VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

D597

Direito, governança e novas tecnologias III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires José Rover; Edson Ricardo Saleme; Jéssica Amanda Fachin. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-157-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

TEXTO INICIAL

GT DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III.

Nos dias 24, 25, 26 e 27 de junho de 2025, realizou-se o VIII Encontro Virtual do CONPEDI com a temática “Direito Governança e Políticas de Inclusão”. O evento objetivou promover a socialização das pesquisas jurídicas, desenvolvidas nos programas de pós-graduação e na graduação no Brasil, com ênfase na governança e das diversas políticas tecnológicas adotadas no Brasil. Com aporte em debate qualificado, coordenado pelos professores doutores Edson Ricardo Saleme (Universidade Católica de Santos), Jéssica Fachin (Universidade de Brasilia e Universidade de Londrina e Aires José Rover (Universidade Federal de Santa Catarina) no âmbito do GT Direito, Governança e Novas Tecnologias III. Observou-se no debate a configuração de agenda que buscou investigar as novas formas de governança, bem como estudar as atuais demandas contemporâneas que emergem das novas tecnologias, impactando nos diversos campos do Direito Nessa agenda foram revisitados, sob diversas abordagens, como temas complexos relacionados aos desafios conectados à regulação de novas tecnologias, a participação democrática no âmbito das relações digitais e ainda outras de fundamental importância à temática.

Nesse diapasão, o primeiro trabalho tratou do tema “Desafios regulatórios das tecnologias disruptivas: inteligência artificial, biotecnologia e blockchain no contexto jurídico brasileiro”, abordando as inovações propostas relativas a normatização da temática, ressaltando as tensões em torno dos problemas mais frequentes relacionados ao tema. O próximo tema “A

no caso PIX DO BRASIL: entre a liberdade de expressão e a responsabilidade nas redes sociais", o qual ponderou que, apesar da proposta de modernização e inclusão financeira, o Pix pode ser alvo de desinformações que minam a confiança sobre essa ferramenta.

O próximo artigo "Exposição digital infanto-juvenil e os limites da personalidade como Direito fez análise teórico-jurídica das deepfakes; enfocou a perspectiva da Teoria do Direito e a construção conceitual dos direitos da personalidade, os riscos emergentes impostos pelas tecnologias de inteligência artificial de falsificação e, especialmente as deepfakes, à privacidade e intimidade de crianças e adolescentes em ambiente digital. A seguir passou-se a explanação do artigo intitulado "do entusiasmo à desilusão: uma reflexão sobre a participação democrática na vida virtual", com enfoque na evolução da participação democrática em tempos digitais, analisando tanto o entusiasmo inicial quanto o ceticismo subsequente que emergiram com o avanço da internet". A seguir expôs-se a temática "A vulnerabilidade digital na sociedade informacional: uma análise econômica da democracia e tecnologia no sistema jurídico brasileiro", que ressaltou a necessidade de reavaliar políticas públicas para alcançar justiça social e eficiência democrática.

Na sequência, o artigo "Inclusão social na era da Smart Cities: o papel do Direito e da governança de tecnologias urbanas", fez analise critica na relação entre Direito, governança tecnológica e inclusão social no contexto das cidades inteligentes. O tema a seguir: "Boas práticas de conformidade à LGPD no desenho de bancos de dados relacionais" teve como objetivo apresentar um conjunto de boas práticas para o design de bancos de dados que atendam aos princípios da LGPD, como finalidade, necessidade, segurança e responsabilização. O próximo artigo: "Os impactos das tecnologias de fronteira na proteção integral de crianças e adolescentes: analise sobre o relatório da UNICEF THE STATE OF THE WORD`S CHILDREN no contexto internacional" buscou identificar as principais tendências que moldam o mundo atual e como prever seus efeitos no futuro dos jovens até 2050.

apresentou-se o “Estudo de caso sobre o potencial de satélites refletores de luz solar da start up ‘‘Reflect Orbital’ para o setor agrícola brasileiro”, o qual observa as novas oportunidades para a geração de energia renovável a exemplo de sua aplicação para aumento da produção agrícola, quanto crescimento e produção de culturas, a evolução de tecnologias para este fim se mostra essencial para a humanidade como um todo.

Importante também o “Estudo de caso da Start Up Reflect Orbital como impulsionadora na produção de energia fotovoltaica e seus aspectos jurídicos à luz da Lei 14.200/2022, que busca determinar o potencial energético e sua conformidade com os aspectos legais e diretrizes da Lei 14.300/2022 que regulamenta a geração de energia por consumidores finais. Outra importante reflexão foi o artigo: “Influência das redes sociais na formação da opinião pública: o papel do Direito na regulação de plataformas digitais” que analisa o papel do Direito na regulação das plataformas digitais, buscando identificar mecanismos jurídicos que garantam a proteção dos direitos fundamentais sem comprometer a liberdade de expressão. O estudo denominado “Neurodireitos na sociedade da transparência: o alerta da série adolescência da Netflix”, que parte da ideia do autor Byung-Chul Han sobre a sociedade da transparência para apontar os riscos da hiperexposição nas redes sociais, diante do uso desses dados pelas neurotecnologias no intuito de controle e manipulação.

