FRAMEWORK DE ADEQUAÇÃO DE BANCOS DE DADOS LEGADOS À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): UM ESTUDO PARA ÓRGÃOS PÚBLICOS BRASILEIROS

Glauco Lauria Marques
Eduardo Amadeu Dutra Moresi

Universidade Católica de Brasília (UCB), Brasília, DF – Brasil

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil se tornou essencial para órgãos públicos e privados se adequarem às novas exigências de proteção de dados. No entanto, existe uma lacuna científica significativa na literatura sobre a aplicação da LGPD em órgãos públicos brasileiros. Este estudo visa desenvolver um *framework* conceitual para ajudar estas entidades a adaptar seus bancos de dados legados à LGPD. A metodologia incluiu uma revisão da literatura disponível na base Scopus, a análise de documentos relevantes e a coleta de dados de dois bancos de dados do Portal do Software Público. O *framework* inicial foi validado por meio de uma pesquisa qualitativa com especialistas em LGPD que forneceram feedbacks para melhorias. Os resultados indicaram que o *framework* proposto é eficaz para apoiar órgãos públicos na conformidade com a LGPD, com ajustes incorporados conforme sugestões dos especialistas. Conclui-se que o *framework* desenvolvido facilita a adaptação de bancos de dados legados às exigências da LGPD, oferecendo um guia sistemático para a implementação de práticas de proteção de dados, contribuindo assim para a segurança jurídica e a confiança dos cidadãos.

Palavras-chave: Regulamento Geral de Proteção de Dados; Lei Geral de Proteção de Dados Pessoais; LGPD; bancos de dados legados; *framework*.

DOI: https://doi.org/10.21874/rsp.v75i4.10941 ISSN: 0034-9240 | e-ISSN: 2357-8017
Submetido: 05 de junho de 2024. Aceito: 22 de outubro de 2024.

MARCO DE ADAPTACIÓN DE BASES DE DATOS LEGADAS A LA LGPD: UN ESTUDIO PARA ORGANISMOS PÚBLICOS BRASILEÑOS

La implementación de la Ley General de Protección de Datos Personales (LGPD) en Brasil se ha vuelto esencial para los organismos públicos y privados adaptarse a las nuevas exigencias de protección de datos. Sin embargo, existe una brecha científica significativa en la literatura sobre la aplicación de la LGPD en organismos públicos brasileños. Este estudio tiene como objetivo desarrollar un marco conceptual para ayudar a estas entidades a adaptar sus bases de datos legadas a la LGPD. La metodología incluyó una revisión de la literatura disponible en la base de datos Scopus, el análisis de documentos relevantes y la recopilación de datos de dos bases de datos del Portal del Software Público. El marco inicial fue validado a través de una investigación cualitativa con expertos en LGPD que proporcionaron comentarios para mejoras. Los resultados indicaron que el marco propuesto es eficaz para apoyar a los organismos públicos en el cumplimiento de la LGPD, con ajustes incorporados según las sugerencias de los expertos. Se concluye que el marco desarrollado facilita la adaptación de bases de datos legadas a las exigencias de la LGPD, ofreciendo una guía sistemática para la implementación de prácticas de protección de datos, contribuyendo así a la seguridad jurídica y la confianza de los ciudadanos.

Palabras clave: Reglamento General de Protección de Datos; Ley General de Protección de Datos Personales; LGPD; bases de datos legadas; marco conceptual.

FRAMEWORK FOR ADAPTING LEGACY DATABASES TO THE LGPD: A STUDY FOR BRAZILIAN PUBLIC AGENCIES

The implementation of the General Data Protection Law (LGPD) in Brazil has become essential for public and private organizations to comply with the new data protection requirements. However, there is a significant scientific gap in the literature regarding the application of the LGPD in Brazilian public agencies. This study aims to develop a conceptual *framework* to assist these entities in adapting their legacy databases to the LGPD. The methodology included a review of the literature available in the Scopus database, the analysis of relevant documents, and the collection of data from two databases of the Public Software Portal. The initial *framework* was validated through qualitative research with LGPD experts who provided feedback for improvements. The results indicated that the proposed *framework* is effective in supporting public agencies in complying with the LGPD, with adjustments incorporated based on experts' suggestions. It is concluded that the developed *framework* facilitates the adaptation of legacy databases to the requirements of the LGPD, offering a systematic guide for implementing data protection practices, thereby contributing to legal security and citizens' trust.

Keywords: General Data Protection Regulation; General Data Protection Law; LGPD; legacy databases; *framework*.

1. INTRODUÇÃO

Em maio de 2018, a União Europeia implementou o Regulamento Geral de Proteção de Dados (GDPR), substituindo a Diretiva de Proteção de Dados 95/46. O GDPR trouxe mudanças significativas no tratamento de dados pessoais por governos e empresas, destacando o consentimento do titular como essencial para a coleta e tratamento. Além disso, o regulamento conferiu poderes de fiscalização e multa às autoridades.

No primeiro ano do GDPR, houve multas substanciais, destacando a seriedade da União Europeia com a privacidade dos dados pessoais (Pohlmann, 2019). A proteção da privacidade é um direito inviolável na União Europeia, exigindo que todas as entidades na região sigam normas rigorosas sobre a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada no GDPR, foi promulgada em 14 de agosto de 2018 e entrou em vigor parcialmente em dezembro. A LGPD trouxe mudanças para o governo, empresas e consumidores, colocando o Brasil entre os países com legislação específica para proteção de dados pessoais. Com a LGPD, o Brasil busca garantir a privacidade dos cidadãos contra uso indevido, comercialização e vazamento de dados, aplicando multas quando necessário.

Apesar da implementação da LGPD, a maioria dos órgãos públicos brasileiros ainda não está conforme a lei, representando uma lacuna na aplicação e adesão às novas normas de proteção de dados. Este gap científico destaca a necessidade urgente de estudos e *framework*s para auxiliar na adaptação e na conformidade dos órgãos públicos com a LGPD.

A criação da Autoridade Nacional de Proteção de Dados (ANPD), em dezembro de 2018, responsável por normatizar, interpretar e fiscalizar a LGPD, foi um passo essencial. Contudo, a conformidade dos órgãos públicos brasileiros ainda é limitada, causando preocupação para os gestores. A falta de adesão expõe as entidades e seus gestores a sanções legais.

Para ajudar na adequação, a Secretaria de Governo Digital do Ministério da Economia lançou o Guia do *Framework* de Privacidade e Segurança da Informação (Guia LGPD)[1], que oferece orientações de boas práticas para a Administração Pública Federal. Em janeiro de 2022, a ANPD publicou o Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público[2], com parâmetros para auxiliar na adequação e implementação da LGPD.

Este estudo visa desenvolver um *framework* conceitual para apoiar órgãos e entidades públicas na adaptação de seus processos à LGPD. O objetivo é identificar as ações necessárias para garantir a conformidade com a lei, evitando sanções legais e promovendo a segurança dos dados pessoais dos cidadãos.

[1]Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos>. Acesso em: 23 mar. 2023.
[2]Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico/>. Acesso em: 23 mar. 2024.

A adequação dos dados pessoais no setor público enfrenta desafios, como compatibilizar prerrogativas estatais com os princípios da LGPD. O Guia da ANPD destaca a importância de equilibrar o direito à privacidade com o direito à informação pública, afirmando que a publicidade é a regra, exceto em casos excepcionais da Lei de Acesso à Informação (Brasil, 2022).

Em 2021, o Tribunal de Contas da União (TCU) auditou a conformidade das organizações públicas com a LGPD. Dos 382 órgãos entrevistados, apenas 45% concluíram a preparação necessária. O relatório final[3] revelou que 77% das organizações não identificaram todas as categorias de titulares de dados, 70% não avaliaram controladores conjuntos, 25% não possuem política de segurança da informação, e 65% não possuem política de classificação. Apenas 29% têm planos de capacitação em proteção de dados, e 46% documentaram as finalidades das atividades de tratamento. Além disso, 51% não avaliaram a coleta de dados necessários, e 61% não avaliaram a retenção dos dados.

A proteção à privacidade e o tratamento adequado de dados pessoais são desafios cruciais em uma sociedade digital em evolução. Estes desafios são maiores no setor público, onde a sociedade demanda menos burocracia e mais eficiência, ao mesmo tempo que exige proteção de dados pessoais. Esta pesquisa se justifica pela complexidade e sensibilidade do tema, propondo um *framework* que assegure a conformidade com a LGPD, promovendo segurança jurídica e confiança nas instituições públicas.

2. REFERENCIAL TEÓRICO

O referencial teórico explora a evolução da privacidade e distinção entre privacidade e proteção de dados, destacando o GDPR da União Europeia como uma legislação influente. Em seguida, examina-se a Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil, inspirada no GDPR, e suas implicações. Aborda-se também a adaptação de bancos de dados legados às novas exigências legais, enfatizando os desafios no setor público. O objetivo é fornecer a base para desenvolver um *framework* de adequação de bancos de dados legados à LGPD.

2.1 Privacidade e proteção de dados

Na sociedade atual, conectada e dependente da tecnologia, os indivíduos precisam se identificar constantemente para acessar bens e serviços. Esta evolução transformou nosso relacionamento com dispositivos em rede. Dados pessoais alimentam todos os aspectos da vida na sociedade em rede (Castells; Cardoso, 2005). Uma vez no sistema, preferências e comportamentos de consumo são armazenados em grandes bancos de dados (Big Data),

[3]Diagnóstico do grau de implementação da LGPD na Administração Pública Federal. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>. Acesso em: 23 mar. 2024.

explorados por empresas para fins lucrativos, resultando em preocupações com a privacidade dos dados pessoais.

