais são tratados. 3. Além disso, o titular dos dados deverá ser informado da existência de definição de perfis e das consequências dessa definição. 4. Quando os dados pessoais forem recolhidos junto do titular dos dados, este deverá também ser informado se é obrigado a fornecer os dados pessoais e das consequências, caso não os forneça. 5. Essas informações podem ser fornecidas em combinação com ícones normalizados, a fim de proporcionar, de forma facilmente visível, inteligível e claramente legível, uma visão geral significativa do tratamento pretendido. 6. Quando os ícones forem apresentados por via eletrônica, deverão ser legíveis por máquina.

O regulamento europeu (GDPR) distinguiu dois cenários para a prestação dessas informações: quando os dados pessoais são obtidos diretamente do titular (artigo 13) e, em contrapartida, quando as informações coletadas são usadas para contatá-lo diretamente, caso em que ele tem o direito de ser informado imediatamente após o primeiro contato (artigo 14).

Para concluir, sem esgotar o tema, é fundamental destacar a definição de transparência no âmbito das organizações privadas, tal como apresentada pelo "Código das Melhores Práticas de Governança Corporativa" do IBGC (2023, p. 18). O documento a conceitua como a prática de tornar acessíveis às partes interessadas informações "verdadeiras, tempestivas, coerentes, claras e relevantes, incluindo tanto as informações positivas quanto as negativas, e indo além do que é exigido por leis e regulamentos" (IBGC, 2023, p. 18). A promoção da transparência não apenas impulsiona o desenvolvimento dos negócios, mas também favorece um ambiente de confiança essencial para o relacionamento com todas as partes interessadas.

6.1.3 O princípio da prestação de contas e responsabilidade (*accountability)*

Continuando no panorama dos princípios que compõem a aplicação da boa governança, a prestação de contas e a responsabilidade emergem como preceitos necessários às instituições e organizações que propõem a obrigação de os agentes serem responsáveis por suas ações, decisões e resultados, garantindo isso por meio da demonstração de medidas em favor da conformidade regulatória.

O "Referencial Básico de Governança Organizacional" considerou o princípio da prestação de contas e da responsabilidade como sinônimos do termo em inglês "*accountability*", que diz respeito a:

> [...] à obrigação que têm as pessoas ou entidades às quais se tenham confiado recursos, incluídas as empresas e corporações públicas, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar o cumprimento dessas a quem lhes delegou essas responsabilidades (Brasil, 2011). Espera-se que os agentes públicos prestem contas de sua atuação espontaneamente, de forma clara e tempestiva, assumindo integralmente as consequências de seus atos e omissões (IBGC, 2015). O Banco Mundial (2017) esclarece que a prestação de contas efetiva está ligada a um conjunto amplo de incentivos e mecanismos institucionais, como os de garantia de responsabilização, de participação social e de parcerias entre atores estatais e não estatais. A OCDE (2018) aborda diferentes tipos de prestação de contas, como a administrativa, a financeira e orçamentária, a social e a referente a resultados de políticas públicas (TCU, 2020, p. 46).

Na estrutura da governança pública, a prestação de contas e a responsabilidade integram o mecanismo de controle e suas práticas. Nesse contexto, os cidadãos, ao delegarem ao setor público a gestão de recursos e a busca por resultados, legitimam a obrigação das organizações em prestar contas à sociedade. Tal prestação implica demonstrar o controle sobre a administração dos recursos públicos, em consonância com os princípios e diretrizes regulatórias, o que se concretiza por meio da transparência, da efetiva prestação de contas e da responsabilização dos agentes envolvidos.

A respeito das práticas de prestação de contas e da responsabilidade, o Referencial Básico de Governança, destacou que:

> A liderança é responsável por garantir que a implementação do modelo de governança pública inclua mecanismos de *accountability* (prestação de contas e responsabilização), em contexto de transparência que lhes garanta a efetividade em direção ao interesse da sociedade e que garanta o acesso a todas as informações de interesse público, e não somente daquelas previamente obrigatórias por norma (TCU, 2020 p. 92).

Observa-se que a promoção da transparência está diretamente ligada à *accountability*, todavia, a transparência, de forma isolada, não configura efetivamente a consolidação da prestação de contas e da responsabilização, pois os agentes devem ir além de apenas informar. É necessário que "justifiquem as suas decisões no que tange à gestão de recursos públicos e, ainda que as estruturas e processos organizacionais garantam que eles sejam responsabilizados por suas ações" (TCU, 2020, p. 92).

Destaca-se que a **responsabilização** também configura um elemento importante, pois, de forma semelhante, diz respeito à competência de gerir os recursos, à identificação e apuração de irregularidades e à aplicação das sanções devidas. Conforme destacado pelo TCU (2020) sobre o comportamento das organizações:

> [...] estabelecer mecanismos que possibilitem a clara atribuição de papéis e responsabilidades e a identificação e apuração de ilícitos, bem como a instauração (ou a requisição às instâncias competentes pela instauração) dos procedimentos necessários à apuração de irregularidades, e a aplicação de sanções nos casos pertinentes. Por isso, é necessário prover os meios para que a organização tome conhecimento das irregularidades e desvios éticos cometidos pelos agentes públicos (TCU, 2020, p. 94).

Nessa direção, o TCU (2020, p. 97) ressaltou que, para garantir a *accountability*, é preciso ir além da apresentação de relatórios aos órgãos de controle e da disponibilização para a sociedade do que é exigido nas normas, mas providenciar que essas informações estejam disponíveis para amplo acesso à sociedade e às partes interessadas, possibilitando a transparência ativa das organizações. Ademais, as organizações devem:

> [...] fomentar o controle social do que tem sido planejado e alcançado por ela, ao publicar os extratos dos planos de sua responsabilidade e ainda os respectivos relatórios de acompanhamento (excepcionados os casos de restrição de acesso amparados pela legislação), de forma que a sociedade possa tomar conhecimento dos desdobramentos desses planos na organização, e acompanhar o alcance de objetivos e metas e a evolução dos indicadores (TCU, 2020, p. 97).

Outrossim, na aplicação prática desses princípios da prestação de contas e da responsabilidade, as organizações também devem assegurar que as partes interessadas possam se manifestar por meio de um canal estruturado para o recebimento, encaminhamento e tratamento das demandas. Nesse sentido, é importante que esse canal disponha de uma política que priorize a boa-fé e a garantia do sigilo nos termos da lei, além de prever sanções para denúncias falsas. Espera-se que os interessados reconheçam "a disponibilidade [e a] adequação do canal de manifestações" (TCU, 2020, p. 98).

Visando assegurar a prestação de contas e a responsabilidade, o TCU (2020, p. 98) também estabeleceu o dever da organização de processar infrações disciplinares e os desvios éticos dos agentes e prestadores de serviços, observando os princípios do contraditório e da ampla defesa. Além disso, considerou de igual importância a padronização dos procedimentos que facilitem a investigação de desvios administrativos e atos ilícitos, inclusive nos procedimentos que visam o encaminhamento dos resultados a órgãos que têm por competência a função de investigar, como o Ministério Público Federal, a Controladoria-Geral da União ou a Comissão de Ética Pública.

Também caracterizou como boa prática da governança, em cumprimento do princípio de prestação de contas e da responsabilidade, a capacitação das equipes com foco na redução e correção dos riscos de nulidades dos procedimentos e, em consequência, no impedimento de punição aos responsáveis. De igual maneira, preconizou a adoção de meios para "apuração e punição de faltas de menor potencial ofensivo, estimulando termos de ajustes de conduta e outros mecanismos que reduzam o custo administrativo de processamento de falhas menores" (TCU, 2020, p. 98).

No âmbito da governança corporativa, o Código das Melhores Práticas de Governança Corporativa aborda os conceitos de prestação de contas e responsabilidade por meio do princípio da responsabilização, termo que também engloba a noção de *accountability*. Este preceito consiste em:

> Desempenhar suas funções com diligência, independência e com vistas à geração de valor sustentável no longo prazo, assumindo a responsabilidade pelas consequências de seus atos e omissões. Além disso, prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, cientes de que suas decisões podem não apenas responsabilizá-los individualmente, como impactar a organização, suas partes interessadas e o meio ambiente (IBGC, 2023, p. 17).

A partir da perspectiva em relação a como se estruturam os princípios nos diferentes cenários de governança pública e corporativa, considera-se importante para esta pesquisa compreender a evolução do conceito de *accountability*, o qual está presente nas discussões internacionais e como foi introduzido no cenário brasileiro, sobretudo nos aspectos da proteção de dados. Para tanto, Bioni (2022) traçou um panorama da evolução do conceito de *accountability* ao longo das últimas décadas, refletindo a respeito de sua origem até as discussões atuais, inclusive reconhecendo a multiplicidade do uso do termo, principalmente no campo das ciências sociais. Além disso, o autor evidenciou como o termo colabora para as chamadas "**práticas informacionais justas**" – um indício para a compreensão do termo. Demonstrou, ainda, como o debate e suas resoluções acerca do tema podem ser utilizados ou ajustados para as necessidades atuais da sociedade (Bioni, 2022, p. 10).

O autor definiu o termo como "camaleão" devido à sua capacidade de atribuir diferentes significados, como responsabilidade, integridade, equidade, eficiência, transparência e, ainda, democracia. Nesse sentido, foram destacadas duas ideias centrais a partir de sua análise aos relatórios do grupo de trabalho sobre sistemas de processamentos automatizados de informações do *Health, Education, and Welfare (HEW*), sendo: (1) a compreensão da proteção de dados como uma atualização do desdobramento da cláusula do devido processo legal, que visava assegurar aos cidadãos o direito de saber e questionar o processamento de suas informações; e (2) a obrigação de adoção de procedimentos para evitar danos colaterais de atividades de tratamento de dados em toda a cadeia de agentes, o que caracteriza medidas de salvaguarda e precaução que minimizam possíveis riscos (Bioni, 2022, p. 5-7).

Em suas análises, Bioni (2022, p. 12) identificou que o diagnóstico do grupo de trabalho, representado na pessoa de Arthur Miller, e alertou para a carência da existência do conceito de privacidade, o qual não deveria se restringir à liberdade negativa do cidadão (ausência de interferência). O que estava em jogo poderia ser uma concepção mais positiva, condicionada a medidas adequadas para a manipulação legítima das informações pessoais.

A partir dessas considerações, o autor destacou o surgimento de quatro princípios que garantiriam deveres aos agentes que processassem as informações, e os direitos aos titulares dos dados, caracterizando práticas mais responsáveis (*accountable*):

> [...] o que se propôs foi basicamente a articulação de deveres e direitos entre quem processa dados e quem é o seu respectivo titular. A partir dessa mutualidade, o objetivo principal foi colocar o cidadão no circuito decisório constitutivo da sua própria identidade, até então construída com o recolhimento opaco de seus dados e sem contraditório de sua parte [...] Esse é exatamente o conteúdo (obrigacional) dos quatro dos cinco princípios estabelecidos pelo HEW: (i) não pode haver sistemas de bases de dados pessoais cuja existência seja secreta; (ii) deve existir um meio para que o indivíduo possa descobrir que tipos de informações sobre ele estão armazenadas e como estão sendo utilizadas; (iii) deve existir um meio para que o indivíduo possa evitar que informações sobre ele sejam obtidas para uma finalidade sejam utilizadas ou disponibilizadas para finalidade diversa sem seu consentimento; (iv) deve haver um meio de o indivíduo corrigir ou emendar um registro de informações sobre ele que o tornam identificável. (Bioni, 2022, p. 13).

Nesse sentido, o autor compreende que esse conjunto de obrigações e direitos colaborou para uma espécie de procedimentação, a qual alterou a dinâmica das relações e melhorou o comportamento de quem manipulava tais dados, uma vez que até então não havia nenhuma recomendação. O que ficou determinado é que, para além do uso legítimo e justo, deveriam garantir, nesse processo, também os resultados. Na mesma direção, Bioni (2022, p. 15) apresentou a análise de um segundo diagnóstico exposto a partir dos encontros do grupo de trabalho, no qual identificou que a necessidade de salvaguardas e medidas adequadas era uma questão de organização e não se relacionava apenas com os aspectos tecnológicos, configurando, assim, o quinto princípio:

> (v) qualquer organização que crie, mantenha, use ou dissemine registros de dados pessoais identificáveis deve garantir a confiabilidade de dados para o uso pretendido e deve tomar as medidas necessárias para evitar o uso inadequado desse dado (Bioni, 2022, p.15).

