ISSN 3085-5624

Eixo Temático 2 - Informação, Comunicação e Processos Tecnológicos

COMPLIANCE DE DADOS E LGPD: A APLICAÇÃO DO MODELO OAIS COMO ESTRUTURA ARQUIVÍSTICA PROMOTORA DO *PRIVACY BY DESIGN*

DATA COMPLIANCE AND LGPD: APPLYING THE OAIS MODEL AS AN ARCHIVAL STRUCTURE PROMOTING PRIVACY BY DESIGN

João Rafael Ribeiro Araújo – Universidade Federal de Alagoas (UFAL), *joaorafael.raraujo@gmail.com*, https://orcid.org/0009-0007-8793-8112

Daniel Flores – Universidade Federal de Alagoas (UFAL), *daniel.flores@ichca.ufal.br*, https://orcid.org/0000-0001-8888-2834

Modalidade: Trabalho Completo

Resumo: O trabalho teve como objetivo analisar a possibilidade de aplicação do modelo de referência *Open Archival Information System* como estrutura arquivística promotora da abordagem de privacidade desde a concepção - *privacy by design* - na gestão e preservação de dados pessoais. A pesquisa possui natureza qualitativa, com método bibliográfico, baseado na análise de livros, artigos acadêmicos e documentos técnicos. Como resultado, verificou-se que o modelo estudado funciona como ferramenta promotora do *compliance* em proteção de dados, especialmente por permitir a integração de seus pacotes com os princípios fundamentais previstos na legislação brasileira.

Palavras-chave: preservação digital; proteção de dados; pacotes informacionais.

***Abstract**: The scientific work aimed to analyze the applicability of the Open Archival Information System reference model as an archival structure that promotes the privacy by design approach in the management and preservation of personal data. The research has a qualitative nature, using a bibliographic method based on the analysis of books, academic articles, and technical documents. As a result, it was found that the model functions as a compliance-enhancing tool for data protection, especially by enabling the integration of its packages with the fundamental principles established by Brazilian legislation.*

***Keywords**: digital preservation; data protection; information packages.*

1 INTRODUÇÃO

A crescente digitalização dos processos informacionais em instituições públicas e privadas gerou, ao longo das últimas décadas, uma verdadeira transformação no modo como dados são produzidos, armazenados, acessados, difundidos e preservados. Neste contexto, os dados pessoais ganharam status de ativo de negócio bastante estratégico, demandando, em contrapartida, práticas cada vez mais sofisticadas de governança e proteção de tais informações.

No Brasil, a promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), consolidou um novo marco normativo, que impõe obrigações legais mais rigorosas sobre o ciclo de vida dos dados pessoais, exigindo o desenvolvimento de mecanismos técnicos e administrativos capazes de promover a privacidade dos usuários e a proteção das informações pessoais tratadas pelas organizações. A legislação ganhou destaque ainda maior, em 2022, quando a Emenda Constitucional nº 115 elevou a proteção de dados ao patamar de direito fundamental.

Entre as diretrizes relevantes da LGPD, destaca-se o princípio do *privacy by design*, cujo termo não está expressamente listado entre os dez princípios do artigo 6º da lei, mas seu conceito se encontra claramente presente no artigo 46, §2º, ao dispor que os agentes de tratamento devem adotar medidas técnicas e administrativas de segurança em todas as etapas da prestação do serviço. Tal diretriz evidencia uma mudança de paradigma: a proteção dos dados pessoais não deve ser apenas uma resposta posterior a riscos ou violações, mas sim um componente estruturante dos projetos e processos institucionais. Isso implica na adoção de modelos e arquiteturas que, desde sua origem, considerem os preceitos da LGPD, como mecanismo viabilizador do *compliance* em proteção de dados pessoais, que fortalece todas as camadas do negócio (Melo; Rockembach; Silva, 2023).

É nesse cenário que se identifica uma oportunidade teórica e prática de aproximação entre o campo da preservação digital sistêmica e o da proteção de dados pessoais. Em particular, o modelo *Open Archival Information System* (OAIS), estabelecido pela norma ISO 14.721:2025 (2025), tem sido amplamente indicado como referência internacional para a organização e preservação de acervos digitais. Estruturado em componentes funcionais e pacotes informacionais – *Submission Information Package* (SIP), *Archival Information Package* (AIP) e *Dissemination Information Package* (DIP) – o OAIS oferece uma arquitetura arquivística robusta, centrada na integridade, na acessibilidade controlada e na rastreabilidade dos objetos digitais ao longo do tempo.