A primeira manifestação formal do direito à privacidade remonta a 1890, com o texto "O Direito à Privacidade"[4] dos advogados norte-americanos Samuel Warren e Louis Brandeis, definindo a privacidade como "o direito de ser deixado sozinho". A Declaração Universal dos Direitos Humanos (1948), no art. 12, reforçou este direito, destacando a privacidade como essencial para o desenvolvimento da personalidade individual e a proteção da dignidade humana.

Na Europa, a Convenção Europeia dos Direitos Humanos (1950)[5], em seu artigo 8º, assegurou o respeito pela vida privada e familiar. No Brasil, a Constituição Federal, no art. 5.º, inciso X, protege a privacidade, garantindo indenização por danos materiais ou morais decorrentes de sua violação (Andrade, 2015).

Os conceitos de privacidade e de proteção de dados frequentemente se confundem. Rodotà (2009) distingue-os: privacidade é o controle sobre a própria informação e a construção da esfera privada, enquanto proteção de dados é um conjunto de direitos fundamentais no novo milênio. A evolução do conceito de privacidade, de "ser deixado em paz" ao controle sobre as informações, culmina na proteção de dados (Rodotà, 2009).

Em 1981, o Conselho Europeu adotou a Convenção 108[6] para a Proteção das Pessoas Singulares no Tratamento Automatizado de Dados Pessoais, o primeiro instrumento internacional vinculativo na proteção de dados. A Convenção visa garantir os direitos e liberdades fundamentais, especialmente o direito à vida privada, frente ao tratamento automatizado de dados pessoais. O Protocolo de alteração ampliou seu escopo, aumentando o nível de proteção e eficácia.

A Convenção de Proteção de Dados representou um avanço significativo, abrangendo todas as esferas da vida social, como raça, posicionamento político, saúde, religião, vida sexual e ficha criminal (Caetano, 2020). Este progresso normativo europeu culminou no Regulamento Geral de Proteção de Dados (GDPR), influenciando normas globais, incluindo a Lei Geral de Proteção de Dados (LGPD) brasileira, que serão discutidas nas seções seguintes.

2.2 Regulamento Geral de Proteção de Dados (GDPR)

O Supervisor Europeu de Proteção de Dados[7] considera as leis da UE um "padrão ouro" mundial. A primeira diretiva europeia sobre proteção de dados pessoais data de 1995, início da era da Internet. Este caminho culminou com a adoção do Regulamento Geral de Proteção de Dados (GDPR) em 2016 por todos os Estados-membros da UE. Para entender essa evolução, o

[4]The Right to Privacy. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 23 mar. 2024.
[5]Disponível em: <https://www.echr.coe.int/documents/convention_por.pdf>. Acesso em: 23 mar. 2024.
[6]Disponível em: <https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>. Acesso em: 23 mar. 2024.
[7]Disponível em: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>. Acesso em: 24 mar. 2024.

Supervisor Europeu de Proteção de Dados apresenta uma linha do tempo no Quadro 1 (União Europeia, 2018).

Quadro 1 – Linha do tempo dos eventos mais relevantes

Data	Evento Importante	Descrição
24/10/1995	Diretiva 95/46/CE	Adoção da primeira diretiva de proteção de dados pessoais na UE.
25/01/2012	Proposta de Reformulação	Proposta para fortalecer as regras de proteção de dados e adaptar à economia digital.
12/03/2014	Aprovação pelo Parlamento Europeu	GDPR aprovado com ampla maioria.
27/04/2016	Publicação do GDPR	Publicação oficial do GDPR, regulamentando a proteção de dados pessoais na UE.
25/05/2018	Aplicação do GDPR	Início da aplicação obrigatória do GDPR em todos os Estados-membros da UE.

Fonte: União Europeia (2018).

O GDPR, diferente de uma diretiva, é aplicável diretamente e deve ser implementado uniformemente em todos os Estados da UE, sem mudanças nas leis nacionais (Lee, 2018; Diblle, 2020). Sua extraterritorialidade atinge qualquer organização que lide com dados de cidadãos europeus, onde quer que esteja (Vermeulen; Lievens, 2017). Esta abordagem inspirou leis de proteção de dados em outros países, como a LGPD no Brasil, a Lei de Proteção de Dados Pessoais de 2019 na Tailândia e a Lei de Proteção de Informações Pessoais da China, de outubro de 2020 (Hsu, 2021). O GDPR tem 173 considerandos, 11 capítulos e 99 artigos, adotados por toda a UE, e influenciou diretamente leis globais de proteção de dados.

2.3 A Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, Lei nº 13.709, foi publicada em 14 de agosto de 2018. Seus dispositivos entraram em vigor em três etapas: em 28 de dezembro de 2018, apenas os artigos que criaram a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; em 1º de agosto de 2021, os artigos que previam sanções administrativas; e, em agosto de 2020, todos os demais dispositivos, 24 meses após a publicação.

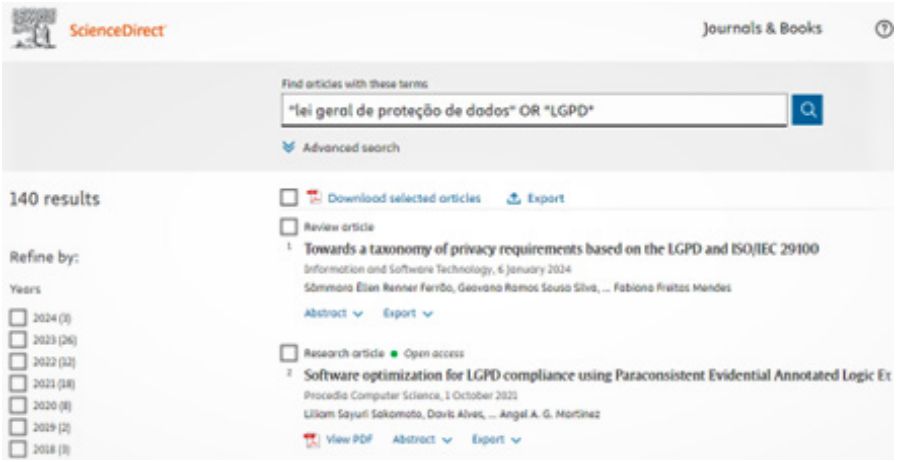
Para ampliar o conhecimento sobre o tema da pesquisa, optou-se por consultar a base Scopus, usando os argumentos de busca "lei geral de proteção de dados OR "LGPD". Foram localizados 140 documentos[8] (Figura 1).

Os documentos recuperados cobrem de 1993 a 2024, com foco maior a partir de 2020. Ferrão et al. (2024) identificaram que garantir conformidade com a legislação de privacidade de dados é um desafio para equipes de desenvolvimento de software. Eles propuseram uma

[8]Pesquisa realizada em 08/04/2024.

taxonomia de requisitos de privacidade baseada na LGPD para alinhar o desenvolvimento aos requisitos legais. Sakamoto et al. (2021) destacaram que a LGPD foi promulgada tardiamente no Brasil, exigindo mais conscientização sobre privacidade de dados, e propuseram homologar um software de proteção de dados para melhorar o controle de riscos. Ponce (2023) discutiu a discriminação nos algoritmos, alertando sobre o aumento da discriminação digital. Maple, Epiphaniou e Bottarelli (2021) notaram interesse crescente na privacidade, mas pouco conhecimento sobre medidas legais necessárias. Eles afirmaram que regulamentações, como o GDPR e a LGPD, buscam criar padrões para o uso de tecnologias e informações.

Figura 1 – Consulta à base Scopus



Fonte: (Scopus, 2024)

Demetzou, Zanfir-Fortuna e Vale (2023) exploraram leis de proteção de dados na UE e em seis jurisdições, focando na América Latina. Eles compararam como estas leis inspiradas no GDPR se aplicam à tomada de decisões automatizadas. Akanfe, Lawong e Rao (2024) discutiram conflitos entre Blockchain e regulamentação de privacidade, analisando 71 estudos para destacar áreas de atrito e propor uma estrutura unificadora. Peixoto et al. (2023) mostraram que desenvolvedores de software frequentemente ignoram requisitos de privacidade, com muitos brasileiros carecendo de conhecimento para criar sistemas que protejam dados.

Reilly (2021) afirmou que modelos de privacidade digital responsabilizam indivíduos pela proteção de dados, o que é insuficiente frente à coleta massiva on-line. Ele defendeu reformas legais para uma melhor proteção. Fantonelli et al. (2023) analisaram a gestão de dados de saúde em países com leis de proteção, concluindo que práticas, como regras de acesso e consentimento, são exemplos para o Brasil. Bueno e Canaan (2024) estudaram o impacto da Lei dos Serviços Digitais da UE no Projeto de Lei de Fake News do Brasil, usando entrevistas com especialistas para avaliar a influência regulatória da UE.

Os artigos revisados abordaram a complexidade e a importância da conformidade com a LGPD e outras regulamentações de privacidade, destacando a necessidade de conscientização,

adaptação tecnológica e implementação de políticas eficazes. Eles exploraram desafios, como discriminação algorítmica, conflitos com tecnologias emergentes, como blockchain, e a gestão de dados sensíveis. A revisão indicou a necessidade urgente de desenvolvimento de conhecimento e de ferramentas práticas para garantir a privacidade e proteção de dados pessoais, especialmente no contexto brasileiro.

2.4 Bancos de dados legados

Um banco de dados é uma coleção de dados que descreve as atividades de uma ou mais organizações relacionadas (Ramarkrishnan; Gehrke, 2011). Por exemplo, um banco de dados de uma universidade poderia conter informações sobre alunos, professores, cursos e turmas; além de relacionamentos entre as entidades, como a matrícula dos alunos nos cursos, cursos ministrados pelos professores, e o uso de salas por cursos. Um sistema de gerenciamento de dados (SGBD) é um software para auxiliar a manutenção e utilização de vastos conjuntos de dados.