Outra discussão relacionada aos temas expostos foi realizada com o levantamento da opinião dos presentes, que registraram sua opinião acerca dos diversos temas enfocados. O Grupo de Trabalho foi para o ultimo bloco a partir do tema “Sistema de registro eletrônico de imóveis – SREI: avanços e desafios ante a sobreposição de terras – análise de Adrianópolis – PR, Vale do Ribeira” que estuda o Sistema de Registro Eletrônico de Imóveis – SREI e sua relevância no contexto jurídico moderno, envolto em significativos avanços tecnológicos. Sequencialmente expôs-se o trabalho “Lei 14.932/2024 – utilização do Cadastro Ambiental Rural – CAR para fins de apuração da área tributável a compatibilização dos dados eletrônicos disponibilizados à Administração Pública para uma gestão mais eficaz”, cujo argumento indica que a Administração Pública já está utilizando inovações tecnológicas em

fundamental foi uma reflexão acerca da complexa relação entre modernidade, tecnologia e direito, com foco nas peculiaridades da modernidade periférica. Na sequência o trabalho "Edição genética de plantas: benefícios, riscos e regulamentação" destacou técnicas como CRISPR/Cas9 como ferramenta promissora para enfrentar desafios globais, como segurança alimentar e mudanças climáticas. O último artigo "Big techs e plataformas digitais: o Direito à informação e à liberdade de expressão no ecossistema tecnológico e a reconfiguração do estado-nação" questiona se as Big Techs e players tecnológicos a partir do direito à informação e à liberdade de expressão podem exercer alguma interferência no ecossistema digital possibilitando a reconfiguração do Estado-Nação contemporâneo.

Oportunizou-se mais uma sequência de discussões com contribuições benéficas para os assuntos discutidos e participação de grande parte dos presentes até o final dos trabalhos.

BOAS PRÁTICAS DE CONFORMIDADE À LGPD NO DESENHO DE BANCOS DE DADOS RELACIONAIS

BEST PRACTICES FOR LGPD COMPLIANCE IN THE DESIGN OF RELATIONAL DATABASES

Luiz Fernando Pereira Nunes

Resumo

A Lei Geral de Proteção de Dados Pessoais (LGPD) introduziu novos parâmetros jurídicos e éticos para o tratamento de dados pessoais no Brasil, exigindo mudanças estruturais em sistemas de informação, em especial na arquitetura de bancos de dados relacionais. Este artigo tem como objetivo apresentar um conjunto de boas práticas para o design de bancos de dados que atendam aos princípios da LGPD, como finalidade, necessidade, segurança e responsabilização. A metodologia adotada baseia-se em revisão bibliográfica e análise normativa, articulando fundamentos técnicos e jurídicos com foco na modelagem, controle de acesso, anonimização, auditoria e descarte seguro de dados. Além de discutir os desafios técnicos e jurídicos da implementação, o estudo propõe diretrizes integradas entre arquitetura e governança de dados, considerando também as tendências emergentes relacionadas à inteligência artificial, descentralização e soberania informacional. Os resultados reforçam a necessidade de um alinhamento multidisciplinar e contínuo para garantir a conformidade legal, a proteção efetiva dos titulares e a ética no tratamento de informações pessoais.

Palavras-chave: Lgpd, Banco de dados, Proteção de dados, Anonimização, Governança da informação

Abstract/Resumen/Résumé

The Brazilian General Data Protection Law (LGPD) introduced new legal and ethical standards for the processing of personal data, requiring structural changes in information systems, especially in the design of relational databases. This article aims to present a set of best practices for database design aligned with the LGPD’s principles, such as purpose

Keywords/Palabras-claves/Mots-clés: Lgpd, Database, Data protection, Anonymization, Data governance

1. Introdução

A transformação digital tem impulsionado uma intensa coleta, armazenamento e tratamento de dados pessoais em múltiplas esferas da sociedade contemporânea. Em especial, os bancos de dados se tornaram o núcleo organizacional de aplicações e sistemas que operam sobre grandes volumes de dados sensíveis, ampliando a relevância de práticas que garantam a conformidade com legislações de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). A LGPD estabelece princípios e diretrizes para o tratamento de dados pessoais, exigindo adequações técnicas e organizacionais no âmbito da arquitetura da informação e na modelagem de dados.

Nesse cenário, o desenho de bancos de dados relacionais passa a demandar novas abordagens de projeto, que considerem desde a minimização da coleta até a rastreabilidade de ações sobre os dados. A estruturação de entidades, atributos e relacionamentos deve respeitar os fundamentos da LGPD, como finalidade, necessidade e segurança, os quais orientam a atuação dos agentes de tratamento de dados (controladores e operadores) ao longo de todo o ciclo de vida da informação (MALDONADO; BLUM, 2020).

A obra de Date (2003) já apontava que o projeto lógico de um banco de dados, quando realizado de forma criteriosa, pode exercer papel decisivo na integridade, consistência e eficiência da manipulação de dados. Ao introduzir o conceito de independência de dados e destacar a importância de mecanismos como o controle de acesso e a normalização, o autor delineia caminhos técnicos que se harmonizam com os princípios contemporâneos de proteção de dados. Esses elementos tornam-se ainda mais relevantes diante das exigências normativas da LGPD.