A partir dessa arquitetura, surge o questionamento central que orienta esta pesquisa: pode o modelo OAIS ser aplicado como uma estrutura arquivística promotora do *privacy by design*, nos termos exigidos pela LGPD, e, consequentemente, como ferramenta de fomento ao *compliance* em proteção de dados pessoais? Esta pergunta articula os três campos interdependentes objeto desta pesquisa: a principal legislação de dados pessoais aplicada no Brasil (LGPD), os princípios de privacidade desde a concepção (*privacy*

by design) e a engenharia arquivística da informação digital presente no modelo OAIS.

O objetivo desta pesquisa é, portanto, analisar a aplicabilidade do modelo OAIS como instrumento capaz de promover, de maneira estruturada, os requisitos do *privacy by design* na gestão e preservação de dados pessoais. Busca-se demonstrar que, embora desenvolvido originalmente para fins arquivísticos, o OAIS pode desempenhar papel estratégico na construção de sistemas digitais que, além de preservar a autenticidade e a integridade dos dados, estejam em conformidade com os princípios da LGPD.

A relevância do estudo reside, portanto, na seguinte intersecção: em um cenário no qual organizações buscam se adequar à LGPD e evitar sanções administrativas e reputacionais, modelos como o OAIS podem fornecer os fundamentos técnicos necessários à estruturação de repositórios que operem com conformidade e governança ativa. Ao integrar práticas arquivísticas, exigências legais e princípios éticos, esta pesquisa pretende contribuir para o desenvolvimento de abordagens interdisciplinares voltadas à proteção de dados pessoais em ambientes digitais, com especial atenção ao papel estratégico da preservação informacional.

2 METODOLOGIA

A presente pesquisa possui natureza qualitativa, com abordagem exploratória e de caráter interdisciplinar. Adotou-se o método bibliográfico, com base na análise crítica e interpretativa de livros, artigos acadêmicos, resoluções técnicas, normas arquivísticas e dispositivos legais relacionados à proteção de dados pessoais, preservação digital, *compliance* e modelos arquivísticos. A pesquisa documental foi uma aliada na busca dos referenciais mais aderentes ao OAIS.

As fontes utilizadas foram selecionadas por sua relevância teórica e aplicabilidade prática. A coleta de dados se deu por meio da identificação e análise sistemática dessas obras, priorizando produções atualizadas e pertinentes ao recorte temático proposto.

A análise concentrou-se na verificação da aderência entre os componentes do modelo OAIS e os requisitos normativos da proteção de dados, principalmente a LGPD, observando de que forma o modelo pode ser aplicado como ferramenta que potencializa o *compliance* de dados, promovendo segurança, transparência, responsabilidade e preservação de longo prazo — aspectos essenciais à ideia de *privacy by design*.

Trata-se, portanto, de uma pesquisa de caráter propositivo e hipotético, que, embora não se baseie em estudo de caso empírico, propõe a aplicabilidade do modelo OAIS como solução viável e estratégica à conformidade com a LGPD, na preservação de dados pessoais em instituições públicas e privadas. A busca pela construção de hipóteses plausíveis foi amplamente pautada na literatura. Busca-se, com isso, contribuir para o aprofundamento das relações entre a Arquivologia, a Ciência da Informação e o Direito Digital, destacando a importância de abordagens interdisciplinares no enfrentamento dos desafios contemporâneos relacionados à proteção e preservação de dados pessoais.

3 PRINCÍPIOS DA LGPD COMO FUNDAMENTO PARA O *COMPLIANCE* EM PROTEÇÃO DE DADOS PESSOAIS

O termo *compliance* deriva do verbo em inglês *to comply*, que significa estar em conformidade com leis, regulamentos e normas aplicáveis. No contexto corporativo e institucional, *compliance* representa um conjunto de práticas e procedimentos voltados à promoção da conformidade legal e ética, à mitigação de riscos e à estruturação de uma cultura organizacional responsável (Assi, 2018). Em tempos de intensificação da coleta e do tratamento de dados pessoais[1] por sistemas informatizados, destaca-se um campo específico dentro do *compliance*: o *compliance* em proteção de dados, ou *compliance* de dados, que abrange justamente a preocupação com o cumprimento das normas e diretrizes legais que regulam o ciclo de vida dessas informações.

No ordenamento jurídico brasileiro, a LGPD, Lei nº 13.709/2018, se configura como o principal marco regulatório aplicável à governança de dados pessoais. Inspirada em legislações internacionais, como o *General Data Protection Regulation* (GDPR) da União Europeia, a LGPD estabelece princípios, direitos e obrigações que orientam o tratamento legítimo de dados, impondo às organizações a adoção de medidas técnicas e administrativas que garantam transparência, segurança, responsabilidade e respeito à privacidade dos titulares (Almeida; Soares, 2022).