Elmasri e Navathe (2005) definiram um SGBD como um conjunto de programas que permite aos usuários criar e manter um banco de dados. O SGBD é um sistema de software de propósito geral que facilita a definição, a construção, a manipulação e o compartilhamento de bancos de dados entre vários usuários e aplicações.

Um banco de dados é legado quando armazena dados usados por um sistema ou software desenvolvido por uma tecnologia "mais antiga" comparada às atuais, chamada "tecnologia legada". Quando se opta por iniciar o desenvolvimento de um novo sistema de tecnologia da informação, reescreve-se o código-fonte ou comandos, em uma linguagem computacional mais atual. O novo software reescrito geralmente necessitará de um banco de dados mais moderno e ágil para armazenamento das informações, antigas e novas. Os dados terão que ser migrados do banco de dados legado para o novo.

O objetivo deste estudo é desenvolver um *framework* que auxilie órgãos e entidades públicas na adequação dos bancos de dados legados à LGPD. Esses bancos de dados não precisam ser de tecnologias antigas, mas não foram adaptados às novas exigências da LGPD que serão abordadas na seção do *Framework* Proposto.

A LGPD, em seu artigo 63, já trouxe essa preocupação:

> Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados (Brasil, 2018).

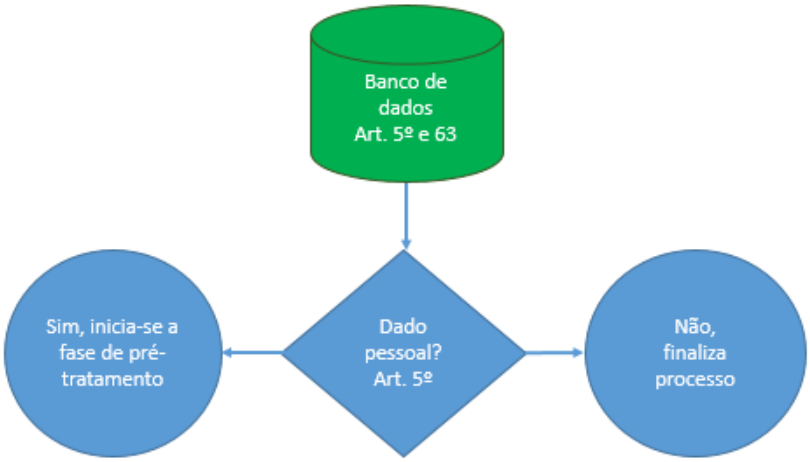
A modernização e a adequação dos bancos de dados legados são essenciais para garantir a conformidade com a LGPD. A transição de sistemas baseados em tecnologias legadas para plataformas modernas e eficientes melhora o gerenciamento e segurança dos dados, e assegura que as práticas de tratamento de dados estejam alinhadas com as exigências legais atuais. A

LGPD reconhece a importância dessa adaptação progressiva, destacando a necessidade de normas claras para orientar esse processo. Portanto, um *framework* bem desenvolvido auxiliará os órgãos e entidades públicas na implementação das normas de proteção de dados, promovendo a segurança e a privacidade das informações pessoais.

3. *FRAMEWORK* PROPOSTO

Após analisar a LGPD, conclui-se que antes do tratamento de dados pessoais existe uma fase de pré-tratamento. Nessa fase, parte-se de um banco de dados legado, conforme o Art. 63 da Lei, e avalia-se se este banco contém dados pessoais (Art. 5º I). Se a resposta for negativa, o processo está finalizado e não há "tratamento". Se a resposta for positiva, inicia-se o pré-tratamento de dados pessoais, conforme Figura 2.

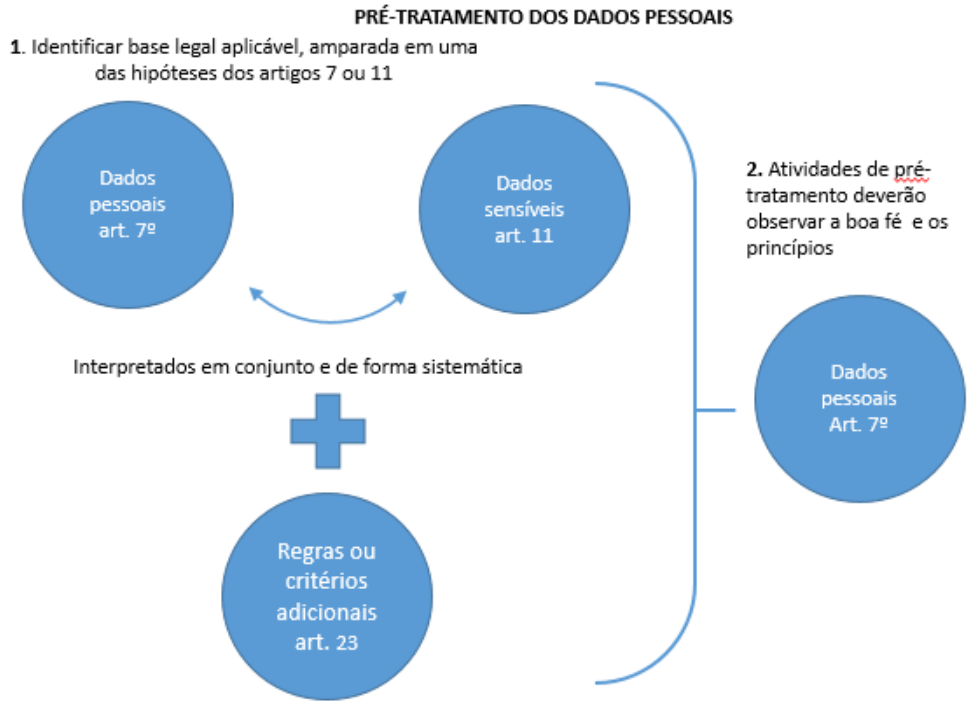
Figura 2 – Processo inicial



Fonte: Elaborada pelos autores (2024)

Na fase de pré-tratamento (Figura 3), o primeiro passo é identificar a base legal aplicável na LGPD, verificando se os dados estão amparados em uma das hipóteses dos artigos 7º (dados pessoais) ou 11 (dados pessoais sensíveis). Segundo o Guia da ANPD, ambos os artigos devem ser interpretados em conjunto. Também deve-se verificar se as regras ou critérios adicionais (Art. 23) foram observados. Por fim, para fechar a análise do pré-tratamento, deve-se certificar de que todas as atividades estejam alinhadas aos princípios da lei (Art. 6º).

Figura 3 – Fase de pré-tratamento



Fonte: Elaborada pelos autores (2024)

O tratamento de dados pessoais, ou seja, as 19 atividades operacionais (Quadro 2) do Art. 5º X se iniciam se o banco de dados analisado atender aos requisitos da fase de pré-tratamento. Porém, esta fase não é objeto de estudo deste trabalho.

Quadro 2 – Tratamento de dados

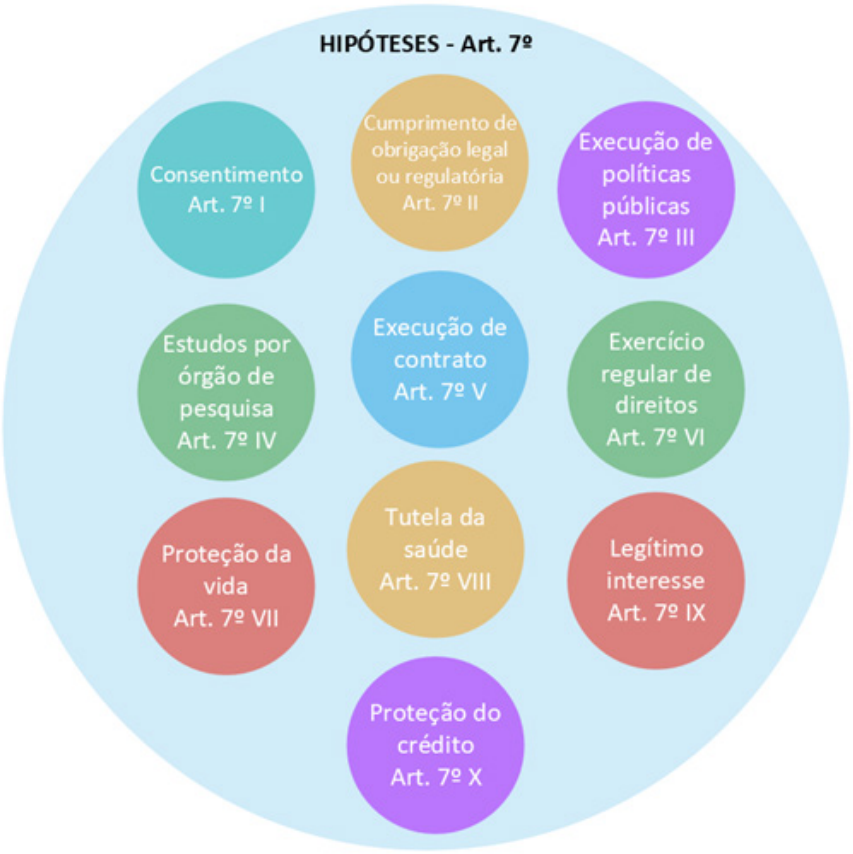
coleta	arquivamento
produção	armazenamento
recepção	eliminação
classificação	avaliação ou controle da informação
utilização	modificação
acesso	comunicação
reprodução	transferência
transmissão	difusão
distribuição	extração
processamento	-

Fonte: Art. 5º X da LGPD (2018)

Para um dado pessoal avançar à fase de tratamento, é necessário atender a pelo menos uma das bases legais do Art. 7º da LGPD (Figura 4).