Além dos aspectos legais, normas internacionais como a ISO/IEC 27002:2022 indicam diretrizes detalhadas de controle de segurança da informação, com ênfase na classificação, proteção e descarte de dados. A norma reforça a necessidade de políticas de segregação de funções, gestão de acesso baseado em papéis e registros de auditoria, os quais devem estar refletidos na infraestrutura lógica dos bancos de dados, inclusive no contexto de ambientes distribuídos e em nuvem (ISO/IEC, 2022).

A LGPD impõe um novo paradigma, em que a privacidade deve ser considerada desde a concepção dos sistemas, abordagem conhecida como "*Privacy by Design*". Assim, a modelagem de dados não pode ser tratada como etapa meramente técnica, mas como momento estratégico de conformidade legal e mitigação de riscos. Kohls, Dutra e Welter (2021) ressaltam

que a implementação eficaz da LGPD depende da articulação entre tecnologia, governança e cultura organizacional, iniciando com a adequada estruturação dos repositórios de dados.

No campo prático, torna-se imperativo adotar técnicas como anonimização e pseudonimização, conforme disposto nos artigos 12 e 13 da LGPD, a fim de proteger os dados em ambientes de desenvolvimento, teste ou análise estatística. Para tanto, o projeto de bancos relacionais deve contemplar tabelas auxiliares, chaves substitutas e estruturas que permitam a reversibilidade controlada, quando aplicável, respeitando os princípios da proporcionalidade e da finalidade (REDECKER et al., 2021).

Wang (2025) aponta que a governança da segurança de dados precisa abranger todo o ciclo de vida da informação, desde sua coleta até a eliminação segura, incorporando mecanismos técnicos e normativos. A integração entre modelos de segurança da informação e os esquemas de dados relacionais requer o alinhamento entre desenvolvedores, arquitetos de dados e responsáveis jurídicos, o que reforça a necessidade de conhecimento interdisciplinar no processo de design de bancos de dados.

Sob a ótica da LGPD, o conceito de minimização de dados torna-se central. Ele implica que apenas os dados estritamente necessários para o cumprimento de uma finalidade legítima devem ser coletados e armazenados. Na prática, isso demanda não apenas critérios objetivos na definição de atributos das entidades, mas também mecanismos para limitar o tempo de retenção e o escopo de acesso — conceitos amplamente discutidos na literatura técnica e jurídica contemporânea (VIGLIAR, 2022).

Ao considerar os impactos da LGPD na estrutura de banco de dados, também se evidenciam os desafios de gerenciamento do consentimento do titular. O banco deve estar apto a armazenar metadados associados ao consentimento, bem como possibilitar sua revogação e a eliminação de dados de forma segura e auditável. Isso envolve o uso de estruturas relacionais adicionais e o desenho de *triggers* e procedimentos armazenados que automatizem parte do processo.

Dessa forma, este artigo busca apresentar um conjunto de boas práticas para o projeto de bancos de dados relacionais orientados à conformidade com a LGPD. Para isso, parte-se de uma fundamentação técnico-jurídica sobre proteção de dados, dialogando com normas técnicas e autores especializados em banco de dados, segurança da informação e direito digital. Ao final, espera-se oferecer contribuições tanto para a engenharia de dados quanto para a governança corporativa de privacidade.

2. Fundamentação Teórica

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), sancionada no Brasil em 2018, representa um marco na regulação do tratamento de dados pessoais. Inspirada na *General Data Protection Regulation* (GDPR) da União Europeia, a LGPD estabelece diretrizes para o uso responsável de informações pessoais, exigindo das organizações medidas técnicas e administrativas para garantir a segurança e a privacidade dos dados coletados, tratados e armazenados (MALDONADO; BLUM, 2020).

Conforme dispõe o artigo 6º da LGPD, os princípios fundamentais do tratamento de dados pessoais incluem, entre outros, a finalidade, a necessidade, a transparência e a segurança. Esses princípios devem ser observados desde o momento da coleta até o descarte das informações, o que implica repensar as práticas de modelagem e gerenciamento de bancos de dados para se adequarem às novas exigências legais (ALMEIDA et al., 2020).

Em ambientes corporativos, os dados são majoritariamente armazenados em Sistemas Gerenciadores de Bancos de Dados (SGBDs), que atuam como estruturas centrais de repositórios digitais. Diante disso, a conformidade com a LGPD passa a depender não apenas da governança da informação, mas também das decisões técnicas adotadas no desenho e na implementação das bases de dados (SILVEIRA, 2022).

A literatura especializada tem sugerido a adoção de boas práticas de segurança da informação em bancos de dados, alinhadas às normas internacionais, como a ISO/IEC 27002:2022, que estabelece diretrizes sobre controles organizacionais, técnicos e físicos para proteção de dados. Entre esses controles, destacam-se a gestão de acessos, o monitoramento de logs e a classificação da informação (ISO/IEC, 2022).

Wang (2025) salienta que a segurança dos dados deve ser tratada como um processo contínuo, envolvendo políticas de proteção que perpassam todas as etapas do ciclo de vida da informação, da coleta à eliminação. Nesse contexto, a arquitetura de banco de dados torna-se elemento estratégico para garantir que tais medidas sejam implementadas de forma eficaz e sustentável.