Neste sentido, para promover uma cultura institucional de *compliance* de dados, é

[1] Segundo o artigo 5º, X, da Lei Geral de Proteção de Dados Pessoais, tratamento de dados é: 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.

fundamental que as organizações implementem a LGPD de forma estruturada, abrangente e contínua. Isso envolve não apenas responder a exigências pontuais, mas internalizar os dez princípios previstos no artigo 6º da LGPD, os quais funcionam como norteadores ético-normativos para todas as etapas do tratamento de dados pessoais. São eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

De forma objetiva, os princípios poderiam ser assim explicados:

1. Finalidade: O tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e previamente informados ao titular. É proibida a utilização posterior dos dados para fins incompatíveis com os inicialmente declarados.
2. Adequação: Exige-se que o tratamento seja compatível com a finalidade informada, respeitando o contexto no qual os dados foram coletados. A adequação assegura coerência entre os dados coletados, o uso de tais dados e a finalidade declarada ao titular.
3. Necessidade: Impõe-se a limitação da coleta e uso ao mínimo necessário para a realização da finalidade declarada. Os dados devem ser pertinentes, proporcionais e não excessivos.
4. Livre acesso: Garante ao titular o direito de consulta facilitada e sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
5. Qualidade dos dados: Obriga o agente a manter os dados em condições adequadas de uso, pois assegura ao titular o direito de que seus dados sejam preservados de maneira atualizada, clara, relevante e mantendo exatidão das informações.
6. Transparência: Garante que o titular tenha informações claras e precisas sobre a realização do tratamento dos dados e os agentes de tratamento envolvidos nestas operações. O objetivo é fazer com que as instituições adotem mecanismos de publicização de informações sobre o tratamento de dados, como, por exemplo, a elaboração de portais de LGPD nos sítios eletrônicos, indicando o contato do encarregado responsável pela proteção de dados, a política de privacidade da instituição e demais documentos que sejam relevantes.
7. Segurança: Exige a adoção de medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou

ilícitas de destruição, perda, alteração, comunicação ou difusão das informações.

8. Prevenção: Orienta a adoção de medidas proativas voltadas à prevenção de incidentes e de minimização de danos aos titulares – caso algum incidente aconteça.

9. Não discriminação: Proíbe o tratamento de dados com fins discriminatórios, ilícitos ou abusivos, assegurando que a utilização dos dados não resulte em práticas que violem direitos fundamentais

10. Responsabilização e prestação de contas: Impõe ao agente de tratamento o dever de demonstrar a adoção de medidas eficazes para assegurar o cumprimento das normas de proteção de dados, incluindo a capacidade de comprovar a efetividade dessas ações (Brasil, 2018).

A aplicação prática desses princípios, em geral, deve permear todas as fases do tratamento de dados – desde a coleta e o armazenamento até o compartilhamento, descarte ou anonimização –, exigindo uma abordagem transversal e proativa. Nesse sentido, embora não esteja nominalmente entre os princípios listados no art. 6º, ganha destaque o conceito de *privacy by design*, previsto de forma implícita no art. 46, §2º da LGPD, ao dispor que as instituições devem adotar medidas de segurança que protejam os dados pessoais desde a fase de concepção dos projetos e processos que estão ou virão a ser implementados. O *privacy by design*, portanto, é uma diretriz estruturante da legislação, que reforça a importância de pensar a proteção de dados como componente fundamental dos processos e sistemas, desde seu nascedouro (Oliveira, 2021).

Oliveira, ao tratar das formas pelas quais as organizações podem se resguardar de sanções administrativas decorrentes do descumprimento da LGPD – ideia intimamente ligada ao *compliance* de proteção de dados –, destaca a relevância da adoção dos princípios associados ao *privacy by design*. Para o autor, essa abordagem implica a incorporação, desde a concepção dos processos de negócio, de mecanismos técnicos e organizacionais voltados à segurança e à proteção contínua dos dados pessoais, visando, por óbvio a implementação de uma estrutura de segurança capaz de melhor viabilizar a privacidade aos titulares em todas as fases do tratamento de dados (Oliveira, 2021).

Assim, ao seguir os princípios da LGPD de forma contínua e integrada aos fluxos informacionais internos, as organizações não apenas promovem o *privacy by design*, mas também implementam, sistematicamente, o chamado *compliance* de dados pessoais. Essa vinculação entre princípios legais e conformidade técnica representa o eixo central para uma

governança de dados pessoais alinhada aos valores democráticos de privacidade, transparência e segurança.