A ANPD, no seu Guia Orientativo para tratamento de dados pessoais pelo poder público, enfatiza as quatro bases legais mais comuns apresentadas como justificativas por um órgão ou entidade pública ao tratar um dado pessoal: consentimento, legítimo interesse, cumprimento de obrigação legal ou regulatória e execução de políticas públicas.

Figura 4 – Bases legais para tratamento de dados pessoais



Fonte: Elaborada pelos autores (2024)

Embora o consentimento (Art. 7º I) seja típico em tratamentos por entes privados, e o poder público exercer prerrogativas estatais que o dispensem, o consentimento pode ser admitido para o tratamento de dados pelo Poder Público. São casos em que o ente estatal prefere assegurar ao titular a possibilidade de autorizar ou não o tratamento de seus dados. O Guia da ANPD exemplifica:

> Matrícula de estudante em universidade pública
> Universidade pública solicita de novos estudantes o fornecimento de dados pessoais necessários para fins de cadastro e matrícula. O procedimento é realizado on-line e, para prosseguir para as etapas seguintes, com a escolha de disciplinas e horários, o estudante deve "aceitar" as condições estipuladas para o tratamento de seus dados. Essas condições são descritas de forma genérica, com a indicação de que os dados poderão ser utilizados para "fins educacionais e outros correlatos". Uma mensagem indica que, caso não fornecido o consentimento, a matrícula não será concluída e o estudante não terá acesso ao curso e a serviços como os de assistência estudantil e empréstimo de livros na biblioteca. No exemplo citado, o consentimento eventualmente obtido será nulo, pois: (i) os estudantes não possuem condições efetivas de aceitar

> ou recusar o tratamento de seus dados pessoais, haja vista o caráter compulsório do tratamento realizado pela universidade; e (ii) a autorização é fornecida para uma finalidade genérica. Com o objetivo de adequar as suas práticas ao disposto na LGPD, a universidade deve fornecer informações claras e precisas sobre a finalidade específica do tratamento, identificando outra base legal mais apropriada para a hipótese, que não o consentimento. Ainda, em atenção ao princípio da necessidade, não devem ser solicitados mais dados do que o necessário para atingir as finalidades informadas ao titular (Brasil, 2022).

A base legal do legítimo interesse (Art. 7º IX) prevê o tratamento de dados pessoais "não sensíveis" quando necessário para atender interesses legítimos do controlador. Assim como no consentimento, invocar o legítimo interesse não é apropriado quando o ente público precisa tratar dados compulsoriamente ou para cumprir obrigações legais. Recomenda-se que o Poder Público pondere as expectativas dos titulares dos dados pessoais com os interesses estatais, e observe se a imputação da base legal legítimo interesse não criará restrições aos direitos individuais.

O cumprimento de obrigação legal ou regulatória (Art. 7º, II) invoca a base legal em duas situações: normas de conduta e normas de organização. No primeiro caso, o tratamento de dados pessoais é necessário para atender a uma determinação legal expressa ou a uma obrigação de um órgão regulador, decorrente de uma conduta ou regra que disciplina um comportamento. No segundo caso, a base legal está fundamentada nos normativos que estruturam os órgãos e as entidades públicas, a partir de suas competências e atribuições. Resumindo, as normas de conduta estabelecem obrigações de forma direta e expressa, enquanto as normas de organização estão vinculadas às atribuições legais do órgão público.

A execução de políticas públicas (Art. 7º III) regula o tratamento de dados pessoais necessários à execução de políticas públicas previstas em leis e regulamentos, ou respaldadas em contratos, convênios ou instrumentos similares. A ANPD recomenda interpretar o conceito de política pública de forma ampla, para abranger qualquer programa ou ação governamental formalmente estabelecida.

Para que um dado pessoal sensível avance à fase de tratamento, é necessário que atenda a uma das bases legais do Art. 11º da LGPD. Segundo a LGPD, o tratamento de dados pessoais sensíveis ocorrerá em duas hipóteses legais, com subdivisões da segunda:

1. Quando o titular ou seu responsável legal consentir;
2. Sem consentimento do titular, quando 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;

e) roteção da vida ou da incolumidade física do titular ou de terceiros;

f) utela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) rantia da prevenção à fraude e à segurança do titular.

Comparando as bases legais de pré-tratamento para dados pessoais sensíveis (Art. 11) e não-sensíveis (Art. 7), tem-se o Quadro 3.

Quadro 3 – Comparativo das bases legais

Base Legal	Dados Pessoais (Art. 7)	Dados Pessoais Sensíveis (Art. 11)
1. Consentimento	Mediante consentimento do titular.	Mediante consentimento do titular ou de seu responsável legal.
2. Obrigação Legal	Para o cumprimento de obrigação legal ou regulatória pelo controlador.	Para o cumprimento de obrigação legal ou regulatória pelo controlador.
3. Políticas Públicas	Para a execução de políticas públicas pela administração pública.	Para o tratamento compartilhado de dados necessários à execução de políticas públicas pela administração pública.
4. Estudos e Pesquisas	Para a realização de estudos por órgãos de pesquisa, garantida a anonimização.	Para a realização de estudos por órgãos de pesquisa, garantida a anonimização, sempre que possível.
5. Contratos	Para a execução ou preparação de contratos.	Para o exercício regular de direitos em contratos e em processos judiciais, administrativos ou arbitrais.
6. Direitos Legais	Para o exercício regular de direitos em processos judiciais, administrativos ou arbitrais.	Para o exercício regular de direitos, inclusive em contratos e processos judiciais, administrativos ou arbitrais.
7. Proteção à Vida	Para a proteção da vida ou da incolumidade física do titular ou de terceiros.	Para a proteção da vida ou da incolumidade física do titular ou de terceiros.
8. Saúde	Não aplicável.	Para a tutela da saúde, exclusivamente, por profissionais ou serviços de saúde, ou autoridades sanitárias.
9. Legítimo Interesse	Para atender interesses legítimos do controlador ou de terceiro.	Não aplicável.
10. Proteção ao Crédito	Para a proteção ao crédito.	Não aplicável.
11. Prevenção à Fraude	Não aplicável.	Para a garantia da prevenção à fraude e à segurança do titular.

Fonte: Elaborado pelos autores (2024)

Analisando o quadro comparativo, o Art. 7 prevê 10 bases legais, enquanto o Art. 11 prevê 8. O Art. 11 resume 2 bases legais do Art. 7 em uma única e inova com a base legal de tratamento para a prevenção à fraude e à segurança. Assim, chega-se a 11 (onze) bases legais de tratamento distintas. A Figura 4 anterior precisa ser revisada para representar corretamente a conjugação das bases legais dos dois artigos da lei, conforme a Figura 5.

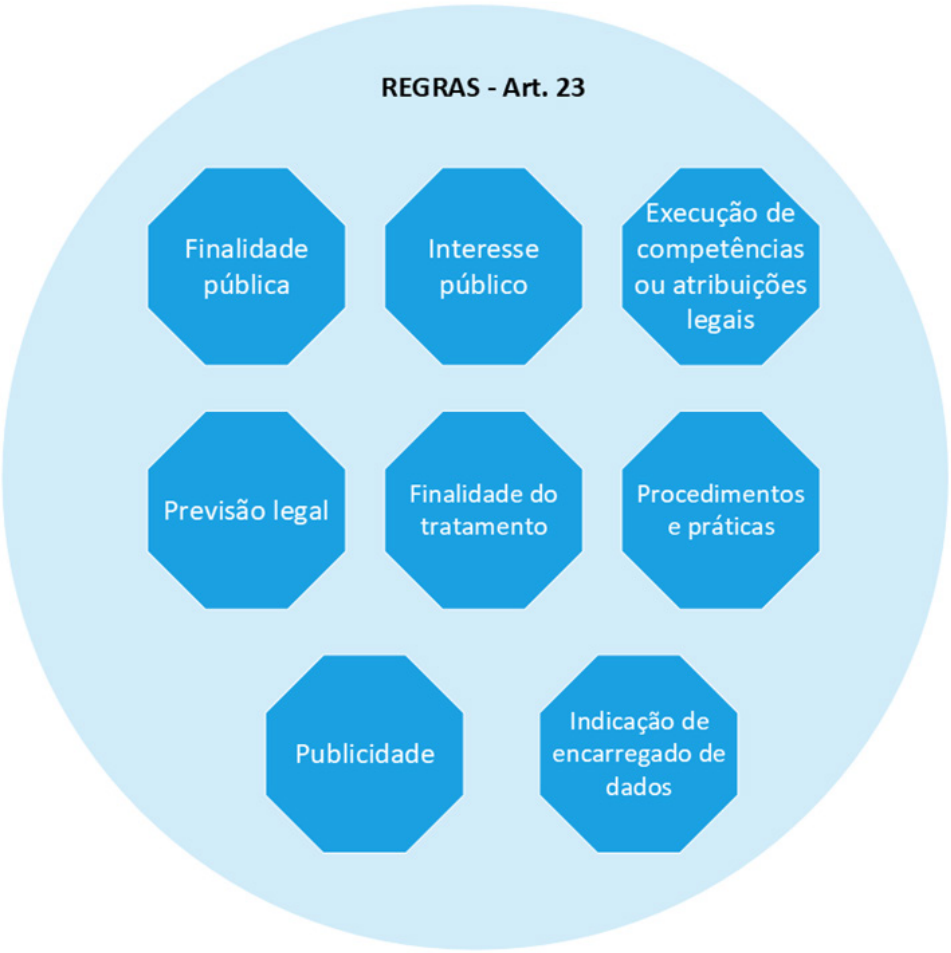
Figura 5 – Bases legais conjugadas

Fonte: Elaborada pelos autores (2024)

O capítulo IV da LGPD, "DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO", seção I, artigo 23, estipula que o tratamento de dados pessoais por entidades públicas deve atender a sua finalidade pública, perseguindo o interesse público e executando suas competências legais. O Guia da ANPD destaca a importância de interpretar as bases legais dos artigos 7º e 11 em conjunto com os critérios adicionais do artigo 23 (incisos I a III). Na visão deste autor, as regras e critérios que se aplicam à etapa de pré-tratamento de dados no setor público são (Figura 6):

a) Finalidade pública do tratamento;
b) Interesse público no tratamento;
c) Execução de competências ou atribuições legais;
d) Previsão legal do tratamento;
e) Finalidade do tratamento;
f) Informação sobre os procedimentos e práticas do tratamento;
g) Publicidade das operações de tratamento;
h) Indicação de encarregado de dados.