Nessa lógica, a tecnologia estaria envolvida como parte da solução, e não o contrário. Mais importante que o controle das informações de uma base de dados, o foco estaria sobre quais mecanismos de contingência, em relação a quais dados, seriam imputados. O autor destacou a respeito de “procedimentos mínimos” de governança para a modelagem de sistemas de informação como uma forma efetiva e preventiva para lidar com o mau uso na manipulação dos dados e para ser auditável, criando, assim, o “senso de responsabilidade” (Bioni, 2022, p. 16).

Embora muitos anos tenham se passado, as recomendações de Miller (1973, p. 43) permanecem atuais em relação ao foco na manutenção dos registros e aos mecanismos para fornecer salvaguardas, conforme podemos observar:

> As salvaguardas que recomendamos não exigem o estabelecimento de novos mecanismos e não buscam impor restrições à aplicação de tecnologias de processamento eletrônico de dados além daquelas necessárias para assegurar a manutenção de padrões razoáveis de privacidade pessoal na manutenção de registros. Visam não criar obstáculos ao desenvolvimento, adaptação e aplicação de uma tecnologia que, todos concordamos, trouxe uma variedade de benefícios a uma ampla gama de pessoas e instituições na sociedade moderna. As salvaguardas propostas visam garantir que as decisões sobre a coleta, o registro, o armazenamento, a disseminação e o uso de dados pessoais identificáveis sejam tomadas com plena consciência e consideração das questões de privacidade pessoal – questões que surgem de conflitos e contradições inerentes em valores e interesses (Miller, 1973, p. 43, tradução nossa).

A propósito, o autor observa que, embora o termo "*accountability*" não seja citado (Bioni, 2022, p. 17), este é o elemento que justifica a necessidade de adoção de diretrizes para responsabilizar o uso das informações, conforme se observa na fala de Miller:

> As salvaguardas que recomendamos não podem garantir a resolução desses conflitos de forma satisfatória para todos os indivíduos e grupos envolvidos. No entanto, podem garantir que esses conflitos sejam plenamente reconhecidos e que os processos de tomada de decisão, tanto no setor privado quanto no público, que levam à atribuição de maior prioridade a um interesse em detrimento de outro, sejam abertos, informados e justos. As salvaguardas que recomendaremos visam criar incentivos para que as instituições que mantêm sistemas automatizados de dados pessoais sigam rigorosamente os princípios básicos de práticas justas de informação. O estabelecimento de uma proteção legal contra práticas desleais de informação que incorpore os requisitos de salvaguarda [...] invocará os mecanismos existentes para garantir que os sistemas automatizados de dados pessoais sejam projetados, gerenciados e operados com o devido respeito à proteção da privacidade pessoal. Pretendemos e recomendamos que as instituições sejam responsabilizadas por práticas desleais de informação e

> sejam responsabilizadas por danos reais e punitivos a indivíduos que representem a si próprios ou a classes de indivíduos. Com tais sanções, os gestores institucionais teriam fortes incentivos para garantir que seus sistemas automatizados de dados pessoais não violassem a privacidade de titulares de dados individuais, conforme definido. De suma importância, do nosso ponto de vista, as salvaguardas que recomendaremos fornecem aos tribunais uma base confiável e de aplicação geral para a proteção da privacidade pessoal em relação à manutenção de registros[58] (Miller, 1973, p. 44, tradução nossa).

A partir dessas reflexões, Bioni definiu o princípio de *accountability* como:

> […] envelope da mensagem regulatória encaminhada pelas práticas informacionais justas. Em um contexto no qual inexistia procedimentos mínimos para que a extração de dados fosse responsável, sustentável e menos lesiva, o ponto de partida seria atribuir, de forma cruzada, direitos e deveres aos agentes da cadeia de tratamento de dados e aos seus respectivos titulares (Bioni, 2022, p. 18).

Bioni (2022, p. 25) também descreveu o conceito como enxuto e camaleônico. Apesar das discussões sobre sua definição, especialmente no que tange à responsabilidade afirmativa e aos mecanismos de boas práticas e políticas organizacionais, a OCDE optou por sintetizá-lo. Segundo a organização, o princípio da *accountability* estabelece que o controlador de dados deve ser responsável pelo cumprimento das medidas que dão efeito aos princípios estabelecidos[59] (OCDE, 2002, p. 16).

---

[58] Texto original: *"Our recommended safeguards cannot assure resolution of those conflicts to the satisfaction of all individuals and groups involved. However, they can assure that those conflicts will be fully recognized and that the decision-making processes in both the private and public sectors, which lead to assigning higher priority to one interest than to another, will be open, informed, and fair. The safeguards we will recommend are intended to create incentives for institutions that maintain automated personal data systems to adhere closely to basic principles of fair information practice. Establishment of a legal protection against unfair information practice to embody the safeguard requirements described in Chapters IV, V, and VI, will invoke existing mechanisms to assure that automated personal data systems are designed, managed, and operated with due regard for protection of personal privacy. We intend and recommend that institutions should be held legally responsible for unfair information practice and should be liable for actual and punitive damages to individuals representing themselves or classes of individuals. With such sanctions institutional managers would have strong incentives to make sure their automated personal data systems did not violate the privacy of individual data subjects as defined. Of greatest importance, from our point of view, the safeguards we will recommend give the courts a reliable and generally applicable basis for protecting personal privacy in relation to record keeping*" (Miller, 1973, p. 44). Disponível em: MILLER, Arthur R. ***Records, Computers, and the Rights of Citizens***. https://www.justice.gov/opcl/docs/rec-com-rights.pdf

[59] Parágrafo 14º: *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.*

No cenário da proteção de dados no Brasil, Bioni (2022, p. 41) aponta que o princípio de *accountability* foi delineado a partir das discussões entre os anos de 2016 e 2018, com a aprovação do Projeto de Lei n.º 4.060/2012[60], o que mudou substancialmente o entendimento e a conceituação acerca da responsabilidade civil, alterando a lógica da reparação[61] para a **prevenção de danos**, a qual priorizou a junção dos termos de prestação de contas e responsabilização. Conforme podemos observar no artigo 6º, inciso X, da lei brasileira:

> [...] responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, 2018).

Nessa direção, o texto da LGPD foi aprofundado visando criar critérios norteadores para a elaboração de boas práticas e outros instrumentos, para que os agentes de tratamento possam demonstrar, por meio de ações e manutenção de registros. Bioni (2022, p. 42), por sua vez, destacou a mudança de uma perspectiva genérica de riscos das atividades para o que seria a implementação de programas de governança. Como podemos observar nas obrigações dispostas no artigo 50, a saber:

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas

---

[60] Bioni (2022, p. 38-40) estruturou em uma linha do tempo as fases de desenvolvimento da LGPD. Totalizando 9 fases, entre os anos de 2010 a 2019. A fase 4, compreende os anos de 2016 a 2016, em que a Câmara dos Deputados aprovou a PL 4.060/2012 e o texto foi enviado ao Senado, onde tramitou como PLC 53/2018.

[61] Conforme levantado pela plataforma Observatório, que realiza o monitoramento, resgate e análise dos debates sobre o tema da privacidade e proteção de dados no Brasil. Identificou a mudança relevante, a partir do projeto de lei 4.060/2012 (e outros acontecimentos como os fatos sobres a espionagem americana em 2013 e a aprovação do Marco Civil da Internet em 2014) para se ter uma "racionalidade precaucionária" do princípio de responsabilidade, unindo-o ao princípio de prestação de contas, ainda Disponível em: https://observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/

> operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional (Brasil, 2018).

Além da implementação das boas práticas, o autor (Bioni, 2022) destacou outros instrumentos estabelecidos pela legislação de proteção de dados que configuram práticas visando garantir a responsabilidade e a prestação de contas (*accountability*): o registro das atividades de tratamento dos dados, a implementação do *privacy by design*, a figura do encarregado de dados e o "Relatório de Impacto à Proteção de Dados Pessoais". Destarte, infere-se que o presente princípio, em articulação com os outros analisados nesta seção, afigura-se como elemento basilar para a efetivação de um programa de privacidade e proteção de dados, contribuindo de modo significativo para a avaliação e a autoavaliação da maturidade organizacional.

No contexto dos arquivos, Hurley (2006, p. 237-242) defendeu que o arquivista é também um agente de responsabilidade e que, além de assegurar a qualidade da gestão de documentos, deve orientar-se por normas e boas práticas. A autora ainda (2006, p. 237-242) definiu várias responsabilidades arquivísticas para o profissional, a saber: (1) estabelecer instruções específicas (semilegislativa); (2) definições normas; (3) favorecer a implementação de requisitos; (4) ofertar serviços profissionais; (5) criação de condições para as obrigações relacionadas ao processamento arquivístico; (6) monitoramento o processamento arquivístico;

(7) tomar medidas regulatórias no caso de desvios de conduta; (8) garantia de obediência às normas e regulamentos; (9) fiscalização do uso e avaliações de performance.

Nesse sentido, pretende explorar a implementação de um programa de governança em privacidade e proteção de dados no contexto do gerenciamento de riscos, utilizando como referência o "Guia de Boas Práticas para Implementação" e outras publicações elaboradas pela Autoridade Nacional de Proteção de Dados. Adicionalmente, incorpora as contribuições da segunda versão, que abrangem as sugestões enviadas pelo Arquivo Nacional.

6.2. A gestão de riscos como foco da governança em privacidade e proteção de dados

Abordar os conceitos dos princípios da governança em favor do gerenciamento arquivístico, para aplicação dos procedimentos advindos da Lei Geral de Proteção de Dados, recomenda-se a estruturação de um programa governança em privacidade e proteção de dados, incorpora a gestão de riscos, de forma a conferir a segurança necessária ao alcance dos objetivos organizacionais.

Prevista como obrigações na lei as boas práticas de segurança e de fiscalização, em que determina que os agentes de tratamento (controladores e operadores) formulem regras que devem estabelecer a organização, o funcionamento, os procedimentos de acesso à informação (petições e reclamações), normas de segurança, padrões técnicos, ações de conscientização e treinamento, além de mecanismos de supervisão e mitigação de riscos, entre outros aspectos para o correto tratamento de dados pessoais (Brasil, 2018).

A aplicação de regras de segurança e boas práticas é tida como uma das partes centrais da lei, nesse cenário, os agentes de tratamento devem considerar a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados. Ademais, devem também considerar a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados (Brasil, 2018).

A LGPD determina que a implementação de um programa de governança em privacidade e proteção de dados deve levar em conta a segurança, por meio da utilização de medidas técnicas e administrativas para a proteção das informações pessoais contra acessos não autorizados e situações ilícitas, bem como perdas, alterações ou comunicações indevidas, e também a aplicação de ações preventivas à ocorrência de danos causados em virtude do tratamento de dados.

Nesse cenário, é crucial ressaltar que torna se indispensável a adoção de programa eficaz de gestão de documentos para assegurar o adequado gerenciamento dos riscos associados aos tratamentos de dados pessoais. Desse modo, a gestão de documentos, se configura no conjunto de procedimentos e operações técnicas referentes à sua produção, a tramitação, o uso adequado, a avaliação e o arquivamento, seja em fase corrente e intermediária, objetivando a sua eliminação ou ainda o recolhimento para guarda permanente (Brasil, 1991).

Por meio dele, é possível identificar com precisão os documentos que são produzidos e acumulados pela organização no exercício das suas funções e atividades, assegurando, por exemplo, os princípios de finalidade, adequação e necessidade. Ademais, uma boa gestão de documentos possibilita a classificação e análise dos conjuntos documentais, garantindo o mapeamento das informações pessoais e sensíveis. Esse mapeamento consiste na importante etapa para a aplicação de critérios técnicos que definem o controle e as restrições de acesso às informações. Outro benefício de uma gestão de documentos eficiente é a avaliação para estabelecer de prazos e condições de guarda, que direciona a destinação final dos documentos, seja para a transferência, recolhimento ou sua eliminação. Essas últimas garantem a observância aos princípios como transparência, livre acesso, segurança, responsabilização e a prestação de contas.