4 ESTRUTURA ARQUIVÍSTICA E ELEMENTOS FUNCIONAIS DO MODELO OAIS

No âmbito da preservação digital, o modelo OAIS, estabelecido na norma ISO 14721:2025, é considerado o referencial conceitual mais sólido e amplamente adotado para a gestão e a custódia de documentos digitais. Segundo Gava e Flores (2022), trata-se do modelo mais relevante da Ciência da Informação no que diz respeito ao gerenciamento do documento digital, constituindo uma parte essencial dos Repositórios Digitais Confiáveis (RDC). O OAIS fornece uma estrutura teórica e funcional capaz de orientar instituições arquivísticas na preservação de longo prazo de objetos digitais, garantindo sua autenticidade, integridade e acessibilidade em uma cadeia de custódia digital para os objetos digitais, documentos e informações.

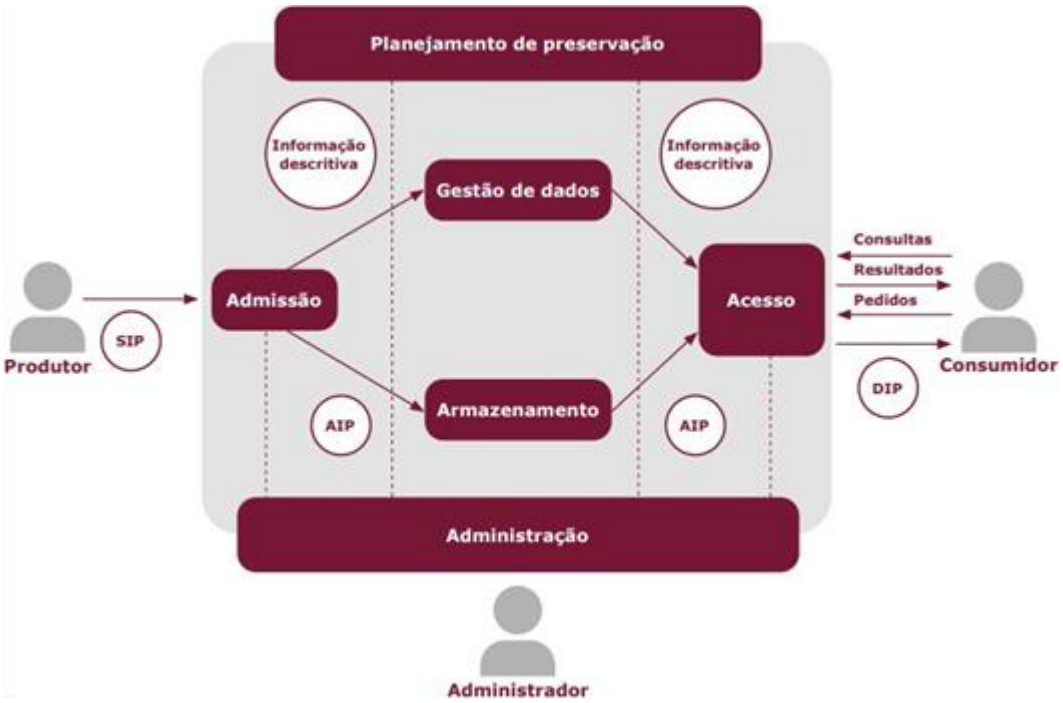
O ambiente OAIS é constituído por seis entidades funcionais internas e três entidades externas. As internas são: admissão (*ingest*), responsável por incorporar as informações ao repositório; armazenamento arquivístico (*archival storage*), que realiza a organização e a guarda segura dos dados; gestão de dados (data management), que está ligada ao controle dos metadados e informações administrativas; administração (*administration*), que coordena o funcionamento do sistema; planejamento da preservação (*preservation planning*), voltado à adoção de estratégias de manutenção da acessibilidade no tempo; e acesso (*access*), que permite a busca e o fornecimento controlado dos documentos à comunidade designada (Santos; Flores, 2022). Já as entidades externas são o produtor, que fornece os dados ao repositório; o administrador, que estabelece as políticas institucionais; e o consumidor, que interage com os conteúdos arquivados.

Segundo Barni e Rocha (2023), as funções desempenhadas por essas entidades cumprem papel central na preservação digital, uma vez que posicionam os documentos dentro do contexto de sua produção e uso. Ainda de acordo com os autores, isso permite compreender tanto o papel dos documentos dentro da organização quanto sua interconexão com outros registros produzidos, o que reforça até mesmo a lógica arquivística de manutenção da memória institucional.