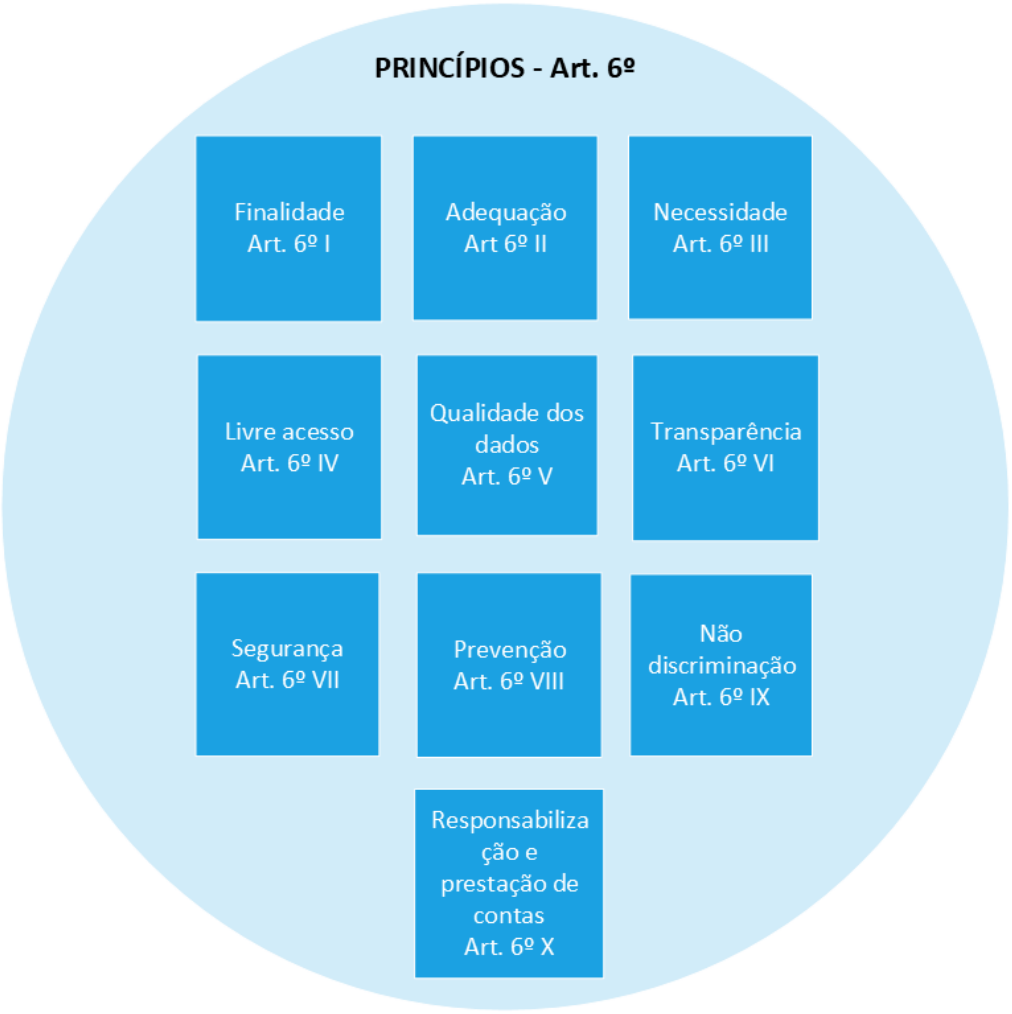
Figura 6 – Regras e critérios para tratamento



Fonte: Elaborada pelos autores (2024)

Por fim, segundo o Art. 6º da LGPD, as atividades de tratamento de dados pessoais devem observar a boa fé e os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Os princípios do *framework* proposto podem ser representados pela Figura 7.

Figura 7 – Princípios para o tratamento de dados pessoais



Fonte: Elaborada pelos autores (2024).

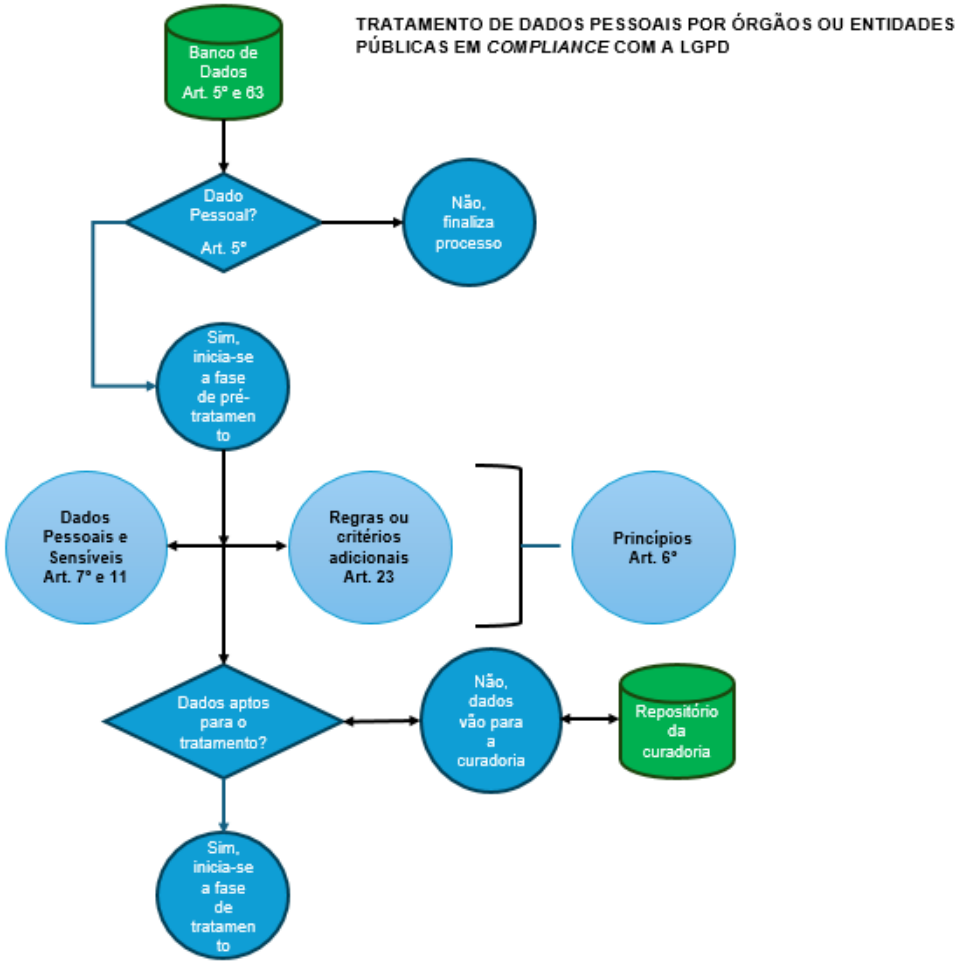
Após concluir a fase de pré-tratamento de dados, surge uma pergunta importante: os dados estão prontos para avançar para a fase operacional de tratamento? Se a resposta for "sim", entende-se que todos os requisitos foram cumpridos, mas podem restar dados pessoais não claramente enquadrados. Para solucionar estas exceções, sugere-se criar uma rotina de curadoria e um repositório, onde esses dados ficariam armazenados aguardando uma decisão humana (Figura 8).

Em um processo automatizado, é normal haver uma curadoria manual, principalmente com dados não objetivos. Isso elimina dúvidas de enquadramento dos dados, permitindo que todos avancem para o tratamento. Após a apresentação das etapas da fase de pré-tratamento, a Figura 9 mostra a visão geral do *framework* proposto.

Figura 8 – Curadoria

Fonte: Elaborada pelos autores (2024)

Figura 9 – Visão geral do *framework* proposto



Fonte: Elaborada pelos autores (2024)

O Quadro 4 apresenta uma síntese dos critérios de conformidade com base no *framework* proposto, visando sistematizar os principais critérios para adaptar bancos de dados legados às exigências da LGPD. Estes critérios servem como referência para órgãos públicos avaliarem e assegurarem a conformidade de seus processos de tratamento de dados pessoais, garantindo que estejam de acordo com as disposições legais.