Ao implementar um programa de governança em privacidade e proteção de dados, a LGPD determina padrões mínimos que se deve ter, a saber:

> a) demonstre o comprometimento do controlador em **adotar processos e políticas internas** que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja a**plicável a todo o conjunto de dados pessoais que estejam sob seu controle**, independentemente do modo como se realizou sua coleta; c) seja **adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados**; d) **estabeleça políticas e salvaguardas** adequadas com base em processo de **avaliação sistemática de impactos e riscos à privacidade**; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de **atuação transparente e que assegure mecanismos de participação do titular**; f) esteja integrado a sua estrutura geral de governança e estabeleça e **aplique mecanismos de supervisão internos e externos**; g) conte com **planos de resposta a incidentes** e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de **monitoramento contínuo e avaliações periódicas**; II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o **cumprimento de boas práticas ou códigos de conduta**, os quais, de forma independente, promovam o cumprimento desta Lei (Brasil, 2018. Grifos nossos).

Para tanto, a Administração Pública, preocupada com o cumprimento regulatório, desenvolveu o "Guia de Elaboração de Programa de Governança em Privacidade", utilizando-se de outras referências para disseminar o conhecimento em relação à privacidade e segurança da informação e orientar as organizações na estruturação de um programa de governança em privacidade e proteção de dados. Nesse sentido, o guia destacou que a governança, além de cumprir com as exigências, inclui as estratégias, habilidades, pessoas, processos e ferramentas que os órgãos e entidades precisam prover para conquistar a confiança das pessoas.

Outrossim, o guia também abordou, como definição do controle n.º 21 da seção **Governança** – diferente de um projeto que possui início, meio e fim –, que este "estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos de impacto à privacidade e melhorias contínuas na maturidade" (MGI, 2024, p. 8). Entretanto, pode-se criar outros projetos para alcançar os objetivos do programa de privacidade, indica-se selecionar uma metodologia que abrange a definição dos objetivos, as metas e os indicadores; os líderes responsáveis por cada frente de atuação dos projetos, observando as interações com outras áreas e a participação da sociedade; e, os canais de comunicação com os líderes, cidadãos, com os operadores e também com a Autoridade Nacional de Proteção de Dados (MGI, 2024, p. 11).

De acordo com o guia, um programa de governança em privacidade estrutura-se em três etapas: **iniciação e planejamento, construção e execução, e monitoramento**. A primeira etapa visa compreender as informações iniciais sobre a organização, com o alinhamento de expectativas e o envolvimento da alta administração, priorizando, ainda, estratégias que ofereçam efetividade e economicidade. Nessa fase, realiza-se a análise da maturidade organizacional, que busca avaliar e gerenciar o nível de proteção em Privacidade e Segurança da Informação. Este momento também envolve a estruturação e direcionamentos do programa de governança e a definição do nome do encarregado pelo tratamento de dados, incluindo o mapeamento de documentos e processos para elaboração dos inventários e adequação de contratos que contenham dados pessoais (MGI, 2024, p. 11-19). Em relação a mapeamento e inventários dos dados, o "Guia de Elaboração de Programa de Governança em Privacidade", destacou que:

> [...] o Inventário de Dados Pessoais representa documento primordial no sentido de documentar o tratamento de dados pessoais realizados pela

> instituição, em alinhamento ao previsto pelo art. 37 da LGPD. O inventário consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles. [...]o inventário permitirá atender tanto o requisito de manter um registro das operações de tratamento de dados pessoais, quanto o de auxiliar no controle do atendimento aos princípios, ambos estabelecidos pela LGPD. (MGI, 2024, p. 20).

Para o desenvolvimento da segunda etapa do programa (construção e execução), o "Guia de Elaboração de Programa de Governança em Privacidade" compreende que estas são etapas que visam a elaboração de políticas e práticas para proteger a privacidade do cidadão, que destinam garantir que todos os "usos dos dados pessoais sejam conhecidos e adequados às leis, bem como protegê-los contra mau uso ou revelação inadvertida ou deliberada" (MGI, 2024, p. 22). Adicionalmente, nesta etapa identificam-se os responsáveis pelas tarefas de coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais, ou seja, o tratamento de dados. De igual importância, neste momento, o desenvolvimento de ações educativas, como as de conscientização e treinamentos, que abordam os direitos à privacidade e ao acesso à informação, para a construção de uma cultura de segurança e proteção de dados e privacidade.

A propósito, o guia aborda a importância de uma cultura de segurança e proteção de dados e privacidade, utilizando o conceito de *Privacy by Design (PbD)*, desenvolvido por Cavoukian (2009), que considera a privacidade durante todo o ciclo de um projeto, desde a sua concepção. Este conceito determina sete princípios fundamentais a serem considerados, a saber:

> **Proativo, e não reativo; preventivo, e não corretivo**: A abordagem de Privacidade desde a Concepção (PdC) antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem, nem oferece soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram. • **Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio**: Busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão. • **Privacidade incorporada ao projeto (design)**: a privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a

> funcionalidade. • **Funcionalidade total**: a PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade, permitindo funcionalidade total com resultados reais e práticos. Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas. Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados: por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim. • **Visibilidade e Transparência**: a PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança. • **Respeito pela privacidade do usuário**: acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados (MGI, 2024, p. 24).

Ainda na segunda etapa, de construção e execução, o guia orienta a elaboração do "Relatório de Impacto à Proteção de Dados". Ressalta-se que este é um instrumento para analisar a conformidade do tratamento de dados e os riscos que podem impactar as liberdades civis e os direitos fundamentais. Além disso, o RIPD visa documentar os registros das medidas de salvaguarda e os mecanismos de mitigação de riscos implementados no programa (MGI, 2024, p. 24).

Concomitantemente, nesta etapa também ocorrem ações que visam estabelecer medidas e políticas de segurança da informação, bem como o desenvolvimento de políticas de privacidade. Essas ações visam procedimentar o art. 6º da LGPD, que determina a verificação do tratamento de dados para fins legítimos, específicos e explícitos; a limitação do tratamento ao mínimo necessário, abrangendo dados pertinentes e proporcionais ao uso; a garantia de acesso transparente aos titulares e com critérios de qualidade dos dados; a definição de critérios de segurança e não discriminação; e a responsabilização e prestação de contas que visem a demonstração da adoção de medidas eficazes em observância à proteção de dados. Além disso, nessa fase também ocorre a adequação das cláusulas contratuais, que impliquem o tratamento de dados pessoais, identificados na primeira fase do programa (MGI, 2024, p. 26).

É importante observar, que nesse cenário possa ocorrer o envolvimento de outros programas e comissões, para assegurar que a conformidade regulatória como programa de integridade e de *compliance.*

O monitoramento caracteriza a terceira etapa do programa de governança em privacidade e proteção de dados, cabendo o acompanhamento da conformidade das diretrizes da Lei Geral de Proteção de Dados. Essa é uma etapa contínua e cíclica, essencial para a sustentação do programa. O TCU (2020, p. 70) destacou que as ações de monitoramento estão relacionadas aos mecanismos de estratégias e suas práticas, devendo ser atualizadas considerando os aprendizados organizacionais e as mudanças no ambiente. Ademais, a gestão de riscos[62] também deve estar integrada ao planejamento, à execução e ao monitoramento nos diversos níveis organizacionais.

A *ISO* 27005 (2023, p. 5) define o processo de gestão de riscos como "aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação[63], análise[64], avaliação [probabilidade][65], tratamento[66], monitoramento e análise crítica dos riscos". Em termos práticos, a gestão de riscos refere-se a:

> a) **definir e implementar a estrutura de gestão de riscos**. A estrutura exige o comprometimento da liderança com a gestão de riscos, por meio de uma política. De acordo com a ISO 31.000:2018, os objetivos e o comprometimento com a gestão de riscos devem ser formalizados numa política, declaração ou outras formas que incluam: o propósito da organização para gerenciar riscos e vínculos com seus objetivos e outras políticas; reforço da necessidade de integrar a gestão de riscos na cultura global da organização; integração da gestão de riscos nas atividades principais e na tomada de decisão; atribuição de autoridades e responsabilidades; comprometimento com a disponibilização de recursos (pessoas, métodos, ferramentas, sistemas de informação, necessidades de treinamento); a maneira pela qual os objetivos conflitantes são tratados; • formas de medição e reporte no âmbito dos indicadores de desempenho da organização; análise crítica e melhoria [...]; b) **estabelecer as funções** da segunda linha (facilitação, apoio e monitoramento das atividades de gestão

[62] Consideram-se riscos como "efeito da incerteza nos objetivos" (ABNT NBR ISO/IEC 27005:2023).
[63] **Identificação dos riscos** é um processo para encontrar, reconhecer e descrever riscos (ABNT NBR ISO/IEC 27005:2023, p.19).
[64] A **análise de riscos** tem o objetivo de determinar o nível dos riscos. (ABNT NBR ISO/IEC 27005:2023, p. 23).
[65] A **avaliação dos riscos consiste** na comparação dos resultados da análise de riscos com os critérios de risco (ABNT NBR ISO/IEC 27005:2023, p. 26).
[66] O **tratamento de riscos** de segurança da informação fundamenta-se nos resultados do processo de avaliação de riscos na forma de um conjunto priorizado de riscos a serem tratados, com base em critérios de risco (ABNT NBR ISO/IEC 27005:2023, p. 28).

> de riscos) [...] c) **implantar o processo de gestão de riscos**, que deve ser incorporado aos demais processos organizacionais, a começar do planejamento estratégico, de forma a subsidiar a tomada de decisão e assegurar o alcance dos objetivos, sejam eles estratégicos, operacionais, específicos de um projeto, processo, função, serviço, produto, ativo, ou programa; d) **gerenciar os riscos críticos**. Os riscos críticos (aqueles com potencial de impacto significativo nas operações e nos resultados) devem ser avaliados com precisão e os respectivos planos de mitigação devem ser monitorados [...]; e) **implementar um processo de gestão de continuidade de negócios**, para se preparar e reduzir os efeitos de possíveis incidentes que tenham o potencial de interromper as atividades da organização, sejam provocados pelo homem (p.ex.: ataques terroristas) ou naturais (p.ex.: incêndios, inundações, terremotos, furacões e pandemias (TCU, 2020, p. 72 - 75. Grifos nossos).

De acordo o "Guia de Elaboração de Programa de Governança em Privacidade" (2024, p. 28) os marcos da etapa de monitoramento, incluem registros e análise das informações, e ainda, a elaboração de outros relatórios para a prestação de contas e transparência dos resultados. Nesse sentido, o documento destacou a respeito dos desenvolvimentos e análises de indicadores de desempenho, gerais e específicos, conhecido como *KPI's (Key Performance Indicator)*, necessários para medir e avaliar o progresso dos objetivos propostos, que se destinam a avaliar evolução das ações e resultados obtidos, bem como fortalecer a cultura de privacidade e proteção dos dados.

A gestão de incidentes também é recomendada no sentido garantir o registro das informações referente aos incidentes de segurança ocorridos que conste: o armazenamento das informações e dos sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a segurança das informações, os riscos e as medidas para mitigação deles (MGI, 2024, p. 29).

Para visualização, o quadro a seguir estrutura em colunas a organização das três etapas propostas pelo Guia de Elaboração de Programa de Governança em Privacidade, cujo qual é possível compreender o desenvolvimento de cada etapa em um programa.