A partir desta compreensão, Santos e Flores (2022) explicam que as entidades estão

intimamente relacionadas a três tipos de pacotes informacionais do modelo OAIS: o *Submission Information Package* (SIP), que é o pacote de submissão recebido do produtor; o *Archival Information Package* (AIP), responsável pelo armazenamento e preservação de longo prazo; e o *Dissemination Information Package* (DIP), que representa o conteúdo disponibilizado ao usuário/público-alvo. Cada pacote contém não apenas os dados em si, mas também informações descritivas (descriptive information) que garantem a autenticidade, proveniência e inteligibilidade dos documentos ao longo do tempo (Santos; Flores, 2022). A Figura 1 bem representa essa relação.

Figura 1 - Entidades funcionais do OAIS



Fonte: CONARQ (2023).

Em termos práticos, o funcionamento do modelo OAIS pode ser compreendido como um fluxo estruturado de preservação digital. Tudo começa quando o produtor da informação — que pode ser um setor institucional, um servidor público ou um sistema automatizado — envia os documentos digitais por meio de um sistema de submissão vinculado a um repositório arquivístico digital confiável. Esse envio inicial compõe o chamado pacote de submissão (SIP), contendo não apenas os dados em si, mas também informações descritivas e contextuais. Após essa fase, o conteúdo é processado internamente e passa por uma etapa de conversão para formatos compatíveis com a preservação digital de longo prazo, com base

em padrões técnicos previamente definidos pela instituição. Por exemplo, um vídeo originalmente em MP4 pode ser convertido para um formato mais adequado à preservação, como MKV, de modo a garantir acessibilidade futura e independência tecnológica.

Esse conteúdo convertido e descrito adequadamente integra o pacote arquivístico (AIP), que será armazenado de forma segura no repositório, com mecanismos de controle de integridade, proveniência e rastreabilidade. O AIP é mantido de forma permanente, seguindo as políticas de preservação digital da instituição. Quando houver solicitação de acesso por parte do usuário — ou consumidor, nos termos do modelo OAIS —, o sistema gera uma cópia derivada do conteúdo original, denominada pacote de disseminação (DIP), que é entregue de forma controlada ao destinatário. O documento original, no entanto, permanece resguardado no repositório. Com isso, o modelo OAIS assegura que os documentos arquivísticos digitais sejam mantidos íntegros, autênticos e acessíveis ao longo do tempo, mesmo diante de mudanças tecnológicas e operacionais.

Outro aspecto importante do modelo OAIS é sua ênfase no controle contínuo da custódia dos documentos digitais, conforme destacado por Gava e Flores (2022). Tal controle se relaciona ao conceito arquivístico de cadeia de custódia, entendida como a manutenção de uma linha ininterrupta de responsabilidade e guarda documental, desde sua criação até sua disponibilização final, assegurando que o conteúdo permaneça autêntico e inalterado. A isso se soma a noção de cadeia de preservação, que busca garantir que os documentos preservem sua confiabilidade e possam ser acessados no longo prazo, mesmo diante das mudanças tecnológicas e contextuais.

Ainda nesse sentido, o OAIS é pensado para assegurar a preservação de longo prazo, definida como aquela que demanda atenção especial aos impactos das mudanças tecnológicas

— como novos formatos, suportes de armazenamento e níveis de conhecimento da comunidade usuária —, ainda que o próprio modelo em si não seja permanente (Santos; Flores, 2019). Essa perspectiva reforça a sua aplicabilidade contínua e a necessidade de revisão e adaptação periódicas conforme as transformações do ecossistema digital.

Cabe observar que o modelo OAIS permite que os repositórios sejam implementados inclusive em ambientes de computação em nuvem, nos quais os documentos digitais podem estar armazenados geograficamente distantes da instituição arquivística responsável, o que reforça ainda mais a necessidade de controle funcional, técnico e normativo sobre a

preservação documental (Gava; Flores, 2022).

Complementando essa perspectiva, a versão 3 do modelo OAIS, publicada em 2025, fortaleceu o conceito de Arquivos Federados, que amplia a capacidade de interoperabilidade entre repositórios distribuídos. A proposta contempla arquiteturas heterogêneas de instituições produtoras e entidades custodiadoras, permitindo a integração funcional de sistemas distintos em rede e garantindo a heterogeneidade dos ambientes de custódia digital e preservação. Essa atualização fortalece a aplicação do OAIS em contextos colaborativos e geograficamente dispersos, como ambientes em nuvem, sem comprometer os requisitos de autenticidade, preservação e acesso aos documentos digitais (The Consultative Committee for Space Data Systems - CCSDS, 2024).

Dessa forma, o OAIS configura-se como uma base arquivística conceitual e funcional indispensável à preservação digital confiável sistêmica, podendo ser adaptado a diferentes contextos institucionais e oferecendo elementos importantes para a governança da informação, em especial quando se trata de documentos digitais que contenham dados pessoais.