Quadro 4 – Síntese dos critérios de conformidade

Critério de Conformidade	Descrição	Base Legal (LGPD)
Identificação de Dados Pessoais	Verificar se o banco de dados contém dados pessoais ou sensíveis, conforme definido pela LGPD.	Art. 5º, I
Verificação da Base Legal	Garantir que o tratamento dos dados está amparado por uma das bases legais especificadas nos artigos 7º (dados pessoais) ou 11º (dados sensíveis).	Art. 7º e Art. 11º
Aplicação de Princípios da LGPD	Assegurar que o tratamento de dados observe os princípios fundamentais da LGPD, como finalidade, adequação, necessidade, livre acesso, transparência e segurança.	Art. 6º
Cumprimento de Critérios Adicionais	No caso de dados tratados por órgãos públicos, verificar o cumprimento dos critérios adicionais: finalidade pública, interesse público e execução de competências legais.	Art. 23
Medidas de Segurança e Proteção	Implementar medidas técnicas e administrativas adequadas para proteger os dados contra acessos não autorizados e incidentes de segurança.	Art. 46º
Curadoria de Dados	Criar uma rotina de curadoria para tratar dados que não se enquadram claramente nas bases legais ou princípios, antes do processamento automatizado.	Parte integrante do *framework* proposto (baseado na interpretação do Art. 5º e 6º da LGPD)
Consentimento ou Outra Base Legal	Garantir que, para dados coletados com consentimento, este seja válido e específico; ou utilizar outra base legal adequada para o tratamento.	Art. 7º e Art. 11º
Anonimização ou Pseudonimização	Adotar técnicas de anonimização ou pseudonimização para proteger a identidade dos titulares de dados sempre que possível.	Art. 13º, II (pseudonimização) e Art. 12º (anonimização)
Tratamento de Dados Sensíveis	Verificar se o tratamento de dados pessoais sensíveis segue os requisitos legais mais restritos, conforme o Art. 11 da LGPD.	Art. 11º
Execução de Políticas Públicas	No caso de órgãos públicos, assegurar que o tratamento de dados está alinhado à execução de políticas públicas, conforme regulamentações aplicáveis.	Art. 7º, III

Fonte: Elaborado pelos autores (2024)

Cada critério visa facilitar a verificação de conformidade e fornecer um guia claro para implementar as exigências legais da LGPD. Os principais pontos destacados são a identificação de dados pessoais, a verificação da base legal para o tratamento, a aplicação dos princípios da LGPD e a implementação de medidas de segurança e rotinas de curadoria de dados.

O Quadro sintetiza os parâmetros para assegurar que os bancos de dados atendam às exigências da LGPD, promovendo a segurança jurídica e a proteção dos dados pessoais dos cidadãos. Este instrumento oferece uma base sólida para a governança de dados, facilitando o processo de adequação e mitigando riscos de não conformidade e sanções legais.

4. VALIDAÇÃO PRELIMINAR DO *FRAMEWORK* PROPOSTO

Para validar, preliminarmente, o *framework* proposto, foram coletados arquivos do Portal Brasileiro de Dados Abertos[9]. Foram acrescentados a esses arquivos dados pessoais, para que os registros resultantes ficassem próximos de uma base de dados legada real. Assim, ao submeter um ou mais arquivos ao *framework* proposto, fosse possível simular um caso concreto de pré-tratamento de dados pela LGPD.

Para a segunda etapa de análise de dados e validação preliminar do *framework* proposto, foram realizadas entrevistas com especialistas em LGPD de órgãos públicos. Eles realizaram análises críticas do *framework*, utilizando suas próprias bases de dados legadas.

Apresentado o *framework* proposto, e em atendimento aos objetivos da pesquisa, segue o momento de validá-lo a partir de um banco de dados real. Permite-se que esse banco possa sofrer pequenas alterações para validação teórica, ou seja, foram simulados modelos de BD para atender a todas as hipóteses possíveis. Neste estudo, observaram-se 6 hipóteses de bancos de dados (BD) legados diferentes:

a) BD sem dados pessoais OU;

b) BD com dados pessoais OU;

c) BD com dados pessoais sensíveis OU;

d) BD com dados anonimizados OU;

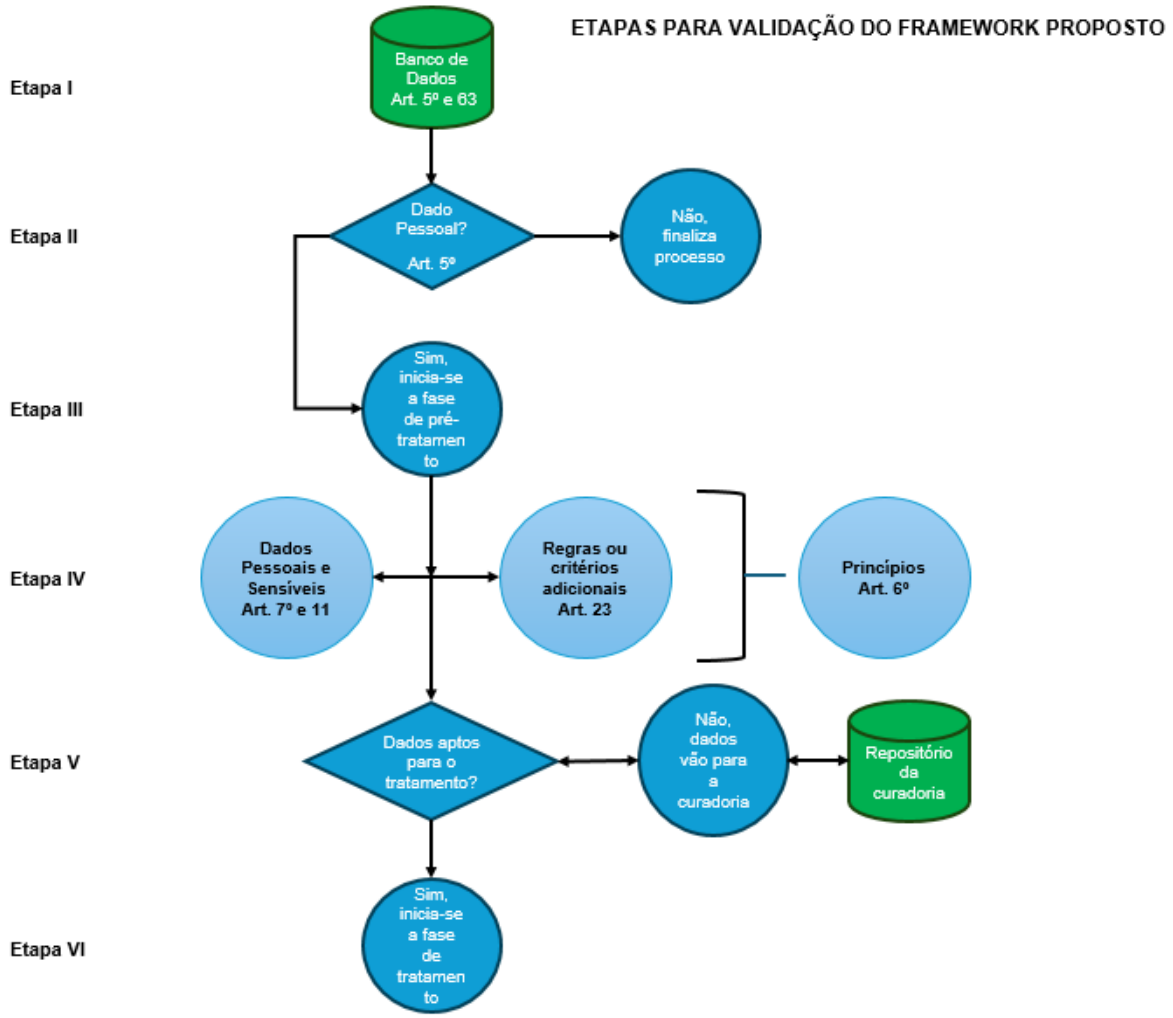
e) BD com dados pseudonimizados OU;

f) BD com dois ou mais dados dos itens anteriores (a/b/c/d/e).

Para facilitar o entendimento e a validação, o *framework* proposto foi dividido em 6 etapas, conforme a Figura 10.

[9]Portal Brasileiro de Dados Abertos. Disponível em: < https://dados.gov.br/>. Acesso em: 24 mar. 2024.

Figura 10 – *Framework* proposto em etapas



Fonte: Elaborada pelos autores (2024)

Após a primeira fase de validação do *framework* proposto, este foi submetido à avaliação de especialistas de entidades do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), com maior maturidade no tema. Doze representantes de órgãos públicos aceitaram participar da entrevista. As orientações sobre a pesquisa e o roteiro de entrevista foram enviadas previamente para os profissionais que aceitaram o convite. As entrevistas ocorreram em julho, agosto e setembro de 2022, por videoconferências, registradas com Google Meet ou Microsoft Teams. Devido às dificuldades no agendamento e à necessidade de finalizar a pesquisa, foram entrevistados os especialistas listados no Quadro 5.

Quadro 5 – Especialistas que contribuíram com a pesquisa

Identificação	Área	Órgão
Entrevistado A	Coordenação de Privacidade e Proteção de Dados	SERPRO
Entrevistado B	Coordenação-Geral de Departamento de Privacidade e Segurança da Informação	Secretaria de Governo Digital do Ministério da Economia
Entrevistado C	Encarregado de Dados	Secretaria Executiva do Ministério da Economia
Entrevistado D	Encarregado de Dados e *Data Protection Officer* – DPO	Casa Civil da presidência da República
Entrevistado E	Encarregado de Dados	Instituto Federal de Santa Catarina
Entrevistado F	Encarregado de Dados	Ministério de Minas e Energia
Entrevistado G	Governança de Dados	Ministério do Desenvolvimento Social

Fonte: Elaborado pelos autores (2024)

Os entrevistados responderam a oito perguntas sobre o *framework*, destacando: bases legais, regras ou critérios adicionais, princípios, sequência, acréscimo de hipóteses, aplicação/validação, verificação da conformidade dos bancos de dados legados e outras sugestões.

A reorganização do *framework* proposto foi atualizada com as sugestões dos entrevistados, de acordo com suas experiências. Algumas contribuições foram aceitas pelos autores deste estudo. Outras motivaram novas reuniões para melhor entendimento, enquanto algumas não foram aceitas parcialmente ou descartadas.

Não houve novas contribuições das entrevistas, que ratificaram o entendimento dos autores. Optou-se por reescrever as regras ou critérios:

a) Finalidade pública do tratamento;

b) Interesse público no tratamento;

c) Execução de competências ou atribuições legais;

d) Previsão legal do tratamento;

e) Informação sobre os procedimentos e práticas do tratamento;

f) Publicidade das operações de tratamento;

g) Indicação de encarregado de dados.