Quadro 9 - Etapas da Elaboração para o Programa de Governança em Privacidade

1º ETAPA **Iniciação e Planejamento**	**2º ETAPA** **Construção e Execução**	**3º ETAPA** **Monitoramento**
Atuação do Encarregado	Atuação do Encarregado	Atuação do Encarregado
Alinhamento de Expectativas com a Alta Administração	Desenvolvimentos de políticas e práticas para proteção da privacidade do cidadão	Indicadores de Performance de desempenho *(KPI's)*

Maturidade da Organização	Cultura de segurança e proteção de dados e Privacidade desde a Concepção (privacy by design)	Gestão de Incidentes
Análise e Adoção de Medidas de Segurança	Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	Análise e Reporte de Resultados a organização e a sociedade
Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais	Medidas e Política de Segurança da Informação e Política de Privacidade	Medidas de segurança técnicas e administrativas
Mapeamento e Inventário de Dados Pessoais	Adequação Cláusulas Contratuais (Gestão de Contratos; Termo de Uso e Política de Privacidade	Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Fonte: elaboração própria, baseados no Guia de Elaboração de Programa de Governança em Privacidade (2024)

Nota-se que embora a gestão de riscos permeia diversos momentos durante o desenvolvimento do programa, é importante ressaltar que, sua sustentação se concretiza de forma mais evidente na terceira etapa, durante o monitoramento, como podemos observar em destaque na gestão de incidentes de segurança, nas análises de reporte de resultados a organização e a sociedade, nas implementações de medidas de seguranças técnicas e administrativas, ou ainda, na elaboração dos relatórios de impactos à proteção de dados pessoais. Além disso, observa-se também a figura do encarregado pelo tratamento de dados atuando em todas as etapas do programa.

No contexto da gestão de riscos, a importância dos registros e informações documentadas é destacada pela norma *ISO* 27005 (2023, p. 42), que complementa a *ISO* 27001 (2022, p. 7). De acordo com a norma, a organização deve assegurar a atualização e o controle dos registros e documentação para o bom aproveitamento dos processos no sistema de gestão de segurança da informação.

Nessa direção, Díaz, Mujica e Valentim (2018, p. 2652) propôs analisar a relação entre a gestão de documentos em cenários de governança da informação e a gestão de riscos associados aos documentos. O foco da análise residiu no contexto do governo aberto, em face à ineficiência da administração pública na prestação de contas, considerando os seguintes aspectos: a democratização da internet e a consequente perda de controle no processamento de documentos; a complexidade na adoção de sistemas de gestão; os escândalos e fraudes organizacionais; e o não cumprimento das regulamentações relativas aos processos de eliminação de documentos.

Um dos modelos identificados foi o Modelo de Maturidade de Governança da Informação / Princípios Geralmente Aceitos de Manutenção de Registros – Governança da

Informação *(GARP-IG)*[67] publicado nos Estados Unidos, em 2009, pela *ARMA International*[68], que visa avaliar a gestão de documentos, nos diferentes suportes. Pode ser aplicado tanto em organizações públicas quanto privadas, independente do porte, baseando-se nas aplicações das boas práticas das *ISO*:15489, o *MoReq2*, entre outras. O modelo visa a conscientização dos padrões e princípios para o desenvolvimento de sistema de gestão de documentos, possibilitando a partir dele a descrição e mensuração dos atributos essenciais, observando os riscos e elaboração de medidas organizacionais (Díaz; Mujica; Valentim, 2018, p. 2658).

O modelo desenvolvido a partir da estrutura conceitual *"Information Governance Reference Model (IGRM)*[69]" inclui a avaliação dos riscos, e sua maturidade ou apetite a riscos pode ser definida a partir da identificação e análise dos oito princípios destinados à gestão de documentos e informações, propostos para determinar os níveis de maturidade, sendo eles: **responsabilidade** *(accountability)*, **transparência** *(transparency)*, **integridade** *(integrity)*, **proteção** *(protection)*, **conformidade** *(compliance),* **disponibilidade** *(availability)*, **retenção** *(retention)* **e descarte** *(disposition)*.

Nesse sentido, pode-se associá-los aos níveis propostos a fim de verificar a maturidade da gestão de documentos (Díaz; Mujica; Valentim, 2018, p. 2659). O **primeiro nível (1)** refere-se a organizações com baixa preocupação com a gestão de documentos, resultando em potencial descumprimento de exigências legais e regulatórias, considerada como “abaixo do padrão”. O **segundo nível (2**) indica algum desenvolvimento da organização nos aspectos da gestão de documentos, porém, apresentam vulnerabilidade, nesses casos consideram que se “em desenvolvimento”. O **terceiro nível (3)** refere-se a um nível “essencial”, em que se desenvolvem requisitos para atendimento dos regulamentos, mas que ainda podem estar perdendo oportunidades. O **quarto nível (4)** caracteriza um ambiente mais “proativo”, no qual há existência um programa de governança com ações integradas às decisões de rotina, aproveitando a oportunidade devido ao seu nível de maturidade. E, por fim, o **quinto nível (5)** refere-se a um ambiente com um bom nível de maturidade, em que existe governança

---

[67] Definição em inglês: *Information Governance Maturity Model / Generally Accepted Recordkeeping Principles – Information Governance*. Disponível: http://nextlevel.arma.org

[68] *ARMA International* (antiga Associação de Gestores de Arquivos e Administradores) é uma associação profissional sem fins lucrativos de gerentes de arquivos e informações e profissionais e fornecedores de setores relacionados.

[69] O *Information Governance Reference Model (IGRM) desenvolvido pelo EDRM,* fornece uma estrutura para definir uma abordagem de governança unificada para informações, mostrando a ligação entre valor e dever para com os ativos de informação. Disponível: https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

integrada em sua infraestrutura e processos organizacionais, conformidade regulatória e satisfação do cliente, configurando a um grau "transformacional"[70] (Díaz; Mujica; Valentim, 2018, p. 2659).

Na análise crítica desse modelo, o autor salientou a respeito das principais vantagens e desvantagens no contexto de implementação organizacional. Utilizou-se de indicadores que correspondem aos aspectos "**origem, audiência, cobertura, conteúdos, processos/formato, recursos, acessibilidade e compatibilidade, usabilidade e enfoque de avaliação**" (Díaz; Mujica; Valentim, 2018, p. 2663). A respeito da **procedência** o modelo fora projeto por organização líder em gestão de documentos, quanto a abrangência de aplicabilidade o modelo se mostrou flexível ao tipo de organização, podendo ser aplicado tanto no cenário público quanto privado. No que concerne a **cobertura**, destacou que o modelo *GARP-IG*, abrange além da gestão de documentos, a gestão da informação, ressaltando que:

> [...] à gestão de ativos de informação, ou seja, também consideram os processos que envolvem a gestão documental, como o correio eletrônico, o conteúdo da Web, dados do negócio, imagens, vídeos e outros tipos de conteúdos, tanto em formato físico quanto digital (Díaz; Mujica; Valentim, 2018, p. 2664).

No entanto, pode-se notar que, diferente da aplicação de outros modelos, este tem sua abordagem pautada no "Ciclo de Vida dos Documentos", cujas fases dicotômicas do processo

---

[70] Tradução em inglês: *The Electronic Discovery Reference Model (EDRM): Maturity Model: Levels of Effective Information Governance6 Level 1 (Sub-standard): This level describes an environment where recordkeeping concerns are either not addressed at all, or are addressed in a very ad hoc manner. Organizations that identify primarily with these descriptions should be concerned that their programs will not meet legal or regulatory scrutiny. Level 2 (In Development): This level describes an environment where there is a developing recognition that recordkeeping has an impact on the organization, and that the organization may benefit from a more defined information governance program. However, in Level 2, the organization is still vulnerable to legal or regulatory scrutiny since practices are ill-defined and still largely ad hoc in nature. Level 3 (Essential): This level describes the essential or minimum requirements that must be addressed in order to meet the organization's legal and regulatory requirements. Level 3 is characterized by defined policies and procedures, and more specific decisions taken to improve recordkeeping. However, organizations that identify primarily with Level 3 descriptions may still be missing significant opportunities for streamlining business and controlling costs. Level 4 (Proactive): This level describes an organization that is initiating information governance program improvements throughout its business operations. Information governance issues and considerations are integrated into business decisions on a routine basis, and the organization easily meets its legal and regulatory requirements. Organizations that identify primarily with these descriptions should begin to consider the business benefits of information availability in transforming their organizations globally. Level 5 (Transformational)7: This level describes an organization that has integrated information governance into its overall corporate infrastructure and business processes to such an extent that compliance with the program requirements is routine. These organizations have recognized that effective information governance plays a critical role in cost containment, competitive advantage, and client service.*

documental são claramente diferenciadas. Diferentemente de alguns fundamentos teóricos que compreendem a gestão de documentos a partir do conceito integrado do documento e que inclusive abordam o seu valor permanente (Díaz; Mujica; Valentim, 2018, p. 2664).

Em relação aos **processos** de coleta das informações para avaliação da maturidade, o *GARP-IG*, acontece por meio de aplicação de questionários, sob um viés qualitativo, que avalia as características particulares de cada nível a partir dos princípios, e posteriormente realizam-se cálculos por meio de combinações de elementos. No entanto, observou como uma desvantagem a falta de descrição dos **recursos** envolvidos no processo de avaliação (Díaz; Mujica; Valentim, 2018, p. 2665).

A respeito da **usabilidade**, o *GARP-IG* apresentou procedimentos articulados e lógicos sobre as fases de implantação do modelo, orientando os usuários de forma confiável, e o produto é de fácil acesso em site oficial. Contudo, Díaz, Mujica e Valentim (2018, p. 266) destacaram dois fatores de desvantagem para a aplicabilidade do modelo no cenário brasileiro, quanto à sua limitação: a falta de aplicabilidade de recursos tecnológicos e os procedimentos oferecidos apenas em inglês. Por fim, no que tange ao enfoque de avaliação, o modelo não dispõe de papéis de responsabilidade arquivística para a execução do diagnóstico. Todavia, é importante ressaltar que o modelo *GARP-IG* dispõe de métodos para aprofundar nos critérios de avaliação do diagnóstico. Além disso, o modelo também tem seu foco na análise de riscos relacionados às boas práticas para acesso aos documentos e informações, contribuindo para uma visão do contexto interno e externo, bem como para a avaliação razoável da maturidade organizacional (Díaz; Mujica; Valentim 2018, p. 2667-2668).

Nesse sentido, destaca-se sobre os alinhamentos e objetivos organizacionais, com definições e requisitos que inclusive, se alinha aos princípios da governança, e que buscam garantia a avaliação de indicadores, com vistas à gestão de riscos, como a última etapa desse processo, com foco no acesso e a prestação de contas.

Figura 6 - Avaliação da Maturidade de Governança da Informação e de Documentos para a Gestão de Riscos

Fonte: Elaboração própria, 2025

A figura 6 evidencia o fluxo dos principais pontos destacados pelo autor em seu modelo de diagnóstico de maturidade *GARP-IG*. Ela orienta a identificação de práticas e estratégias que visam à mensuração e avaliação dos atributos da maturidade organizacional, com foco na gestão de documentos que impactam diretamente a governança e o gerenciamento arquivísticos. Nesse sentido, destacam-se os alinhamentos e objetivos organizacionais, com definições e requisitos que, inclusive, se alinham aos princípios da governança, os quais buscam avaliar os indicadores na perspectiva da gestão de riscos como a última etapa desse processo, com foco no acesso e na prestação de contas.

Portanto, a gestão de riscos configura-se um pilar essencial de um programa de governança em privacidade e proteção de dados, conforme preconizado pela Lei Geral de Proteção de Dados. Ela abrange desde o planejamento inicial e a avaliação da maturidade organizacional até o desenvolvimento de políticas e o monitoramento contínuo, visando à identificação e a mitigação de riscos, assegurando os princípios da boa governança.

7 CONSIDERAÇÕES FINAIS

A pesquisa se desenvolveu tendo como ponto de partida a Lei Geral de Proteção de Dados, aprovada em 2018 e criada para proteger os direitos fundamentais dos indivíduos à liberdade, à privacidade e à livre formação da personalidade. Inspirada no regulamento europeu, a *General Data Protection Regulation (GDPR)*, a LGPD versa sobre o tratamento de dados pessoais realizados por pessoas físicas e jurídicas de direito público e privado, abrangendo um amplo conjunto de operações tanto em meios manuais quanto digitais.

A lei brasileira estabelece condições nas quais os dados e informações pessoais devem ser tratados, a partir de um conjunto de direitos para os titulares dos dados, gerando obrigações relacionadas a uma série de procedimentos e normas e que também se relaciona com princípios da governança. Nesse sentido, observando a proximidade e aplicabilidade dos arquivos, em favor da colaboração, da prestação de contas, da responsabilidade e da transparência.