No campo da engenharia de software, o conceito de *Privacy by Design* surge como uma diretriz central. Proposto originalmente por Cavoukian, este conceito preconiza que a proteção da privacidade deve ser incorporada desde as fases iniciais do desenvolvimento de sistemas. No âmbito da modelagem de dados, isso implica projetar estruturas que permitam o

controle granular do acesso, o mascaramento de dados sensíveis e a anonimização de atributos pessoais (FREITAS JÚNIOR; SOUZA, 2023).

Ustaran (2023) destaca que a adequação à legislação de proteção de dados requer o conhecimento e a aplicação de conceitos fundamentais como dado pessoal, dado sensível, controlador, operador e titular, os quais devem ser compreendidos no contexto técnico dos sistemas de informação. Essa compreensão é essencial para que a modelagem do banco de dados esteja alinhada com as bases legais de tratamento previstas na LGPD.

Em termos práticos, a modelagem relacional de dados deve ser capaz de representar o consentimento do titular, as finalidades do uso da informação e os mecanismos de revogação e anonimização. Isso implica, por exemplo, a inclusão de tabelas auxiliares para registrar os termos de consentimento, com metadados sobre o escopo, a duração e a finalidade da autorização concedida (ALVES, 2024).

De acordo com Almeida et al. (2020), uma das formas de operacionalizar os princípios da LGPD em bancos de dados é a adoção de mecanismos como views, roles e grants, que permitem restringir e controlar o acesso aos dados conforme o perfil do usuário. Essa estratégia é particularmente útil em ambientes com múltiplos níveis de permissão, como ocorre em sistemas corporativos e governamentais.

O trabalho de Silveira (2022) propõe a construção de um framework orientado à segurança em banco de dados, com base em cinco pilares: criptografia, auditoria, mascaramento, anonimização e segregação de funções. Tais estratégias, quando implementadas em conjunto, reduzem significativamente os riscos de vazamento de dados e contribuem para a conformidade regulatória.

A obra de Wang (2025) também enfatiza a necessidade de uma abordagem holística da segurança da informação, integrando políticas organizacionais, treinamentos periódicos e tecnologias de proteção em camadas. Essa abordagem deve ser refletida na arquitetura de dados, por meio de esquemas que permitam o controle centralizado e o monitoramento contínuo dos acessos e modificações.

A anonimização dos dados, prevista nos artigos 12 e 13 da LGPD, é apresentada como uma técnica eficaz para eliminar o vínculo entre os dados e seus titulares. No entanto, sua implementação exige cuidados técnicos rigorosos, como a remoção de identificadores diretos e

a verificação da impossibilidade de reidentificação por meios razoáveis (MENEZES VIGLIAR, 2022).

O mascaramento de dados, por sua vez, é uma técnica que visa ocultar a visualização de informações sensíveis em tempo de execução, mantendo a estrutura do dado, mas alterando seu conteúdo. Essa prática é particularmente útil em ambientes de desenvolvimento, onde é necessário preservar o formato da informação sem expor dados reais (ALVES, 2024).

Outro ponto crucial é o conceito de minimização de dados, que estabelece que apenas os dados estritamente necessários à finalidade declarada devem ser coletados. Na modelagem de banco de dados, isso implica em evitar a criação de campos supérfluos ou a duplicação de dados pessoais em diferentes tabelas, mitigando riscos de exposição desnecessária (MALDONADO; BLUM, 2020).

A rastreabilidade e a responsabilização dos agentes de tratamento também devem estar previstas na estrutura do banco de dados, por meio de logs que registram acessos, alterações e operações críticas. Esses registros devem ser protegidos contra adulterações e acessos não autorizados, além de estar disponíveis para auditorias internas ou externas (WANG, 2025).

O conceito de pseudonimização, ainda que diferente da anonimização, também é relevante na estruturação de bancos de dados conforme a LGPD. Ele permite a substituição de dados identificáveis por pseudônimos, desde que exista um controle seguro que viabilize sua reversão em situações legalmente justificadas (REDECKER et al., 2021).

A obra de Kalin (2024) destaca que o fluxo transfronteiriço de dados exige das empresas o cumprimento de requisitos adicionais de proteção, especialmente em bancos de dados integrados a sistemas internacionais. A ausência de adequação pode acarretar barreiras comerciais e conflitos regulatórios, o que reforça a importância da conformidade estrutural desde a concepção do banco.

A literatura também evidencia que o papel do administrador de banco de dados (DBA) tem se expandido, passando de um perfil técnico-operacional para uma função estratégica na governança da informação. O DBA torna-se corresponsável pela implementação de mecanismos de proteção exigidos por lei, devendo atuar em colaboração com áreas jurídicas e de compliance (ALVES, 2024).

Nesse sentido, o desenvolvimento de estereótipos específicos para modelagem de dados pessoais pode ser uma alternativa interessante. Freitas Júnior e Souza (2023) propõem o

uso de estereótipos visuais nos diagramas de entidade-relacionamento para identificar dados pessoais e sensíveis, promovendo a visualização dos riscos e a adequação já na fase de análise.