Sobre os princípios, não houve contribuição que requeresse alterar o *framework* proposto, apenas sugestões para trabalhos futuros. Quanto ao sequenciamento do *framework*, a maioria dos entrevistados concordou com a disposição apresentada. Quanto às hipóteses de bancos de dados diferentes, os entrevistados sugeriram uma nova redação:

a) BD sem dados pessoais OU;

b) BD com dados pessoais OU;

c) BD com dados pessoais sensíveis OU;

d) BD com dados descaracterizados OU;

e) BD com dois ou mais dados dos itens anteriores (b/c/d).

Assim, foram eliminadas as hipóteses de dados anonimizados e pseudonimizados, e substituídas por descaracterizados, ou seja, dados que ainda não foram tratados, mas tiveram sua forma ou aparência alteradas. Ainda sobre as hipóteses, houve uma importante contribuição de um entrevistado, sugerindo a inclusão no *framework* a base legal do Art. 14 da LGPD, que prevê o tratamento de dados pessoais de crianças e adolescentes.

Sobre a aplicação/validação, foi recebida uma sugestão para melhorar a descaracterização da data de nascimento do titular dos dados, para que sua idade não seja identificada. Sobre a verificação de conformidade, não foram recebidas contribuições relevantes. Os entrevistados fizeram sugestões para estudos futuros e recomendações sobre o conceito de anonimização e pseudonimização, já tratados na revisão do *framework*.

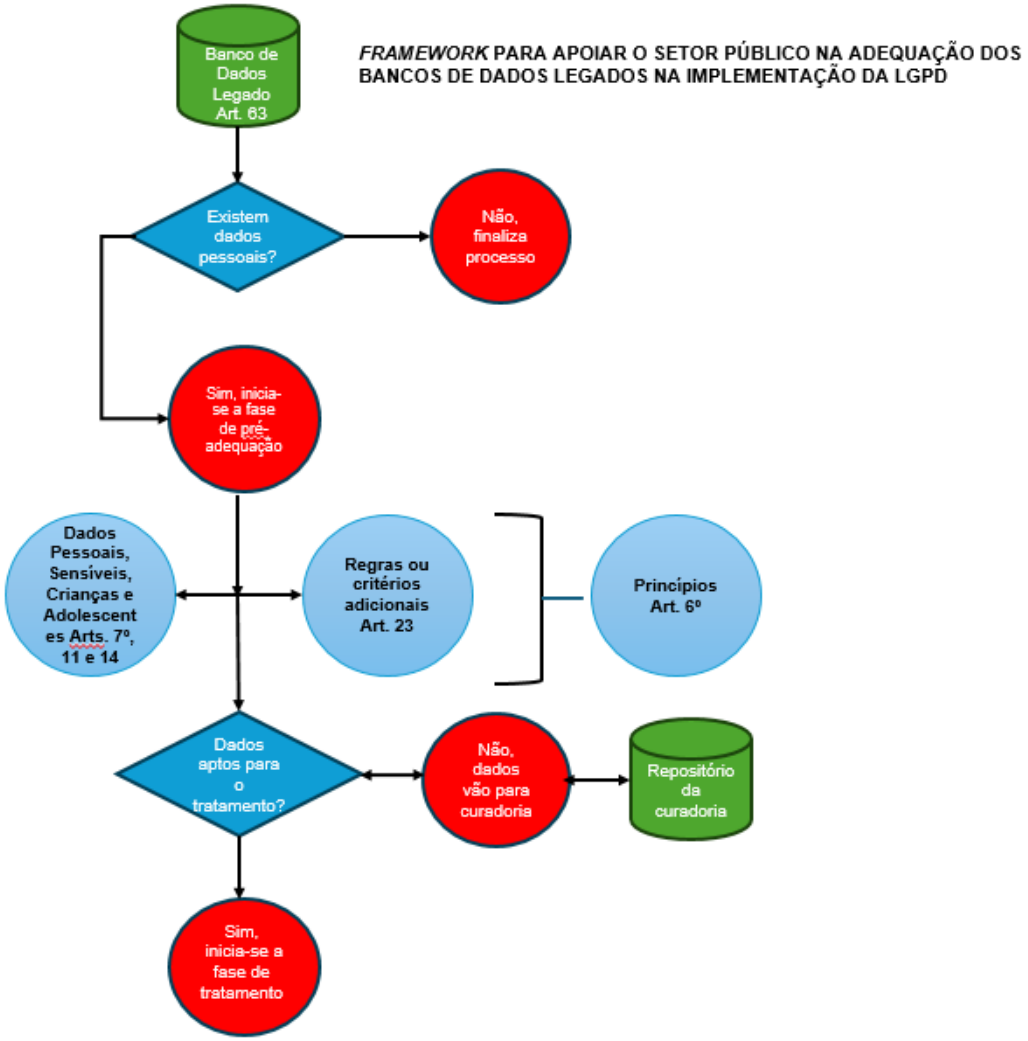
Portanto, a visão geral do *framework* inicial evoluiu para o modelo apresentado na Figura 11. O órgão ou entidade pública com bancos de dados legados poderá usar o *framework* proposto para iniciar a adequação preliminar dos dados à LGPD.

5. DISCUSSÃO DOS RESULTADOS

O *framework* proposto para adequação de bancos de dados legados à LGPD se fundamentou em uma análise do referencial teórico sobre a evolução da privacidade e proteção de dados, com ênfase nas influências do GDPR da União Europeia. A literatura revisada destacou a importância de diferenciar privacidade de proteção de dados. Conforme Rodotà (2009), privacidade envolve controle sobre a informação, enquanto proteção de dados abrange direitos fundamentais na era digital. O *framework* proposto incorporou essa distinção, garantindo que os princípios de privacidade e proteção de dados sejam aplicados desde a fase de pré-tratamento dos dados pessoais. Essa abordagem assegura que os dados pessoais sejam gerenciados conforme as expectativas legais e éticas, promovendo a proteção da privacidade dos cidadãos.

O GDPR, padrão ouro global de proteção de dados, influenciou a criação da LGPD no Brasil. A análise do GDPR revelou a importância de uma legislação robusta e extraterritorial que assegura direitos de privacidade independentes da localização do controlador dos dados (Lee, 2018; Vermeulen; Lievens, 2017). O *framework* proposto adotou uma abordagem semelhante ao GDPR, integrando princípios fundamentais de proteção de dados e requisitos legais específicos da LGPD. Isso garante que os bancos de dados legados atendam às normas exigidas, mitigando riscos e assegurando a conformidade.

Figura 11 – Modelo final do *framework*



Fonte: Elaborada pelos autores (2024)

O referencial teórico explorou os desafios na adaptação de bancos de dados legados no setor público. A literatura indicou que a maioria dos órgãos públicos enfrenta dificuldades para se adequar à LGPD (Brasil, 2022). O *framework* proposto abordou esses desafios ao fornecer uma estrutura clara e sistemática para identificar e tratar dados pessoais conforme as exigências legais. A metodologia adotada, que incluiu a validação com especialistas, assegurou que o *framework* seja prático e aplicável no contexto real dos órgãos públicos brasileiros.

A LGPD estabelece diversas bases legais para o tratamento de dados pessoais, conforme Art. 7º e 11. O *framework* integrou essas bases de forma estruturada, permitindo que os órgãos públicos avaliem e justifiquem cada operação de tratamento de dados. Além disso, o *framework* incorporou os princípios da LGPD, como finalidade, adequação, necessidade, transparência, e segurança, assegurando que todas as atividades de tratamento de dados sejam realizadas em conformidade com a lei (Brasil, 2018).

A implementação do *framework* proposto indica critérios de conformidade com a LGPD e fortalece a governança de dados nos órgãos públicos. Estudos revisados (Ferrão et al., 2024; Peixoto et al., 2023) apontam que a falta de conhecimento e ferramentas para a proteção de dados é um desafio significativo. O *framework* ajuda a preencher essa lacuna, oferecendo diretrizes claras e práticas para a gestão de dados pessoais, promovendo a segurança jurídica e a confiança dos cidadãos nas instituições públicas.

6. CONSIDERAÇÕES FINAIS

A conclusão deste estudo destaca a relevância e a eficácia do *framework* proposto para adaptar bancos de dados legados à LGPD. Por meio da análise da legislação, literatura relevante e validação preliminar com especialistas, o *framework* se mostrou um guia prático e sistemático para auxiliar órgãos públicos na adequação de seus bancos de dados.

O *framework* aborda as exigências da LGPD, como a identificação de dados pessoais, verificação das bases legais, aplicação de princípios e implementação de medidas de segurança. A inclusão de uma fase de pré-tratamento garante que os dados estejam em conformidade antes do tratamento operacional. Esta abordagem minimiza riscos de não conformidade e sanções legais, promovendo a segurança jurídica e a confiança dos cidadãos nas instituições públicas.

Apesar dos resultados positivos, o *framework* proposto possui limitações: escalabilidade e generalização, complexidade técnica, adaptação a tecnologias legadas e *feedback* de usuários finais. Contudo, essas limitações apontam perspectivas de pesquisas futuras:

- aplicação em cenários mais amplos, como bancos de dados heterogêneos ou com grandes volumes de dados, que poderiam revelar desafios de escalabilidade e performance não abordados;

- verificar a capacidade técnica para lidar com dados pessoais e sensíveis, aprofundando a discussão sobre a complexidade técnica da implementação;

- análise da adaptação a diferentes sistemas de gestão de bancos de dados (SGBDs), incluindo os desafios da migração de dados em sistemas antigos e obsoletos, com limitações técnicas;

- verificar o impacto do *framework* para os usuários finais (gestores de dados e administradores de TI), que podem enfrentar dificuldades práticas na implementação e aplicação;

- inclusão de métricas quantitativas para medir a eficácia do *framework* com indicadores como o tempo de adequação, a redução de incidentes de segurança ou o grau de conformidade com a LGPD.