5 CONVERGÊNCIAS ENTRE O MODELO OAIS E OS PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS

O modelo OAIS, além de consolidar-se como um referencial técnico para a preservação digital, apresenta aderência significativa aos princípios previstos na LGPD, especialmente quando considerado sob a perspectiva da proteção contínua, segura e estruturada de documentos arquivísticos digitais que contenham dados pessoais. A correlação entre os pacotes informacionais do OAIS — SIP, AIP e DIP — e os princípios legais da LGPD revela um alinhamento conceitual e operacional que fortalece o *compliance* de dados e consolida o *privacy by design* como um elemento transversal em repositórios arquivísticos digitais.

O SIP, pacote de submissão que contempla os dados e seus metadados no momento da entrada no sistema, guarda forte correspondência com os princípios da finalidade, adequação e necessidade, ao exigir que os dados submetidos sejam pertinentes, compatíveis com a finalidade do tratamento e limitados ao estritamente necessário. Nesse estágio, o sistema que implementa o OAIS já começa a viabilizar uma gestão documental informada

por critérios éticos e legais, exigindo que apenas dados devidamente justificados sejam aceitos e armazenados. Ainda no momento da ingestão, conforme esclarecem Santos, Mazuco e Flores (2020), os pacotes SIP já contemplam a organização de metadados essenciais — como a informação de empacotamento e de preservação —, o que permite a rastreabilidade e a identificação clara dos documentos desde sua origem.

No estágio intermediário, o AIP assume papel central na preservação segura e de longo prazo dos dados, conectando-se de maneira direta aos princípios da segurança, qualidade dos dados e prevenção. É nesse momento que ocorrem a fixação do conteúdo, a validação da integridade e a garantia da autenticidade documental, pilares que asseguram a confiabilidade da informação. A cadeia de preservação e de custódia contínua digital — conforme salientam Gava e Flores (2022) — evita que documentos sejam modificados indevidamente ou corrompidos, garantindo o acesso futuro e a autenticidade da informação.

O AIP não armazena qualquer tipo de dado de forma irrestrita: há, nesse ponto, um processo técnico de conversão para formatos digitais adequados à preservação, muitas vezes distintos daqueles originalmente submetidos, justamente para garantir longevidade, acessibilidade e integridade. Esse processo é orientado por um Plano de Preservação Digital - comumente vinculado a uma Política de Preservação Digital -, que define os formatos de entrada, os procedimentos de conversão e as condições de disponibilização dos dados aos usuários. Essa diretriz é incorporada nas soluções técnicas compatíveis com o modelo OAIS, especialmente em softwares livres, indicados sobretudo para instituições públicas. O repositório PRONOM, do Reino Unido, é exemplo de implementação bem-sucedida dessa lógica.

Já o DIP está associado à entrega ou disponibilização das informações ao usuário final e está fortemente alinhado aos princípios do livre acesso, da transparência, da responsabilização e prestação de contas e da não discriminação. O OAIS determina que esse acesso ocorra de forma controlada, segura e com garantia de que os dados entregues correspondem exatamente à versão preservada e autorizada. Isso reforça o princípio da prestação de contas e da responsabilidade institucional diante da comunidade usuária e dos titulares de dados. A Resolução CONARQ nº 50/2022, ao recomendar expressamente a utilização do OAIS (ISO 14721:2025) para a preservação digital, destaca a necessidade de classificação, proteção especial e cuidado com os dados pessoais, principalmente os

considerados sensíveis[2], estabelecendo um elo direto entre preservação arquivística e governança informacional nos moldes da LGPD.

Além dos aspectos técnicos, o modelo OAIS, enquanto estrutura arquivística sistêmica, incorpora uma abordagem holística que vai ao encontro do conceito de *privacy by design*. A ideia de que a proteção de dados deve ser implementada desde a concepção dos sistemas e processos está diretamente refletida na forma como o OAIS organiza suas entidades funcionais (ingestão, armazenamento, acesso, planejamento da preservação, administração e gestão de dados) e estrutura os pacotes informacionais. Conforme destacam Santos, Mazuco e Flores (2020), a confiabilidade de um Repositório Digital Confiável (RDC-Arq) está condicionada à sua conformidade com o modelo OAIS, cuja auditoria abrange desde questões tecnológicas e organizacionais até a responsabilidade administrativa, segurança da informação e prestação de contas — pontos convergentes com os pilares do *compliance* de dados.