Por fim, a articulação entre os requisitos legais da LGPD, as normas internacionais de segurança da informação e as práticas de modelagem de dados torna-se essencial para garantir a integridade, a segurança e a conformidade dos sistemas de banco de dados relacionais. Essa integração deve ser vista como um processo contínuo de maturação técnica, organizacional e jurídica.

3. Boas Práticas para o Design de Banco de Dados sob a Ótica da LGPD

A conformidade à Lei Geral de Proteção de Dados Pessoais (LGPD) exige a adoção de práticas estruturais desde as fases iniciais da modelagem de sistemas de informação, em especial no projeto de bancos de dados. Neste contexto, esta seção propõe um conjunto de boas práticas para o desenho de bancos de dados relacionais alinhados aos princípios da LGPD, respaldado por literatura técnica, regulatória e normativa.

3.1 Minimização de Dados e Normalização

A minimização de dados é um princípio basilar da LGPD (art. 6º, III), que determina que o tratamento deve se limitar ao mínimo necessário para a realização de sua finalidade. Em bancos de dados, isso implica projetar esquemas com estruturas enxutas, evitando redundâncias e atributos desnecessários. Técnicas como a normalização são aliadas nesse processo, garantindo consistência e eficiência sem comprometer a privacidade (DATE, 2003; ALMEIDA et al., 2020).

3.2 Representação do Consentimento e da Finalidade

O modelo lógico do banco de dados deve incluir estruturas para armazenar os registros de consentimento dos titulares, contendo metadados como finalidade, duração e canal de obtenção. Isso permite auditar a conformidade do uso dos dados e respeitar os princípios de finalidade e transparência (MENEZES VIGLIAR, 2022; LGPD, art. 8º).

3.3 Controle de Acesso e Segregação de Funções

A atribuição de perfis e privilégios diferenciados por meio de roles e views é uma prática fundamental para garantir o princípio do menor privilégio. Sistemas como PostgreSQL e Oracle oferecem mecanismos robustos para implementar esse controle, restringindo o acesso aos dados conforme a função do usuário (SILVEIRA, 2022; ISO/IEC 27002:2022).

3.4 Anonimização, Pseudonimização e Mascaramento

Técnicas como anonimização e pseudonimização devem ser implementadas quando o tratamento puder ser realizado sem identificar diretamente o titular. A anonimização exige irreversibilidade, enquanto a pseudonimização permite a reidentificação sob condições controladas (FREITAS JÚNIOR; SOUZA, 2023; ALVES, 2024). Já o mascaramento é útil para ambientes de teste, mantendo a estrutura do dado sem revelar seu valor real.

3.5 Auditoria, Logs e Rastreabilidade

Para garantir a responsabilização dos agentes de tratamento, é recomendável o uso de logs e auditoria de acessos e operações. A rastreabilidade das ações no banco de dados deve ser garantida com registros que permitam reconstruir o histórico de interações com dados pessoais (WANG, 2025; ISO/IEC 27002:2022).

3.6 Retenção e Eliminação Programada

A LGPD exige que os dados sejam eliminados após o término do tratamento ou mediante solicitação do titular (art. 15). Isso exige a criação de políticas de expurgo automático com base em metadados como datas de coleta ou de validade da finalidade (REDECKER et al., 2021).

Prática Recomendada	Autor/Referência	Fundamento LGPD / Norma	Observações Técnicas
Minimização de dados e normalização	Date (2003); Almeida et al. (2020)	Art. 6º, III	Elimina redundância, melhora integridade e reduz risco de exposição.
Registro de consentimento e finalidade	Menezes Viglar (2022); LGPD	Art. 7º e 8º	Inserir tabelas auxiliares com data, canal e escopo do consentimento.
Controle de acesso por perfis (roles/views)	Silveira (2022); ISO/IEC 27002 (2022)	Art. 46	Uso de RBAC (Role-Based Access Control) e segregação de funções.
Anonimização e pseudonimização	Freitas Júnior e Souza (2023); Alves (2024)	Art. 12 e 13	Técnicas aplicadas no nível lógico com tabelas derivadas.
Mascaramento de dados	Kohls et al. (2021); Silveira (2022)	Art. 6º, VII	Uso em ambientes de desenvolvimento ou terceiros.
Auditoria e rastreabilidade	Wang (2025); ISO/IEC 27002 (2022)	Art. 46	Trigger de auditoria e log de acesso/controladores.
Políticas de retenção e expurgo	Redecker et al. (2021); Maldonado e Blum (2020)	Art. 15	Procedimentos automatizados por trigger ou jobs SQL.

Tabela 1 - Tabela de Síntese: Boas Práticas, Autores e Fundamento Legal

A tabela 1 sintetiza as principais boas práticas recomendadas para a modelagem de bancos de dados relacionais conforme os princípios da LGPD. Cada prática está relacionada a autores e documentos técnicos ou normativos que fundamentam sua adoção, permitindo que a proposta seja sustentada tanto juridicamente quanto tecnicamente.

As práticas foram organizadas para cobrir todo o ciclo de vida dos dados, desde a sua coleta (minimização e consentimento), passando pelo controle (acesso, auditoria) até sua

desidentificação (anonimização) e descarte (retenção). Essa abordagem sistêmica visa garantir que a proteção de dados seja incorporada desde a concepção dos sistemas – conforme preconiza o princípio de "Privacy by Design".