Este estudo contribui para a proteção de dados no setor público brasileiro, oferecendo um modelo estruturado e preliminarmente validado para adequar bancos de dados legados à LGPD. As implicações dos resultados são vastas, fornecendo uma base para a segurança jurídica

e a confiança dos cidadãos nos processos de tratamento de dados pelos órgãos públicos. Além disso, o *framework* indica práticas de governança de dados mais seguras, alinhadas às exigências da LGPD, servindo como referência para futuros estudos e aprimoramentos na proteção de dados pessoais.

REFERÊNCIAS

AKANFE, O.; LAWONG, D.; RAO, H. R. Blockchain technology and privacy regulation: reviewing frictions and synthesizing opportunities. **International Journal Of Information Management**, v. 76, 102753, jun. 2024. DOI: http://dx.doi.org/10.1016/j.ijinfomgt.2024.102753. Acesso em:30 jun. 2024.

ANDRADE, G. **Direito à privacidade**: intimidade, vida privada e imagem. Jusbrasil, 2015. Disponível em: <https://quentasol.jusbrasil.com.br/artigos/214374415/direito-a-privacidade-intimidade-vida-privada-e-imagem>. Acesso em: 23 mar. 2024.

BRASIL. Controladoria Geral da União (org.). **Portal Brasileiro de Dados Abertos**. Disponível em: <https://dados.gov.br/>. Acesso em: 20 mar. 2024.

BRASIL. **Ministério da Gestão e Inovação em Serviços Públicos. Secretaria de Governo Digital**. Guia do Framework de Privacidade e Segurança da Informação. Brasília, DF: Presidência da República 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos>. Acesso em: 23 mar. 2024.

BRASIL. **Ministério da Edu**cação. Fundo de Financiamento Estudantil. Disponível em: https://dados.gov.br/dataset/mec-fundo-de-financiamento-estudantil-fies. Acesso em: 23 mar. 2024.

BRASIL**. Ministério da Justiça e Segurança Púb**lica. Autoridade Nacional de Proteção de Dados. Guia Orientativo – Tratamento de Dados Pessoais pelo Poder Público. Brasília, DF, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico>. Acesso em: 23 mar. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 mar. 2024.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação. Brasília, DF: Presidência da República, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 15 mar. 2024.

BRASIL. [Constituição(1988)]. **Constituição da República Federativa do Brasil de 1988**. DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 23 mar. 2024.

BRASIL. Secretaria de Fiscalização de Tecnologia da Informação. **Diagnóstico do grau de implementação da Lei Geral de Proteção de Dados na Administração Pública Federal**. Brasília, DF: Tribunal de Contas da União,, 2022. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>. Acesso em: 23 mar. 2024.

BUENO, T. M.; CANAAN, R. G. The Brussels Effect in Brazil: analysing the impact of the EU digital services act on the discussion surrounding the fake news bill. **Telecommunications Policy**, v. 48, n. 5, 102757, mar. 2024. Elsevier BV. DOI: http://dx.doi.org/10.1016/j.telpol.2024.102757. Acesso em: 05 abr. 2024.

CAETANO, J. V. L. O regulamento geral de proteção de dados (GDPR): uma análise do extraterritorial scope à luz da jurisdição internacional. **Cadernos Eletrônicos**: Direito Internacional sem Fronteiras, Fortaleza, v. 2, n. 1, p. 1-25, 30 jun. 2020.

CASTELLS, M. **End of Millennium.** Oxford. Blackwell Publishing. 2010, p. 489.

CASTELLS, M; CARDOSO, G. **The Network Society: From the Knowledge to Policy**. Washington, DC. Johns Hopkins Center for Transatlantic Relations, 2005.

DEMETZOU, K.; ZANFIR-FORTUNA, G.; VALE, S. B. The thin red line: refocusing data protection law on adm, a global perspective with lessons from case-law. **Computer Law & Security Review**, v. 49, 105806, jul. 2023. DOI: http://dx.doi.org/10.1016/j.clsr.2023.105806. Acesso em:15 mar. 2024.

ELMASRI, R.; NAVATHE, S. B. **Sistemas de banco de dados**. São Paulo: Pearson Addison Wesley, 2005.

ELSEVIER, B.V. Holanda. **Scopus**. Disponível em: https://www.scopus.com/. Acesso em: 10 mar. 2024.

FERRÃO, S. É. R.; SILVA, G. R. S.; CANEDO, E. D.; MENDES, F. F. Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100. **Information and Software Technology**, v. 168, 107396, abr. 2024. Elsevier BV. DOI: http://dx.doi.org/10.1016/j.infsof.2024.107396. Acesso em: 30 abr. 2024.

FRANCE. Tribunal Europeu dos Direitos do Homem. **Convenção Europeia dos Direitos Humanos**. Estrasburgo, 2013. Disponível em: <https://www.echr.coe.int/documents/convention_por.pdf>. Acesso em: 23 mar. 2024.

HSU, P. Emerging China data protection law: soft power from EU GDPR? **Tamkang Journal of International Affairs**, v. 25, n. 1, p. 287-310, jul. 2021.

LEE, S. **A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing**. PHD Dissertation. (Phd in International Law) – China University of Political Science and Law, Beijing. 2018, p. 539.

MAPLE, C.; EPIPHANIOU, G.; BOTTARELLI, M. Trustworthy digital infrastructure for identity systems: why should privacy matter to security engineers? **Computer Fraud & Security**, v. 2021, n. 6, p. 6-11, jan. 2021. DOI: http://dx.doi.org/10.1016/s1361-3723(21)00063-4. Acesso em: 15 mar. 2024.

MORESI, E.; PINHO, I. Bibliometric analysis of learning assessment. **CONTECSI USP - International Conference on Information Systems and Technology Management - ISSN 2448-1041**, Brasil, set. 2020. Disponível em: <https://www.tecsi.org/contecsi/index.php/contecsi/17thCONTECSI/paper/view/6510>. Acesso em: 15 mar. 2024.

PEIXOTO, M.; FERREIRA, D.; CAVALCANTI, M.; SILVA, C.; VILELA, J.; ARAðJO, J.; GORSCHEK, T. The perspective of Brazilian software developers on data privacy. **Journal Of Systems and Software**, v. 195, 111523, jan. 2023. DOI: http://dx.doi.org/10.1016/j.jss.2022.111523. Acesso em: 05 abr. 2024.

POHLMANN, S. A. **LGPD Ninja**: entendendo e implementando a lei geral de proteção de dados nas empresas. Nova Friburgo: Fross, 2019. P. 238.

PONCE, P. P. Direct and indirect discrimination applied to algorithmic systems: reflections to brazil. **Computer Law & Security Review**, v. 48, 105766, abr. 2023. DOI: http://dx.doi.org/10.1016/j.clsr.2022.105766. Acesso em: 23 mar. 2024.

RAMARKRISHNAN, R.; GHRKE, J. **Sistema de Gerenciamento de Banco de Dados**. 3.ed. Porto Alegre: Mc Graw Hill, 2011.

REILLY, C. A. Reading risk: preparing students to develop critical digital literacies and advocate for privacy in digital spaces. **Computers and Composition**, v. 61, 102652, set. 2021. DOI: http://dx.doi.org/10.1016/j.compcom.2021.102652. Acesso em: 23 mar. 2024.

RODOTÀ, S. Data protection as a fundamental right. In: GUTWIRTH, S.; POULLET, Y.; DE HERT, P.; TERWANGNE, C. de; NOUWT, S. (ed.). **Reinventing data protection?** Dordrecht: Springer, 2009. cap. 3, p. 77-82. Disponível em: https://doi.org/10.1007/978-1-4020-9498-9_3. Acesso em: 23 mar. 2024.

SAKAMOTO, L. S.; ALVES, D.; ABE, J. M.; SOUZA, J. S. de; SOUZA, N. A. de; MARTINEZ, A. A.G. Software optimization for LGPD compliance using Paraconsistent Evidential Annotated Logic Eτ. **Procedia Computer Science**, v. 192, p. 3049-3059, 2021. DOI: http://dx.doi.org/10.1016/j.procs.2021.09.077. Acesso em: 05 abr. 2024.

UNIÃO EUROPEIA. Parlamento Europeu. **Proteção de Dados Pessoais**. Estrasburgo, 2021. Disponível em: <https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>. Acesso em: 05 abr. 2024.

UNIÃO EUROPEIA. Supervisor Europeu de Proteção de Dados. **A História do Regulamento Geral de Proteção de Dados**. Bruxelas, 2018. Disponível em: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>. Acesso em: 24 mar. 2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation)**. Disponível em: <>https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt. Acesso em: 05 abr. 2024.

VERMEULEN, Gert; LIEVENS, Eva. **Data Protection and Privacy under Pressure**. Antwerp. Maklu Publishing. 2017, p. 341.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.

Glauco Lauria Marques
https://orcid.org/0000-0002-3735-2523
Mestre em Governança, Tecnologia e Inovação pela Universidade Católica de Brasília (UCB). MBA em Administração de Organizações pela Universidade de São Paulo (USP/Ribeirão Preto). Professor na Faculdade de Tecnologia do Centro Universitário de Brasília (UniCEUB).
glaucolauriamarques@hotmail.com

Eduardo Amadeu Dutra Moresi
https://orcid.org/0000-0001-6058-3883
Doutor em Ciência da Informação e Mestre em Engenharia Elétrica pela Universidade de Brasília (UnB). Professor na Universidade Católica de Brasília (UCB).
moresi@p.ucb.br