A pesquisa se propôs a analisar e refletir acerca da possibilidade de o arquivista assumir funções como membro de comitês de governança ou de encarregado pelo tratamento de dados para a implementação de programas de governança em privacidade e proteção de dados, destacando, ainda, a avaliação da maturidade organizacional e o desenvolvimento de indicadores pertinentes à gestão de riscos e à eficaz prestação de contas conforme as exigências legais. Dessa maneira, a pesquisa buscou responder à pergunta central: **de que maneira o conhecimento e a colaboração do arquivista podem contribuir para a conformidade da Lei Geral de Proteção de Dados, considerando, aspectos do gerenciamento arquivístico e da governança arquivística?** Para tanto, numa abordagem qualitativa e exploratória, objetivou-se compreender os princípios fundamentais da LGPD, investigar os aspectos da governança arquivística a partir dos princípios da transparência, prestação de contas e responsabilidade, correlacionando-os com as diretrizes da lei e, ainda, avaliar as competências necessárias para que o arquivista possa atuar como mediador da gestão de riscos em um programa de privacidade e proteção de dados.

Na segunda seção, a pesquisa tratou da evolução das leis de privacidade, considerando o contexto da expansão das tecnologias, o que ampliou e facilitou a comunicação e o acesso à informação. Em contrapartida, observou que aumentaram as preocupações e as fragilidades contemporâneas em relação à privacidade, bem como os impactos da economia dos dados e o processo de *commoditização* destes. A partir da perspectiva de autores analisados, foi

identificada a dinâmica de um possível gerenciamento de dados e informações centrado no indivíduo, no qual a pessoa se torna a detentora de suas informações pessoais.

Em seguida, a pesquisa apresentou a conceituação da privacidade como um direito fundamental. Apesar da falta de consenso para o termo, foi possível observar a respeito da sua evolução, e a relação com outros direitos positivados na Constituição Federal de 1988. Evoluindo do que antes era considerado referência da vida privada e do isolamento (inclusive para a obtenção de privilégios) à evolução da independência e da intimidade, e os desenvolvimentos aos chamados direitos da personalidade, bem como as garantias existentes em outros ordenamentos jurídicos, a exemplo do Código Penal e no Código Civil.

Ademais, a pesquisa buscou analisar a privacidade sob a perspectiva de suas implicações a partir de transformações sociais, políticas e econômicas, como pano de fundo para o desenvolvimento da proteção de dados atualmente. Para isso, procurou compreender a evolução de outros direitos incorporados à Constituição Federal, como o *habeas data* e o acesso à informação, e como os possíveis conflitos entre esses direitos podem ser determinantes para o gerenciamento arquivístico.

A pesquisa também evidenciou o surgimento do conceito de autodeterminação informativa. Embora o termo figure na Lei Geral de Proteção de Dados sem apresentar uma definição mais detalhada, sua análise permitiu elucidar a origem (estrangeira), a partir da jurisprudência alemã, bem como sua evolução até os dias atuais, estando positivado na Constituição Federal de 1988.

De modo estratégico, a pesquisa analisou as leis de privacidade no mundo, tendo como ponto de partida as relações e os impactos no cenário brasileiro. Observando os debates e as discussões a respeito dos limites individuais e dos interesses coletivos, bem como o empenho dos Estados para o desenvolvimento de leis de proteção de dados e a defesa dos indivíduos contra invasões arbitrárias. Para tanto, propusemos a compreensão de quais critérios os Estados estão adotando para que as atividades comerciais e sociais, e também para que o fluxo transfronteiriço de dados, aconteçam de forma justa, transparente e igualitária, favorecendo as relações multilaterais. Nesse sentido, foram avaliadas ações de organizações como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), bem como suas resoluções e normativas acerca da proteção de dados. Além disso, também foi analisada a harmonia entre blocos econômicos como o Mercosul e grupos de países emergentes como o BRICS.

A respeito da proteção de dados no Brasil, a pesquisa se dispôs a avaliar, na seção três, os desdobramentos do direito no país até sua definição como direito fundamental, concretizada pela Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Essa emenda alterou a Constituição Federal, incluindo a proteção de dados pessoais entre os direitos e garantias fundamentais, evidenciando as fases de maturação de pautas que tratam de informações acerca do tema. Foi possível observar que a inclusão dos princípios de responsabilização e de prestação de contas não foi por acaso. Houve um cuidado para que as organizações adotassem medidas para demonstrar suas responsabilidades. Em concordância com isso, a criação de uma autoridade como autarquia especial, com atuação independente, favoreceu a atuação da ANPD para a fiscalização também do setor público.

A quarta seção da pesquisa teve como objetivo específico avaliar as competências necessárias para que o arquivista possa atuar como mediador da gestão de riscos na implementação de programas de privacidade e proteção de dados. Esse ponto da pesquisa buscou compreender, a partir dos cursos de Arquivologia no Brasil, a evolução do profissional, identificando suas competências humanas e profissionais necessárias ao desenvolvimento das atividades. Buscou ainda o entendimento a respeito das competências arquivísticas e da análise documental de regulamentos que versam sobre o arquivista e a ocupação categorizada pela Classificação Brasileira de Ocupações (CBO), que visa a identificação e atualização das ocupações profissionais. Ademais, traçou-se uma relação comparativa, a fim de encontrar similaridades e convergências com a função do encarregado pelo tratamento de dados, a partir da aprovação, em 2024, da Resolução CD/ANPD n.º 18. Nesse cenário, o encarregado ou *Data Protection Officer* atua como mediador na orientação quanto às melhores práticas de proteção de dados dentro das organizações. Nessa análise comparativa, revelou-se de forma positiva, embora não exaustiva, que ambas as funções possuem semelhanças e convergências importantes, especialmente no que tange ao planejamento, à organização, à orientação e à direção dos serviços arquivísticos para a proteção de dados no que diz respeito às informações.

A penúltima seção desta pesquisa teve como propósito analisar as relações conceituais entre o gerenciamento arquivístico e a governança arquivística, o que requereu uma investigação dos princípios da governança institucional e corporativa, em favor da avaliação da maturidade organizacional. Na proposta inicial, a análise seguiria em relação aos princípios da transparência, da equidade, da prestação de contas e da responsabilidade. Todavia, durante o aprofundamento, observou-se a necessidade de ajustes, optando-se por excluir o princípio

da equidade, pela sua natureza subjacente às práticas arquivísticas, permeando-as de maneira implícita, e a opção pela inclusão do princípio da integridade, uma vez que fora acrescido após ter ganhado relevância no Brasil a partir de 1995 e não constava nos objetivos iniciais desta pesquisa. Nesse cenário, os princípios foram analisados, com foco na governança, como o conjunto de mecanismos de liderança, estratégias e controle, bem como suas práticas para a avaliação, o direcionamento e o monitoramento do gerenciamento. Com vistas à condução da prestação de serviço ao interesse da sociedade, em conformidade regulatória. A partir disso, analisaram-se brevemente esses elementos no contexto arquivístico, considerando sua natureza administrativa, jurídica, informacional, probatória, orgânica e cumulativa. Buscou-se examinar regulamentos nacionais e internacionais que discorrem sobre tais princípios e suas relações com os direitos fundamentais de acesso à informação e privacidade. Avaliaram-se também as restrições e orientações de acesso a dados com informações pessoais, bem como as normas de boas práticas que oferecem medidas organizacionais para a aplicação destes princípios.

Como resultado, foi possível também uma compreensão acerca da prestação de contas e da responsabilidade arquivística, o que favoreceu o entendimento sobre a responsabilização (*accountability*). Este conceito, na proposta inicial, mostrou-se amplo e com pouca definição. Apesar da pouca explicação a respeito do termo em inglês, a pesquisa evidenciou sua origem e sua relação com as chamadas práticas informacionais justas. Isso garante que, para além da manipulação de dados no uso legítimo das obrigações, as organizações devem garantir também os resultados, bem como a necessidade de salvaguardas e medidas adequadas para a proteção dos dados pessoais. Nessa lógica, a tecnologia precisa ser parte da solução e não o contrário.

Em seguida, a pesquisa se propôs a relacionar os princípios com a responsabilidade arquivística, considerando o arquivista como agente na implementação de programas de governança em privacidade e proteção de dados. Como parte final da seção, a pesquisa buscou analisar a gestão de riscos como foco essencial para a governança no contexto dos arquivos, considerando o art. 50 da LGPD, que estabelece diretrizes e obrigações para regras de segurança e aplicação de boas práticas. Essas regras foram definidas para a organização e seu funcionamento, os procedimentos de acesso à informação pelo titular dos dados, as ações educativas sobre a proteção de dados e, ainda, a supervisão e a mitigação dos riscos que ofereçam perigo aos direitos fundamentais das pessoas.

Em face disso, a pesquisa analisou, a partir do Guia de Elaboração de Programa de Governança em Privacidade, a estrutura de um programa de governança nas organizações, que se baseava em três etapas: (1) iniciação e planejamento, (2) construção e execução, e (3) monitoramento. Como resultado, foram evidenciados os usos de metodologia e normas, como a utilização das normas *ISO's*, conhecidas e aplicadas em arquivos, e outras menos comuns, como o uso da metodologia de *Privacy by Design*, a qual tem sua abordagem em um conjunto de princípios que visam garantir a privacidade desde a concepção e a sua manutenção durante todo o ciclo de um projeto, programa, produto ou serviço, como também é determinado no segundo parágrafo do art. 46 da LGPD.

Quanto ao monitoramento, a terceira etapa do programa de governança em privacidade, a pesquisa analisou a conformidade das diretrizes em um ciclo contínuo, a partir de mecanismos de controle que configuram a gestão de riscos. De forma sistemática, essa gestão considera o estabelecimento de políticas e procedimentos em favor da identificação do risco (o processo de encontrar, reconhecer e descrevê-lo), da análise dos riscos (que determina os critérios), da avaliação e do tratamento dos riscos, utilizando, neste último, medidas de segurança da informação que fundamentam o seu tratamento.

Por último, no âmbito da governança e do gerenciamento arquivísticos, analisou um modelo de maturidade de governança desenvolvido pela ARMA International. Mesmo proposto em um cenário internacional, esse modelo, o Modelo de Maturidade de Governança da Informação / Princípios Geralmente Aceitos de Manutenção de Registros – Governança da Informação (GARP-IG), demonstrou ser aplicável a organizações privadas e públicas de qualquer porte. Foi considerando a avaliação e o apetite a riscos para a gestão de documentos, identificando princípios de forma bastante semelhante aos princípios gerais de governança. Fica evidente, portanto, que um programa de gestão de documentos eficiente é fundamental para o desenvolvimento de um bom gerenciamento e governança arquivística.

A pesquisa se debruçou na análise dos resultados dos questionários e buscou uma amostra que fosse representativa, tendo em vista que poderíamos encontrar poucos profissionais atuando na área de proteção de dados. De forma muito positiva, tivemos um retorno expressivo, considerando o tempo em que a pesquisa ficou disponível (um mês), o que possibilitou a compreensão da atuação desses profissionais ocupando cargos dentro de comissões e na função de encarregado pelo tratamento de dados.

Por fim, ressalta-se a relevância de futuras pesquisas sobre a proteção de dados, com ênfase na criação de indicadores para avaliar a maturidade da implementação da LGPD no

contexto brasileiro. Esses estudos poderiam explorar a relação entre os procedimentos de proteção de dados e a garantia do acesso à informação. Adicionalmente, enfatiza-se a importância de que os profissionais arquivistas busquem um processo contínuo de aquisição de conhecimento para poderem ocupar espaços estratégicos, promovendo o acesso pleno aos arquivos, pautados na segurança necessária das informações pessoais, bem como a harmonização no que diz respeito aos direitos fundamentais.

REFERÊNCIAS

ALCASSA, F. DPO: atividade inscrita no CBO, pelo Ministério do Trabalho. **Migalhas**, [*S. l.*], 25 mar. 2022. Disponível em: https://www.migalhas.com.br/depeso/362444/dpo-atividade-inscrita-no-cbo-pelo-ministerio-do-trabalho

ALTOUNIAN, C. S; SOUZA, D. L. de; LAPA, L. R. G. **Gestão e governança pública para resultados:** uma visão prática. 2. ed. Belo Horizonte: Fórum, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:** Gestão de riscos - princípios e diretrizes. Rio de Janeiro: ABNT, 2009. Disponível em: http://www.abntcatalogo.com.br/norma.aspx?ID=57311. Acesso em: 24 mar. 2025.