Ao adotar essas práticas, o administrador de banco de dados e os desenvolvedores ampliam sua responsabilidade ética e jurídica, promovendo não apenas a conformidade regulatória, mas também a confiança do titular de dados na governança da informação institucional.

4. Desafios Técnicos e Jurídicos na Implementação da LGPD em Bancos de Dados

A implementação da LGPD no contexto dos bancos de dados relacionais impõe uma série de desafios que transcendem o domínio técnico, alcançando esferas jurídicas, organizacionais e culturais. A principal dificuldade reside na tradução prática dos princípios legais abstratos da LGPD, como os da necessidade, finalidade e segurança, em estruturas técnicas de modelagem e governança de dados. Embora o ordenamento jurídico estabeleça diretrizes claras sobre o tratamento adequado dos dados pessoais, a concretização desses princípios depende de decisões arquiteturais que, por vezes, carecem de normatização específica (MALDONADO; BLUM, 2020).

Do ponto de vista técnico, um dos principais desafios é a distinção entre dados anonimizados e pseudonimizados. A LGPD define a anonimização como o uso de meios técnicos razoáveis para que os dados não possam ser associados, direta ou indiretamente, a um indivíduo. No entanto, em ambientes relacionais complexos, a recombinação de tabelas e atributos pode inadvertidamente permitir a reidentificação de titulares. Isso torna a anonimização um processo altamente dependente do contexto, dificultando a aplicação de uma solução única e segura (REDECKER et al., 2021).

Outro obstáculo está na necessidade de revisão de bases de dados legadas, que frequentemente foram desenvolvidas em épocas anteriores à vigência da LGPD. Muitas dessas estruturas armazenam informações de forma redundante ou desorganizada, desrespeitando os princípios da minimização e da finalidade. A reestruturação dessas bases exige investimentos financeiros, esforço técnico e, em alguns casos, a interrupção temporária de serviços críticos, o que impõe resistência organizacional à adequação plena (ALVES, 2024; SILVEIRA, 2022).

O gerenciamento do consentimento é outro ponto nevrálgico. A LGPD exige que o consentimento do titular seja livre, informado e inequívoco, além de revogável a qualquer

tempo. Transpor essas exigências para a estrutura de banco de dados requer modelagens que permitam armazenar informações sobre o contexto do consentimento — como canal de obtenção, escopo, validade e data da revogação — e que ainda sejam suficientemente flexíveis para sustentar a exclusão ou anonimização dos dados mediante solicitação do titular (MENEZES VIGLIAR, 2022; USTARAN, 2023).

A compatibilização entre performance e privacidade também se apresenta como desafio recorrente. A aplicação de técnicas como criptografia, mascaramento e auditoria de acessos pode impactar diretamente o desempenho dos sistemas, especialmente em aplicações com grandes volumes de dados e exigência de alta disponibilidade. A busca por soluções que equilibrem proteção e eficiência requer conhecimento especializado e planejamento arquitetônico de longo prazo (WANG, 2025).

Além disso, os desafios jurídicos se manifestam na ausência de jurisprudência consolidada sobre a interpretação de alguns dispositivos da LGPD. Termos como “meios técnicos razoáveis” ou “legítimo interesse” são passíveis de múltiplas leituras, o que torna incerta a adoção de determinadas práticas de banco de dados. Essa insegurança jurídica pode levar empresas a adotar estratégias mais conservadoras ou, em contrapartida, a postergar adequações por receio de investir em estruturas que venham a ser desconsideradas em análises futuras da Autoridade Nacional de Proteção de Dados (ANPD) (KALIN, 2024; ALMEIDA et al., 2020).

Do ponto de vista organizacional, há também um desalinhamento frequente entre as equipes técnicas e jurídicas. Enquanto os desenvolvedores de banco de dados operam com foco em performance, consistência e integridade, os profissionais do direito e da conformidade trabalham com base em princípios e obrigações legais. A ausência de uma linguagem comum entre essas áreas pode dificultar a implementação de medidas coerentes com a LGPD, exigindo esforços interdisciplinares e formação continuada (KOHLS et al., 2021; HEWAGE et al., 2024).

Por fim, destaca-se a necessidade de atualização constante frente ao avanço tecnológico. Novas ameaças, como reidentificação por inteligência artificial, técnicas de inferência sobre dados mascarados e ataques a repositórios distribuídos, impõem um cenário dinâmico em que as práticas de proteção de dados precisam ser permanentemente revisadas e adaptadas. A aplicação da LGPD, portanto, não se resume à conformidade inicial, mas à manutenção de um estado contínuo de governança e vigilância sobre os sistemas de banco de dados (WANG, 2025; USTARAN, 2023).

5. Integração entre Governança de Dados e Arquitetura de Banco

A governança de dados tem se consolidado como um eixo estratégico essencial para organizações que desejam alinhar seus processos informacionais à conformidade legal, à ética digital e à segurança. No contexto da LGPD, essa governança não pode ser dissociada da infraestrutura técnica que sustenta o ciclo de vida dos dados, sendo o banco de dados um de seus elementos mais sensíveis e críticos. A integração entre políticas de governança e a arquitetura de banco é, portanto, uma condição indispensável para a efetivação dos direitos dos titulares e a responsabilização dos agentes de tratamento (WANG, 2025).