Essa sinergia é igualmente enfatizada por Gomes e Souza (2024), ao reconhecerem a importância de sistemas informatizados distribuídos geograficamente, com o objetivo de assegurar a acessibilidade e a proteção contra perdas, sinistros e falhas. Esses mecanismos técnicos são, em si, expressões práticas do princípio da prevenção, previsto na LGPD e, como já citado anteriormente, fomentado pelo modelo OAIS ao dispor sobre arquivos federados. Por fim, a própria concepção de um RDC-Arq baseado em OAIS, enquanto arranjo composto por pessoas, políticas, sistemas e acervos – e não um mero software –, revela uma aderência profunda à lógica da responsabilização institucional, transparência operacional e comprometimento ético com a proteção de dados pessoais, conforme reforça Lóssio (2023).

Portanto, a aplicação do modelo OAIS como estrutura arquivística para a preservação digital não apenas satisfaz requisitos técnicos da ciência da informação, como também atende de forma integrada aos princípios estruturantes da proteção de dados pessoais, promovendo o *compliance* e consolidando o *privacy by design* como diretriz transversal de governança documental e informacional.

[2] Segundo o artigo 5º, X, da Lei Geral de Proteção de Dados Pessoais, dado pessoal sensível é: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

6 CONCLUSÃO

A consolidação da proteção de dados pessoais como princípio estruturante da governança informacional impõe às instituições públicas e privadas não apenas o cumprimento formal da LGPD, mas também a adoção de estruturas e práticas que viabilizem, de forma contínua e sistêmica, o *compliance* e a privacidade desde a concepção dos sistemas – em consonância com o princípio do *privacy by design*. Nesse contexto, este trabalho demonstrou que o modelo OAIS, por sua natureza arquivística, normativa e técnica, oferece um arcabouço robusto para atender a tais exigências, atuando como base estratégica para repositórios digitais confiáveis e para o tratamento responsável de dados pessoais.

Dessa forma, a presente pesquisa cumpre o objetivo proposto, de analisar a aplicabilidade do modelo OAIS como instrumento capaz de promover, de maneira estruturada, os requisitos do *privacy by design* na gestão e preservação de dados pessoais. Procurou-se evidenciar que, embora o OAIS tenha sido originalmente concebido para o campo arquivístico, ele apresenta forte potencial de integração com os princípios da LGPD, especialmente ao garantir a autenticidade, a integridade e o acesso seguro aos dados durante todo seu ciclo de vida, culminando na manutenção da cadeia de custódia digital arquivística (CCDA).

Neste sentido, a análise desenvolvida demonstrou que os pacotes informacionais previstos no OAIS (SIP, AIP e DIP) não apenas correspondem a etapas críticas da preservação digital, mas também guardam correlação direta com os princípios legais que fundamentam a proteção de dados. O SIP se alinha aos princípios da finalidade, adequação e necessidade; o AIP aos da segurança, qualidade dos dados e prevenção; e o DIP aos do livre acesso, transparência, não discriminação e prestação de contas. Essa correspondência reforça a vocação do modelo OAIS para atuar como estrutura arquivística promotora do *privacy by design*, contribuindo para a construção de sistemas que conciliem preservação documental, proteção legal e responsabilidade institucional.

Além disso, é válido pontuar que, por se tratar de um modelo conceitual e normativo baseado em ferramentas abertas e de domínio público, o OAIS revela-se tecnicamente viável para implementação tanto em instituições públicas quanto privadas. Sua compatibilidade com a filosofia dos softwares livres — especialmente recomendados para ambientes públicos, por atenderem aos princípios de transparência, interoperabilidade e soberania

tecnológica — reforça sua atratividade, inclusive pelo custo relativamente reduzido. Esse aspecto, aliás, pode ser aprofundado em futuras investigações que analisem a viabilidade econômica da adoção do modelo em projetos de conformidade com a legislação de proteção de dados.

Por fim, ao integrar práticas de preservação digital com segurança, transparência e disponibilidade das informações a quem de direito, o modelo OAIS se alinha com os pilares contemporâneos do *compliance* em proteção de dados pessoais. No entanto, essa integração exige uma mudança de paradigma: é preciso abandonar abordagens fragmentadas e setoriais. Não se pode mais pensar em implementar a LGPD sem dialogar com os princípios da arquivologia e da preservação digital, da mesma forma que não se deve aplicar o OAIS apenas sob o viés da transparência e da disponibilidade dos dados, ignorando a natureza sensível e legalmente protegida dos dados pessoais. A complexidade dos sistemas digitais contemporâneos demanda uma abordagem interdisciplinar e holística, que considere os limites e convergências entre os marcos regulatórios, os saberes técnicos e as exigências sociais envolvidas na gestão da informação.

REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 27, ed. 3, p. 26-45, jul/set 2022. DOI http://dx.doi.org/10.1590/1981-5344/25905. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/25905/31548. Acesso em: 12 jul. 2025.

ASSI, Marcos. **Conformidade: como implementar**. São Paulo: Trevisan Editora, 2018. E- book. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788595450356/. Acesso em: 12 jul. 2025.