ARGENTINA. Ley 25.326, octubre 4 de 2000. Protección de los datos personales. Buenos Aires: Congresso Nacional, 2000. Disponível em: https://www.argentina.gob.ar/normativa/nacional/64790/actualizacion.

ARGENTINA. Decreto n. 1.558/2001. Apruébase la reglamentación de la Ley n. 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Buenos Aires, Boletín Nacional, 3 dez. 2001. Disponível em: https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368

ARQUIVO NACIONAL (Brasil). **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro, 2005. (Publicações Técnicas, n. 51). Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/dicionrio_de_terminologia_arquivistica.pdf. Acesso em: 31 mar. 2025.

AUSTRALIAN NATIONAL AUDIT OFFICE. **Public sector governance:** better practice guide. Framework, processes and practices. Canberra: National Institute for Governance, 2003. Disponível em: https://www.anao.gov.au/sites/default/files/Barrett_better_practice_public_sector_governance_2003.pdf. Acesso em: 22 mar. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf . Acesso em: 01 nov. 2024.

BAGATINI, J. A.; GUIMARÃES, J. A. Chaves; SANT'ANA, R. C. Gonçalves. Gerenciamento dos dados pessoais em arquivos: uma perspectiva centrada no indivíduo com base na LGPD**. Acervo,** *[S. l.]*, v. 34, n. 3, p. 1–20, 2021. Disponível em: https://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/1749. Acesso em: 30 out. 2023.

BAHIA, E. M. S. **Competências arquivísticas no mercado de trabalho.** Curitiba: Appris, 2018.

BARROS, G. S.; SILVA, L. S.; SCHMIDT, C. Documentos públicos e dados pessoais: o acesso sob a ótica da lei geral de proteção de dados pessoais e da lei de acesso à informação. **Revista do Arquivo,** São Paulo, v. 5, n. 9, p. 22-39, out. 2019. Disponível em: http://www.arquivoestado.sp.gov.br/revista_do_arquivo/09/artigo_01.php#início deste artigo. Acesso em: 26 mar. 2024.

BELLOTTO, H. L. **Arquivística**: objeto, princípios e rumos. São Paulo: Associação dos Arquivistas de São Paulo, 2002.

BELLOTTO, H. L. **Arquivo**: estudos e reflexões. Belo Horizonte: UFMG, 2014

BELLOTTO, H. L. **Arquivos permanentes:** tratamento documental, 4. ed. Rio de Janeiro. FGV, 2004, p. 301.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil:** promulgada em 5 de outubro de 1988. Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 mar. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CNPD n.º 2, de 26 de setembro de 2024. Estabelece o Regimento Interno do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD). **Diário Oficial da União:** Seção 1, Brasília, DF, p. 92, 30 de set. 2024.

BRASIL. Controladoria-Geral da União. **Modelo de Maturidade em Integridade Pública (MMIP)** [versão 1.0]**.** Brasília, DF: Controladoria Geral da União: 2023. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/12/ministro-da-cgu-anuncia-modelo-de-maturidade-em-integridade-publica/SIPMMIP.pdf . Acesso em: 18 abr. 2025.

BRASIL. Decreto 8.259, 6 de novembro de 1978. Regulamenta a Lei n.º 6.546, de 4 de julho de 1978, que dispõe sobre a regulamentação das profissões de Arquivista e de técnico de Arquivo. **Diário Oficial da União:** Seção 1, Brasília, DF, 5 jul. 1978.

BRASIL. Decreto n.º 11.529, de 16 de maio de 2023**.** Dispõe sobre o Sistema de Integridade, Transparência e Acesso à Informação e a Política de Integridade do Poder Executivo federal. **Diário Oficial da União:** Seção 1, Brasília, DF, ano 161, n. 93, p. 4, 17 maio 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11529.htm. Acesso em: 19 abr. 2025.

BRASIL. Decreto n.º 9.203, de 22 de novembro de 2017**.** Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. **Diário Oficial da União**: Seção 1, Brasília, DF, p. 223, nov. 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm . Acesso em: 05 abr. 2025.

BRASIL. Emenda Constitucional n.º 115, de 10 de fevereiro de 2022**.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de

dados pessoais. **Diário Oficial da União:** Seção 1, Brasília, DF, ano 160, n. 30, p. 2, 11 fev. 2022.

BRASIL. Lei n. 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. **Diário Oficial da União**, Brasília, 13 nov. 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm

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

BRASIL. Lei n. 13.853, de 8 de julho de 2019. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 157, n. 130, p. 1, 9 jul. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União:** Seção 1, Brasília, DF, ano 151, n. 77, p. 1, 24 abr. 2014. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: Seção 1, Brasília, DF, ano 155, n. 157, p. 59, 15 ago. 2018.

BRASIL. Lei n.º 6.546, de 4 de julho de 1978. Dispõe sobre a regulamentação das profissões de Arquivista e de Técnico de Arquivo. **Diário Oficial da União: Seção 1,** Brasília, p. 102965, 5. Jul. 1978. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/1970-1979/l6546.htm. Acesso em 13 out. 2022.

BRASIL. Ministério da Educação. **Diretrizes curriculares para curso de Arquivologia**. Brasília: MEC, Conselho Nacional de Educação, 2001.

BRASIL. Ministério do Trabalho e Emprego. **Classificação Brasileira de Ocupações:** Buscas por Título: Arquivistas e Encarregado pelo tratamento de dados. Brasília: Ministério do Trabalho e Emprego, 2007-2017a. Acesso em 23 de nov. 2024.

BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. Resolução CNPD n.º 1, de 6 de maio de 2022. Estabelece o Regimento Interno do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. **Diário Oficial da União**: Seção 1, Brasília, DF, ano 160, n. 87, p. 2, 10 maio 2022

BRASIL. Resolução CD/ANPD n.º 18, de 16 de julho de 2024. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. **Diário Oficial da União**: Seção 1, Brasília, DF, n. 136, p. 42, 17 jul. 2024.

BRASIL. Resolução n.º 54, de 8 de dezembro de 2023. Estabelece diretrizes e regras para a aplicação da Lei n.º 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos arquivos permanentes custodiados por pessoa física ou jurídica de direito público ou privado. **Diário Oficial da União**: seção 1, Brasília, DF, ano 161, n. 236, p. 84, 13 dez. 2023.

BRASIL. Supremo Tribunal Federal. **Acórdão no Recurso Extraordinário (RE) 418.416/SC**. Relator: Ministro Sepúlveda Pertence. Julgado em 10 maio 2006. Publicado no DJ de 19 dez. 2006. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/14732487. Acesso em: 30 jul. 2025.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança aplicável a órgãos e entidades da administração pública**. Brasília: TCU, 2014.

CAMARGO, Ana Maria de Almeida; BELLOTTO, Heloísa L. (coord.). **Dicionário de terminologia arquivística**. São Paulo: Associação dos Arquivistas Brasileiros - Núcleo Regional de São Paulo: Secretaria de Estado da Cultura, 1996. Acesso em: 30 jul. 2025

CANCELIER, Mikhail V. L. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência:** Estudos Jurídicos e Políticos, Florianópolis, v. 38, n. 76, p. 213–240, 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213. Acesso em: 07 jul. 2023

CARBONE, P. P; BRANDÃO, H. P.; LEITE, J. B. D. **Gestão por competências e gestão do conhecimento**. Rio de Janeiro: FGV, 2005.

CAVOUKIAN, A. **Privacy by design:** the 7 foundational principles: implementation and mapping of fair information practices. Ontario, Canada: Information & Privacy Commissioner of Ontario, 2011.

CHIAVENATO, I. **Introdução à Teoria Geral da Administração:** uma visão abrangente da moderna administração das organizações. 6. ed. Rio de Janeiro. Campus, 2000.

CONSELHO INTERNACIONAL DE ARQUIVOS. Comitê de Boas Práticas e Normas. Grupo de Trabalho sobre Acesso. **Princípios de acesso aos arquivos:** orientação técnica para gestão de arquivos com restrições. Tradução de Silvia Ninita de Moura Estevão e Vitor Manoel Marques da Fonseca. Rio de Janeiro: Arquivo Nacional, 2014. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/principios_acesso_arquivos.pdf. Acesso em: 26 mar. 2024.

CONSELHO INTERNACIONAL DE ARQUIVOS. **Princípios de acesso aos arquivos**. Tradução de Silvia Ninita de Moura Estevão e Vitor Manoel Marques da Fonseca. Rio de Janeiro: Arquivo Nacional, 2012. Acesso em: 26 mar. 2024.

COOK. T. **The Archival appraisal of records containing personal information:** a RAMP study with guidelines. Paris: United Nations Educational, Scientific and Cultural Organization, 1991. Acesso em: 06 mar. 2024. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000090644

CORRÊA, F. G., & MARQUES, A. A. da C. Princípio da territorialidade: trajetórias e definições. **ÁGORA**: Arquivologia em Debate, p.13, 2016. Disponível: https://agora.emnuvens.com.br/ra/article/view/582 . Acesso em: 12 jun. 2024

DELMAS, B. Arquivos servem para quê? *In:* ____. **Arquivos para quê?:** textos escolhidos. Trad. Danielle Ardaillon. São Paulo: Instituto Fernando Henrique Cardoso, 2010, p. 18-20.

DIAZ, M. P.; MUJICA, M. M. M.; VALENTIM, M. L. P. Modelos de diagnóstico de gestão documental em cenários de governança da informação e gestão de riscos. *In*: ENCONTRO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO, 19., 2018, Londrina. **Anais [...]**. Londrina, 2018. Disponível em: http://hdl.handle.net/20.500.11959/brapci/102542. Acesso em: 28 nov. 2023.

DLA PIPER. **Manual de leis de proteção de dados do mundo.** *[S.l.]:* DLA PIPER, 2025. Disponível em: https://www.dlapiperdataprotection.com/. Acesso em: 15 mar. 2025.

DONEDA, D; SARLET, I. W; MENDES, L. S; **Estudos sobre proteção de dados pessoais**. São Paulo: Expressa, 2022. (Coleção Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação).

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periódicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 26 mar. 2024.

EASTWOOD, T.; MACNEIL, H. (org.). **Correntes atuais do pensamento arquivístico.** Belo Horizonte: UFMG, 2016.

EDRM - The Electronic Discovery Reference Model. How the Information Governance Reference Model (IGRM) Complements ARMA International's Generally Accepted Recordkeeping Principles (GARP®). Durham (NC), 2011. 15 p.

EUROPEAN UNION. Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 april 2016. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). **Official Journal of the European Union,** 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04. Acesso em: 26 mar. 2024.

FREITAS, I. A; BRANDÃO, H. P. Trilhas de aprendizagem como estratégia para desenvolvimento de competências. *In:* ENCONTRO DA ASSOCIAÇÃO NACIONAL DOS PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 29., Brasília, 2005. **Resumo dos trabalhos [...]**. Brasília: ANPAD, 2005. p. 2.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2024.

GÓMEZ, M. N. G. O objeto de estudo da ciência da informação: paradoxos e desafios**.** **Ciência da Informação**, v. 19, n. 2, 1990. Disponível em: http://dx.doi.org/10.18225/ci.inf.v19i2.332. Acesso em: 23 maio 2023.

GONÇALVEZ, A. O Conceito de governança. *In:* CONGRESSO NACIONAL DO CONPEDI, 14., 2005, Fortaleza. **Anais [...].** Fortaleza, 2005. Disponível em: https://www.unisantos.br/upload/menu3niveis_1258398685850_alcindo_goncalves_o_conceito_de_governanca.pdf. Acesso em: 13 out. 2022.

GREEN, J. A proteção da privacidade com a abertura plena dos arquivos. **Acervo**, Rio de Janeiro, v. 24, n. 1, p. 205-216, jan./jun. 2011. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/379. Acesso em: 26 mar. 2024.

HABERMAS, Jürgen. Mudança estrutural da esfera pública: investigações sobre uma categoria da sociedade burguesa. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014.

HEYMANN, L. Sobre privacidade, direitos, ética e arquivos, sobre a obra de Heather MacNeil "Sem consentimento: a ética na divulgação de informações pessoais em arquivos públicos". **Acervo**, [*S. l.*], v. 34, n. 1, p. 261–268, 2020. Disponível em: https://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/1707. Acesso em: 30 out. 2023.