A arquitetura de banco de dados define, na prática, como os dados são armazenados, acessados, compartilhados e descartados. Quando essa arquitetura é projetada sem considerar os princípios da LGPD — como finalidade, necessidade, transparência e segurança —, mesmo a mais robusta política de governança torna-se inócua. Por isso, deve-se compreender que a governança de dados não se limita à gestão documental ou à conformidade normativa; ela precisa se refletir nas decisões técnicas do desenho lógico e físico das bases de dados (SILVEIRA, 2022; ISO/IEC 27002:2022).

Nesse cenário, o papel do administrador de banco de dados (DBA) se expande de um perfil meramente técnico-operacional para um ator-chave da governança da informação. O DBA, ao lado dos responsáveis jurídicos e do encarregado pelo tratamento de dados (DPO), participa da estruturação de políticas de acesso, anonimização, retenção e exclusão, sendo corresponsável por sua implementação e monitoramento. Tal postura requer capacitação interdisciplinar e comunicação contínua com os demais setores envolvidos (ALVES, 2024; FREITAS JÚNIOR; SOUZA, 2023).

Um dos instrumentos mais eficazes para promover essa integração é a adoção dos princípios de Privacy by Design e Privacy by Default, previstos no artigo 46 da LGPD. Esses princípios recomendam que a proteção à privacidade seja incorporada desde a concepção dos sistemas, inclusive no banco de dados. Isso se traduz em práticas como criptografar colunas com dados sensíveis, limitar a visibilidade de atributos pessoais via views personalizadas e criar rotinas automáticas de eliminação de dados expirados (USTARAN, 2023; REDECKER et al., 2021).

A integração entre governança e arquitetura também pode ser facilitada pelo uso de catálogos de dados e classificações automatizadas. Esses instrumentos permitem rotular os dados conforme seu grau de sensibilidade, associando metadados sobre a base legal, escopo de

uso e prazo de retenção. A implementação desses mecanismos em nível estrutural facilita auditorias, reduz riscos de acessos indevidos e aumenta a eficiência de processos internos, além de reforçar o compliance com a LGPD (WANG, 2025; ISO/IEC 29134:2020).

Outro aspecto relevante é a incorporação da governança de dados nos processos de desenvolvimento ágil e DevOps. Em arquiteturas modernas, como microsserviços e aplicações serverless, os bancos de dados frequentemente são distribuídos e autônomos. Nesses contextos, o controle centralizado de privacidade é inviável, sendo necessária a descentralização das políticas de governança e a aplicação local de práticas de segurança e controle, orientadas por um modelo federado de gestão da privacidade (KOHLS et al., 2021; HEWAGE et al., 2024).

A comunicação entre as equipes envolvidas na governança e na infraestrutura também precisa ser fortalecida por meio de fluxos de trabalho bem definidos, com responsabilidades claras sobre o ciclo de vida dos dados. A atuação conjunta entre o DPO, o jurídico, os arquitetos de dados e os desenvolvedores deve ser orientada por planos de ação que estabeleçam protocolos para situações como solicitação de acesso, revogação de consentimento, incidentes de segurança e análise de impacto (MENEZES VIGLIAR, 2022; SILVEIRA, 2022).

Por fim, a integração entre governança de dados e arquitetura de banco exige um esforço institucional contínuo de cultura organizacional voltada à ética digital. Não se trata apenas de adequar sistemas, mas de promover uma nova mentalidade sobre o uso responsável das informações, onde a conformidade à LGPD não seja um ônus, mas um ativo reputacional e estratégico da organização (MALDONADO; BLUM, 2020; USTARAN, 2023).

6. Conformidade, Auditoria e Monitoramento Contínuo

A conformidade com a Lei Geral de Proteção de Dados (LGPD) não pode ser concebida como um evento pontual, mas sim como um processo contínuo de avaliação e aperfeiçoamento. Essa continuidade é especialmente relevante no contexto dos bancos de dados, uma vez que estes são estruturas dinâmicas, constantemente modificadas por inserções, atualizações e exclusões de dados. Assim, manter a conformidade exige mecanismos de auditoria e monitoramento que sejam automatizados, auditáveis e integrados às operações da organização (WANG, 2025; SILVEIRA, 2022).

A auditoria de acessos e transações em bancos de dados permite verificar a observância das permissões atribuídas, identificar abusos e rastrear atividades suspeitas. Técnicas como o versionamento de registros (audit trails), logs de transações criptografados e alertas

automatizados em tempo real são exemplos de recursos recomendados para garantir a responsabilização e a transparência no tratamento dos dados. Esses mecanismos atendem ao artigo 46 da LGPD, que impõe a adoção de medidas técnicas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda ou alteração (ISO/IEC 27002:2022).

O monitoramento contínuo também inclui a validação periódica da aderência das estruturas do banco de dados aos princípios legais e políticas internas. Isso pode ser viabilizado por meio de ferramentas de varredura automática de esquemas, que sinalizem a presença de atributos sensíveis não protegidos ou a ausência de metadados de controle, como data de expiração ou registro de consentimento. Essas ferramentas contribuem para o trabalho do encarregado pelo tratamento de dados (DPO), fornecendo subsídios objetivos para os relatórios de impacto exigidos pela LGPD (USTARAN, 2023; ISO/IEC 29134:2020).