BARNI, Lucieli Francini; ROCHA, Rafael Port da. Um olhar arquivístico do modelo OAIS para o desenvolvimento de um repositório digital no contexto de uma organização. FÓRUM DE ESTUDOS EM INFORMAÇÃO, SOCIEDADE E CIÊNCIA, 5., Porto Alegre, 2023. **Anais** [...]. Porto Alegre, 2023. Disponível em: https://cip.brapci.inf.br//download/324921. Acesso em: 15 jul. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 jun. 2025.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução CONARQ nº 50, de 06 de maio de 2022**. E-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos, Rio de Janeiro, mai. 2022. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/publicacoes-conarq. Acesso em: 15 jul. 2025.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução CONARQ nº 51, de 25 de agosto de 2023**. Diretrizes para implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq), Rio de Janeiro, 2023. Disponível em: https://www.gov.br/conarq/pt-br/centrais- de-conteudo/publicacoes/publicacoes-conarq. Acesso em: 15 jul. 2025.

GAVA, Tânia Barbosa Salles; FLORES, Daniel. Problematizando a Pós-Custódia com a contemporaneidade da Cadeia de Custódia Digital Arquivística compartilhada e distribuída na Preservação Digital Sistêmica. **InCid:** Revista de Ciência da Informação e Documentação, Ribeirão Preto, v. 13, n. 2, p. 222–243, 2022. Disponível em: https://revistas.usp.br/incid/article/view/191654. Acesso em: 15 jul. 2025.

GOMES, Wellington da Silva; SOUZA, Edivanio Duarte de. A trilha para a preservação digital sistêmica na arquivologia: abordagem teórico-conceitual de um modelo de gestão compartilhada e distribuída. ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 24., 2023, Espírito Santo. **Anais** [...]. Espírito Santo, 2023. Disponível em: https://brapci.inf.br/v/342800. Acesso em: 15 jul. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 14721:2025.** Space Data System Practices — Reference model for an open archival information system (OAIS), [S. l.], 2025. Disponível em: https://www.iso.org/standard/87471.html. Acesso em: 11 ago. 2025.

LÓSSIO, Claudio Joel Brito**. Proteção de dados e compliance digital**. São Paulo: Almedina, 2023. Ebook. ISBN 9786556279893. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556279893. Acesso em: 12 jul. 2025.

MELO, Jonas Ferrigolo; ROCKEMBACH, Moisés; SILVA, Armando Malheiro da. CIÊNCIA DA INFORMAÇÃO E PRIVACY BY DESIGN: aspectos éticos e possibilidades de pesquisa. **Logeion:** Filosofia da Informação, Rio de Janeiro, v. 9, n. 2, p. 124-143, mar/ago 2023. Disponível em: https://lume.ufrgs.br/handle/10183/256213. Acesso em: 12 jul. 2025.

OLIVEIRA, Ricardo. **LGPD:** como evitar as avaliações administrativas. Rio de Janeiro: Expressa, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786553623262/. Acesso em: 12 jul. 2025.

SANTOS, Henrique Machado dos; FLORES, Daniel. Introdução aos conceitos básicos do modelo open archival information system no contexto da arquivística. **Acervo**, [*s. l.*], v. 32, n. 1, p. 8-26, 2019. Disponível em: https://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/1029. Acesso em:

15 jul. 2025.

SANTOS, Henrique Machado dos; FLORES, Daniel. Transformações dos pacotes de informação na cadeia de custódia digital arquivística. **Páginas a&b:** Arquivos E Bibliotecas, [*s. l.*], n. 18, p. 18-35, dez 2022. Disponível em: https://ojs.letras.up.pt/index.php/paginasaeb/article/view/12540. Acesso em: 14 jul. 2025.

SANTOS, Henrique Machado dos; MAZUCO, Fabiana Ciocheta; FLORES, Daniel. Preservação sistêmica de documentos arquivísticos digitais: uma perspectiva holística. **PerCursos**, [*s. l.*], v. 21, n. 46, p. 244-271, mai/ago. 2020. DOI http://dx.doi.org/10.5965/1984724621462020244. Disponível em: https://periodicos.udesc.br/index.php/percursos/article/view/17401. Acesso em: 15 jul. 2025.

THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS). CCSDS 650.0-M-3. **Reference Model For An Open Archival Information System (OAIS)**, Washington, v. 3, dez 2024.

NOTA
Este trabalho foi realizado no escopo das atividades do Projeto “Socialização do Método do Estudo Imanente em Informação”, Chamada CNPq/MCTI Nº 10/2023, sob a supervisão do Professor Doutor Edivanio Duarte de Souza.