HIRATA, A. Direito à privacidade. *In:* CAMPILONGO, C. F. ; GONZAGA, A. A. G.; FREIRE, A. L. (coord.). **Enciclopédia jurídica da PUC-SP.** 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. **(**Tomo: Direito Administrativo e Constitucional). Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 26 mar. 2024.

IACOVINO, L. Os arquivos como arsenais de responsabilidade. *In:* EASTWOOD, T.; MACNEIL, H. (org.). **Correntes atuais do pensamento arquivístico**. Belo Horizonte: UFMG, 2016. p. 262-267

ÍNDIA. Ministry of Law And Justice. The Digital Personal Data Protection Act, 2023. **The Gazette of India,** New Delhi, 11 ago. 2023. Disponível em: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf. Acesso em: 21 mar. 2025.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**. 5. ed. São Paulo: IBGC, 2015. Disponível em: http://www.ibgc. org.br/CodigoMelhoresPraticas.aspx. Acesso em: 21 mar. 2025.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 6. ed. São Paulo: IBGC, 2023. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640&assessment=1. Acesso em: 27 mar. 2024

INTERNATIONAL COUNCIL OF ARCHIVES. **Declaração Universal sobre os Arquivos**. 2009. Disponível em: https://www.ica.org/download.php?id=1484. Acesso em: 6 mar. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000:2018:** Information Technology - Security techniques - Information security management systems - Overview and vocabulary. *[S. l.]*: ISO/IEC, 2018.

JARDIM, J. M. A produção de conhecimento arquivístico: perspectivas internacionais e o caso brasileiro (1990 - 1995). **Ciência da Informação**, v. 27, n. 3, 1998. Disponível em: https://doi.org/10.1590/S0100-19651998000300001. Acesso em: 26 abr. 2025.

JARDIM, J. M. Caminhos e perspectivas da gestão de documentos em cenários de transformações. **Acervo**, Rio de Janeiro, v. 28, n. 2, p. 19-50, jul./dez. 2015.

JARDIM, J. M. Governança arquivística: contornos para uma noção. **Acervo**, Rio de Janeiro, v. 31, n. 3, p. 31-45, 2018. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/987. Acesso em: 26 abr. 2025

JARDIM, J. M. Governança Arquivística: um território a ser explorado. **Revista Arquivo.** São Paulo, ano 2, n. 7, p. 12-23, 2018. Disponível em: https://revista.arquivoestado.sp.gov.br/ojs/revista_do_arquivo/article/view/130/79. Acesso em: 26 abr. 2025

KAWABATA, P. E.; VALENTIM, M. L. P. Competências e habilidades solicitadas em concursos públicos para a atuação profissional do arquivista. **Revista Brasileira de Educação em Ciência da Informação**, São Paulo, v. 2, n. 1, p. 84–116, 2015. Disponível em: https://portal.abecin.org.br/rebecin/article/view/25. Acesso em: 28 set. 2024.

LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2011.

LIMA MARQUES, C; PEREIRA DE LIMA, C. R.; PEROLI DOS REIS, K. A proteção de dados pessoais nos Estados-Membros do Mercosul. **Revista CNJ**, Brasília, v. 7, n. 1, p. 45–56, 2023. Disponível em: https://www.cnj.jus.br/ojs/revista-cnj/article/view/486. Acesso em: 20 fev. 2025.

MACNEIL, H. **Sem consentimento:** a ética na divulgação de informações pessoais em arquivos públicos. Belo Horizonte: UFMG, 2019.

MALUF, I. M. P. **Governança Arquivística Pública Institucional como meio de viabilização e melhoria do gerenciamento arquivístico e da gestão arquivística de documentos:** protótipo para a elaboração de modelo para implementação. 2023. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal de Minas Gerais, Belo Horizonte, Minas Gerais, 2023.

MALUF, I. M. P., & SILVA, W. A. (2024). A noção de governança arquivística no contexto brasileiro: em busca de perspectivas de observação: **ÁGORA**: Arquivologia Em Debate, *34*(68), p. 1–21. 2024. Acesso em: 26 abr. 2025

MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. **Rev. de Ciências Jurídicas Pensar,** v. 25, n. 4, 2020. Disponível em: https://periodicos.unifor.br/rpen/article/view/10828/pdf. Acesso em 18 mar. 2025

MENDONÇA, J. F de; RIELLI, M. A constitucionalização da proteção de dados pessoais no Brasil e a trajetória até a promulgação da PEC 17/2019. **Observatório da Privacidade**, [*S. l.*], 10 fev. 2022. Disponível em: https://observatorioprivacidade.com.br/2022/02/10/a-constitucionalizacao-da-protecao-de-dados-pessoais-no-brasil-e-a-trajetoria-ate-a-promulgacao-da-pec-17-2019/. Acesso em: 29 abr. 2025.

MERCOSUL**. Declaração Especial dos Presidentes do MERCOSUL sobre Democracia e Integridade da Informação em Ambientes Digitais**. [S. l.]: MERCOSUL, [2023]. Disponível em: https://documentos.mercosur.int/public/declaraciones/163. Acesso em: 27 jan. 2025.

MERCOSUL. MERCOSUL/GMC/RES. N.º 36/2019. Defesa do consumidor: princípios fundamentais. Santa Fé, Argentina: Conselho do Mercado Comum, 15 jul. 2019. Disponível em: https://normas.mercosur.int/public/normativas/3767

MERCOSUL. MERCOSUL/GMC/RES. N.º 37/2019. Defesa do consumidor: proteção ao consumidor no comércio eletrônico. Santa Fé, Argentina: Conselho do Mercado Comum, 15 jul. 2019. Disponível em: https://normas.mercosur.int/public/normativas/3768.

MILLER, A. R. **Records, computers, and the rights of citizens:** Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, D.C.: U. S. Department of Health, Education & Welfare, 1973. Disponível em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Acesso em: 26 abr. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Diretrizes da OCDE sobre a proteção da privacidade e fluxos transfronteiriços de dados pessoais.** Paris: OECD Publishing, 2002. Disponível em: https://doi.org/10.1787/9789264196391-en. Acesso em: 26 abr. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Fortalecendo a liderança em integridade na administração pública federal do Brasil:** Aplicando Insights Comportamentais para Integridade Pública. Paris: OECD Publishing, 2023. Disponível em: https://doi.org/10.1787/55376da4-pt. Acesso em: 26 abr. 2025.

PARAGUAI. Lei n.º 6.534, de 27 de outubro de 2020. Ley de Protección de Datos Personales Crediticios. Gaceta Oficial, Assunção, 27 out. 2020. Disponível em: http://www.gacetaoficial.gov.py/index/getDocumento/65863.

PINHEIRO, P. P. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. **Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região**, Curitiba, v. 10, n. 93, p. 75-87, mar. 2021. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/186011. Acesso em: 26 mar. 2024.

PINHEIRO, P. P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018. 2. ed. São Paulo: Saraiva, 2020.

PONJUÁN. D, G. Perfil del profesional de información del nuevo milenio. *In:* VALENTIM, M. L. P. (org.). **O profissional da informação:** formação, perfil e atuação. São Paulo: Polis, 2000. São Paulo: Polis, 2000. 156p.; p.91-105.

REPUBLIC OF SOUTH AFRICA. Parliament of the Republic of South Africa. Act n.º 4 of 2013. **Protection of Personal Information Act**. Government Gazette, vol. 581, n. 37067, Cape Town, RSA, Parliament of the Republic of South, [2013]. Disponível em: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf. Acesso em: 16 mar. 2025.

ROCKEMBACH, M. Estudos de usuários de arquivo e os desafios da Lei Geral de Proteção de Dados. **Acervo**, [*S. l.*], v. 33, n. 3, p. 102–115, 2020. Disponível em: https://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/1554. Acesso em: 25 jul. 2023.

RODRIGUES, G. M. Nota à edição brasileira. *In:* MACNEIL, H. (org.). **Sem consentimento:** a ética na divulgação de informações pessoais em arquivos públicos; tradução Shirley Carvalhêdo Franco e Mônica Tenaglia. Belo Horizonte: Editora UFMG, p. 9-13, 2019.

RODRIGUES, G. M. O acesso aos arquivos sigilosos: um estudo comparado entre o Brasil e a França. *In:* ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 12., 2011, Brasília. **Conferências [...].** Brasília: IBICT, 2011. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/o_acesso_-_rodrigues.pdf. Acesso em: 24 abr. 2023.

ROUSSEAU, J. Y.; COUTURE, C. **Os fundamentos da disciplina arquivística**. Lisboa: Dom Quixote, 1998.

SCHELLENBERG, T. R. **Arquivos modernos**: princípios e técnicas. 6. ed. Rio de Janeiro: FGV, 1973.

SCHWAITZER, L.; NASCIMENTO, N.; COSTA, A. de S. Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). **Acervo**, *[S. l.]*, v. 34, n. 3, p. 1–17, 2021. Disponível em: https://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/1732. Acesso em: 31 ago. 2021.

SIERRA ESCOBAR, L. F. Cómo medir la eficiencia, eficacia y efectividad en los archivos: propuesta de indicadores de gestión. *In:* CONVENCIÓN INTERNACIONAL DE ARCHIVISTAS, 4., 2012, San Barnardo. **Anales [...].** San Barnado, 2012. Disponível em: http://apalopez.info/ivcoindear/12sierra_txt.pdf. Acesso em: 26 jul. 2023.

SILVA, A. L.; HAIKAL, B.; BECKER, D. Era uma vez em Bollywood: nova lei de proteção de dados pessoais da Índia. **Revista Consultor Jurídico,** São Paulo, 26 nov. 2023. Disponível em: https://www.conjur.com.br/2023-nov-26/era-uma-vez-em-bollywood-nova-lei-de-protecao-de-dados-pessoais-da-india/ Acesso em: 16 mar. 2025

SILVA, E. P.; CARDOSO, C. As relações entre a Arquivologia e a Lei Geral de Proteção de Dados, uma análise dos cursos da Enap sobre LGPD. **Revista P2P e Inovação**, v. 8, p. 141-159, 2022.

SILVA, L. G.; NASCIMENTO, R. F**.** ; SANTOS, A. M. M. . Proteção de dados pessoais nos países do BRICS. **Revista Jurídica-Unicuritiba**, v. 4, p. 690-704, 2023.

SILVA, W A. **Exceções legais ao direito de acesso à informação:** dimensões contextuais das categorias de informação pessoal nos documentos arquivísticos. 2017. 541 f. Tese (Doutorado em Ciência da Informação) - Escola de Ciências da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2017.

SILVA, W. A. Gerenciamento arquivístico no serviço de arquivo permanente: identificação de elementos mobilizados. **Informação Arquivística**, v. 1, p. 78-99, 2024. Disponível em: https://aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/166/136. Acesso em: 16 mar. 2025

SILVA, W. A. O gerenciamento arquivístico. *In*: MARIZ, Anna Carla Almeida; RANGEL, Thayron Rodrigues. **Arquivologia**: temas centrais em uma abordagem introdutória. Rio de Janeiro: FGV, 2020.

SILVA, W. A.; MALUF, I. M. P. Governança e gerenciamento arquivístico na perspectiva organizacional: propondo funções básicas. *In:* MALVERDES, A.; SILVA, L. C.; MORAES, M. F. (org.). **Multiverso arquivístico:** ensino e pesquisa na Arquivologia brasileira. Vitória: AARQES; Antíteses, 2025. p. 429-446.

SILVA, W. A.; ROCHA, M. M. V. ; SILVA, J. T. E. ; ESTEVES, R. C. S. P. A. Direito de acesso à informação e proteção aos dados pessoais: um dilema para arquivos e arquivistas?. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, v. 15, p. 262-275, 2020.

UNCTAD. UNCTAD Global Cyberlaw Tracker. Genebra: UNCTAD, [2021]. Disponível em:https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide. Acesso em: 18 fev. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN.

UNIÃO EUROPEIA. COMISSÃO. Decisão 2003/490/CE da Comissão, de 30 de junho de 2003, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à proteção adequada de dados pessoais na Argentina. **Jornal Oficial da União Europeia**, Bruxelas, L 168, 5 jul. 2003. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003D0490&qid=1741545410045

UNIÃO EUROPEIA. COMISSÃO. Decisão de Execução 2012/484/UE da Comissão, de 21 de agosto de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à proteção adequada de dados pessoais pela República Oriental do Uruguai no que diz respeito ao tratamento automatizado de dados pessoais. **Jornal Oficial da União Europeia**, Bruxelas, L 215, 22 ago. 2012. Disponível em:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02012D0484-20161217&qid=1741547820632

UNIÃO EUROPEIA. COMISSÃO. Decisão de Execução 2016/2295 da Comissão, de 16 de dezembro de 2016, que altera a Decisão 2003/490/CE no que se refere ao nível adequado de proteção dos dados pessoais na Argentina. **Jornal Oficial da União Europeia**, Bruxelas, L 344, 17 dez. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016D2295.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Considerando n. 49**. **Jornal Oficial da União Europeia**, Bruxelas, L 119, 4 maio 2016. Disponível em: https://gdpr-info.eu/recitals/no-49/

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Considerando n. 121**. **Jornal Oficial da União Europeia**, Bruxelas, L 119, 4 maio 2016. Disponível em: https://gdpr-info.eu/recitals/no-121/

WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. Harvard Law Review, v. IV, n. 5, December, 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

ZANON, S. B. Arquivos públicos: proteção de dados frente ao acesso à informação. **Revista Ibero-Americana de Ciência da Informação**, v. 15, n. 2, p. 416-435, 2022.

ZARIFIAN, P. **Objetivo competência:** por uma nova lógica. M. H. C. V. Trylinski trad. São Paulo: Atlas, 2012.

APÊNDICE A - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO - TCLE

Prezado(a) arquivista,

Você está sendo convidado(a) a participar da pesquisa em contribuição ao mestrado intitulado **"Relações Conceituais entre a Governança Arquivística e o Papel do Arquivista para a Implementação da Lei Geral de Proteção de Dados Pessoais"** desenvolvido por Daiane Coutinho da Rocha Ferreira, mestranda pelo Programa de Pós-Graduação na Escola de Ciência da Informação na Universidade Federal de Minas Gerais (PPGCI-UFMG), sob a orientação do professor Dr. Welder Antônio Silva.

Essa pesquisa pretende analisar o papel do arquivista na atuação como encarregado pelo tratamento de dados ou como membro de comitê de governança de privacidade e proteção de dados. Como benefício à comunidade arquivística, esse estudo pode auxiliar para o entendimento da contribuição do arquivista para a avaliação da maturidade organizacional, observando os princípios de transparência, prestação de contas e responsabilidade, a partir das diretrizes da LGPD, publicada em 14 de agosto de 2018. Pretende-se ainda colaborar nesta pesquisa para com o desenvolvimento de indicadores pertinentes para a gestão de riscos e a prestação eficaz de contas para a conformidade com a legislação vigente.

A sua participação consistirá em responder às perguntas de forma anônima, online, voluntária e gratuita, com base na sua experiência profissional no desempenho de suas atividades como encarregado ou membro de comitê, desde a promulgação da referida lei.

Serão apresentadas duas perguntas iniciais no questionário, com o intuito de selecionar exclusivamente os profissionais arquivistas que atuaram ou atuam com implementação da LGPD. Em caso afirmativo, você será direcionado a dar continuidade nas demais perguntas, totalizando 12 questões[71]. Estima-se que o tempo necessário para o preencher o questionário seja de aproximadamente 10 minutos.

Não há riscos conhecidos associados à sua participação neste estudo, porém ressaltamos que a sua participação é voluntária e recusar a participar não acarretará qualquer penalidade. Como registro, ao final do preenchimento você receberá uma cópia de suas respostas e os dados oriundos da sua participação serão utilizados exclusivamente para fins acadêmicos e científicos, e sua identidade não será divulgada em nenhuma publicação ou apresentação resultante desta pesquisa.

---

[71] Informações sobre o Comitê de Ética em Pesquisa (CEP-UFMG) podem ser acessadas por toda a comunidade no site www.ufmg.br/bioetica/coep

☐ Aceito participar da pesquisa

Mestranda responsável pela pesquisa: Daiane Coutinho da Rocha Ferreira
Programa de Pós-Graduação em Ciência da Informação - PPGCI/UFMG
Contato: daianecoutinho89@gmail.com

Professor orientador: Dr Welder Antônio Silva
Programa de Pós-Graduação em Ciência da Informação - PPGCI/UFMG
Contato: weldsilva@gmail.com

Agradecemos a sua colaboração!

APÊNDICE B - QUESTIONÁRIO APLICADO

As duas perguntas iniciais, tem o objetivo de selecionar exclusivamente os profissionais arquivistas que atuaram ou atuam com implementação da LGPD, na função de encarregado pelo tratamento dos dados ou como membro de comitê de governança de privacidade e proteção de dados. Em caso afirmativo, você será direcionado a dar continuidade nas demais perguntas, totalizando 18 questões.

Seção 1 - Seleção da Amostra

1 - Você é arquivista*?
*Conforme disposto nos incisos I e II, do art. 1º da Lei 6.546/1978 – diplomado(a) por curso superior de Arquivologia
( ) Sim
( ) Não

2 - Você atua ou já atuou na área de privacidade e proteção de dados como Encarregado pelo Tratamento de Dados (Data Protection Officer-DPO) ou como membro de um Comitê de Governança em Privacidade e Proteção de Dados na sua organização?
( ) Não
( ) Sim, como encarregado pelo tratamento de dados/ data protection officer, apenas.
( ) Sim, como Membro de um Comitê de Governança em Privacidade e Proteção de Dados, apenas.
( ) Sim, como encarregado pelo tratamento de dados e como membro de um Comitê de Governança em Privacidade e Proteção de Dados.

Nessa seção você responderá com base na sua atuação e conhecimentos para os seguintes eixos: A proteção dos documentos arquivísticos, a responsabilidade pela gestão arquivística desde a produção até a destinação final dos documentos, a gestão de riscos para avaliação e monitoramento de incidentes relacionados ao uso dos dados, e a prestação de contas no desenvolvimento de políticas de acesso e privacidade

3 - Você se sente ou se sentia confortável com seu nível de conhecimento e competência em relação à LGPD e outras regulamentações relevantes sobre privacidade e proteção de dados?
( ) Discordo Totalmente

( ) Discordo parcialmente
( ) Nem concordo, nem discordo
( ) Concordo parcialmente
( ) Concordo totalmente

4 - Você acredita que sua experiência e vivência profissional o capacita para lidar de forma eficaz com os desafios relacionados à LGPD?
( ) Discordo Totalmente
( ) Discordo parcialmente
( ) Nem concordo, nem discordo
( ) Concordo parcialmente
( ) Concordo totalmente

5 - Você buscou ou aprimorou seus conhecimentos acadêmicos, seja por meio de cursos de pós-graduação stricto ou lato sensu, para lidar com as demandas relacionadas à privacidade e proteção de dados?
( ) Discordo Totalmente
( ) Discordo parcialmente
( ) Nem concordo, nem discordo
( ) Concordo parcialmente
( ) Concordo totalmente

6 - Você concorda que a responsabilidade arquivística abrange mais do que apenas a gestão de documentos, incluindo também os aspectos da governança arquivística da organização como um todo?
( ) Discordo Totalmente
( ) Discordo parcialmente
( ) Nem concordo, nem discordo
( ) Concordo parcialmente
( ) Concordo totalmente

7 - Como você avalia a sua responsabilidade na garantia da integridade dos documentos arquivísticos, desde o momento da produção até a destinação final, durante a implementação da LGPD?

Integridade:

"Estado dos documentos que se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada". (CONARQ, Glossário Documentos Arquivísticos Digitais, 2016)

( ) Não me sinto/sentia responsável
( ) Poucas vezes me sinto/sentia responsável
( ) Às vezes me sinto/sentia responsável
( ) Frequentemente me sinto/sentia responsável
( ) Sempre me sinto/sentia responsável

8 - Você considera a proteção dos documentos arquivísticos uma prioridade na implementação da Lei Geral de Proteção de Dados?
( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo, nem discordo
( ) Concordo parcialmente
( ) Concordo totalmente

9 - Em que medida você considera efetiva a transparência e a prestação de contas no tratamento de dados em relação ao acesso aos documentos arquivísticos em sua instituição?
( ) Nada efetiva
( ) Pouco efetiva
( ) Moderadamente efetiva
( ) Muito efetiva
( ) Totalmente efetiva

10- Você considera que sua participação como membro de comitês de governança ou como encarregado têm sido/foi significativa para o desenvolvimento e a implementação eficaz de políticas de acesso e de privacidade?

( ) Discordo Totalmente

( ) Discordo parcialmente

( ) Nem concordo, nem discordo

( ) Concordo parcialmente

( ) Concordo totalmente

11 - Você reconhece a importância da gestão de riscos como crucial para a garantia da segurança dos documentos arquivísticos em sua instituição?

( ) Não é importante

( ) Pouco importante

( ) Importante

( ) Às vezes importante

( ) Muito Importante

12 - Você implementa ou implementou medidas de conformidade orientadas no art. 50º "Das Boas Práticas e da Governança" da LGPD, para os documentos arquivísticos?

Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Lei 13709/2018

( ) Não implementei

( ) Implementei parcialmente

( ) Implementei de forma moderada

( ) Implementei completamente

( ) Implemento continuamente e monitoro regularmente

13 - Você poderia fornecer exemplos de como implementou medidas de boas práticas e governança em sua experiência como membro de comitê ou como encarregado de dados?

_____

14 - Você utiliza ou já utilizou padrões de *frameworks* e controles de segurança da informação para melhorar o desempenho do gerenciar e avaliar riscos de privacidade e proteção de dados?

Framework é uma estrutura pronta que fornece um conjunto de diretrizes, condutas, padrões e ferramentas, servindo como modelo a ser aplicado em diversas áreas. Os frameworks auxiliam no desenvolvimento, na implementação e na organização de sistemas e das boas práticas, melhorando a qualidade e a padronização.

Exemplos: Normas ISO/IEC, ABNT NBR, Privacy by Design (PbD), COBIT, e-ARQ Brasil.

( ) Não utilizei
( ) Utilizei parcialmente
( ) Utilizei de forma moderada
( ) Utilizei completamente
( ) Utilizo continuamente e monitoro regularmente

15 - Como você avalia suas habilidades no processo de implementação do framework da norma ISO 27005 para a identificação, avaliação, e monitoramento da gestão de riscos?

Organização Internacional de Normalização (ISO) é uma organização não governamental independente e globalmente reconhecida, que desenvolve normas internacionais. No Brasil são traduzidas no Brasil pela Associação Brasileira de Normas Técnicas (ABNT).

"**ISO/IEC 27005:2023 Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação:** Este documento fornece orientações para ajudar as organizações a: cumprir os requisitos da ABNT NBR ISO/IEC 27001 em relação às ações para abordar riscos de segurança da informação; realizar atividades de gestão de riscos de segurança da informação, especificamente avaliação e tratamento de riscos de segurança da informação" (ABNT, 2023)

( ) Nenhuma experiência na implementação
( ) Pouca experiência na implementação
( ) Alguma experiência na implementação
( ) Boa experiência na implementação
( ) Excelente experiência na implementação

16- Você poderia fornecer exemplos de medidas implementadas para o direcionamento, avaliação e monitoramento na gestão de riscos?

17 - Em que medida você colaborou com a elaboração de algum Relatório de Impacto à Proteção de Dados Pessoais (RIPD) no desempenho de suas atividades?

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O RIPD é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). (ANPD,2021)

( ) Não colaborei
( ) Colaborei muito pouco
( ) Colaborei moderadamente
( ) Colaborei bastante
( ) Colaborei totalmente

18 - Em que medida você considera efetiva a sua atuação como profissional arquivista na condução da avaliação dos riscos e na tomada de decisões sobre o correto tratamento de dados pessoais?
( ) Nada efetivo
( ) Pouco efetivo
( ) Moderadamente efetivo
( ) Muito efetivo
( ) Totalmente efetivo

Você gostaria de falar algo a respeito da implementação da Lei Geral de Proteção de Dados em sua vivência profissional que não tenha sido abordado no questionário?

_____

Obrigada pela sua participação!