Para além da tecnologia, a conformidade depende da maturidade dos processos organizacionais. A existência de planos de governança que integrem ciclos regulares de auditoria, treinamentos contínuos para desenvolvedores e DBAs, e revisões frequentes das políticas de segurança da informação são essenciais para manter a conformidade de forma perene. A ausência desses processos favorece o surgimento de vulnerabilidades, especialmente em contextos de mudança frequente, como atualizações de sistemas, migração de bases ou integração com novos serviços (REDECKER et al., 2021).

Por fim, a cultura de conformidade precisa ser institucionalizada e documentada. Isso implica a definição de métricas de desempenho e indicadores de risco relacionados à proteção de dados, bem como a formalização de processos de resposta a incidentes. Quando incorporada à arquitetura de banco de dados, essa cultura proporciona não apenas maior segurança jurídica à organização, mas também fortalece a confiança dos titulares e parceiros institucionais no tratamento ético e transparente de suas informações (MALDONADO; BLUM, 2020; HEWAGE et al., 2024).

7. Considerações Éticas e Futuras Tendências

A proteção de dados pessoais transcende os limites da técnica e da legislação, alcançando dimensões éticas que exigem reflexão profunda sobre o uso da informação em sociedades cada vez mais orientadas por dados. O design de bancos de dados, nesse contexto, não pode ser concebido apenas como uma atividade técnica neutra, mas como um ato com implicações diretas sobre os direitos fundamentais à privacidade, à autodeterminação

informativa e à dignidade humana. A LGPD, ao reconhecer esses direitos como elementos estruturantes do tratamento de dados, reforça a necessidade de uma abordagem ética em todas as etapas da modelagem e administração de dados (USTARAN, 2023; MALDONADO; BLUM, 2020).

As decisões arquitetônicas e operacionais tomadas no projeto de um banco de dados devem considerar os riscos de reidentificação, de discriminação algorítmica e de exclusão informacional. Em especial, em sistemas que alimentam modelos de inteligência artificial ou de perfilamento automatizado, a arquitetura de dados deve ser projetada para mitigar vieses, controlar inferências e permitir revisões humanas. Essa perspectiva encontra respaldo em iniciativas como a proposta de Responsible AI, que enfatiza a transparência, a auditabilidade e a explicabilidade dos dados utilizados por sistemas automatizados (HEWAGE et al., 2024).

Com o avanço de tecnologias como aprendizado de máquina, Internet das Coisas (IoT), blockchain e computação em nuvem, surgem novos desafios para a proteção de dados em bancos distribuídos, ambientes híbridos e estruturas descentralizadas. A rastreabilidade, o controle granular de acesso e a implementação de políticas de privacidade em redes heterogêneas tornam-se mais complexas, exigindo o desenvolvimento de soluções escaláveis e interoperáveis. Tendências como Data Mesh, Data Fabric e Data Privacy Engineering ganham espaço como alternativas viáveis para lidar com essa crescente complexidade (WANG, 2025).

No âmbito normativo, há uma tendência de convergência internacional entre legislações de proteção de dados, como observado nas reformas da GDPR europeia, na Lei de Privacidade da China e nas legislações estaduais norte-americanas. Esse movimento exige que as arquiteturas de banco de dados estejam preparadas para atender a múltiplos regimes regulatórios, incluindo regras sobre fluxos transfronteiriços de dados, portabilidade e interoperabilidade, conforme discutido por Kalin (2024) ao abordar a interseção entre comércio digital e proteção de dados.

Outro aspecto ético emergente diz respeito ao conceito de soberania informacional. Em um contexto de vigilância digital e monetização de dados em larga escala, os cidadãos exigem maior controle sobre as informações que lhes dizem respeito. As organizações, portanto, devem pensar seus bancos de dados não apenas como ativos internos, mas como ambientes compartilhados com os próprios titulares, sujeitos a revisões, correções, objeções e auditorias. Essa mudança de paradigma implica reposicionar o titular no centro da governança da

informação, não como objeto, mas como sujeito ativo do tratamento (MENEZES VIGLIAR, 2022; FREITAS JÚNIOR; SOUZA, 2023).

Por fim, a evolução do papel da arquitetura de dados e de seus profissionais caminha no sentido de uma prática mais ética, multidisciplinar e socialmente responsável. O domínio técnico deve ser complementado por uma visão crítica sobre os impactos sociais da tecnologia, especialmente em contextos como saúde, educação, trabalho e segurança pública. A adoção de princípios éticos no design e operação de bancos de dados, conforme preconizado pela LGPD e pelas normas internacionais, não representa apenas uma exigência regulatória, mas uma contribuição efetiva para uma sociedade digital mais justa e equitativa (ALVES, 2024; HEWAGE et al., 2024).

8. Conclusão

A conformidade com a Lei Geral de Proteção de Dados (LGPD) no design de bancos de dados relacionais representa um desafio complexo e multifacetado, que demanda a articulação entre saberes jurídicos, técnicos e éticos. O presente artigo demonstrou que a proteção de dados pessoais não se restringe à implementação de ferramentas ou soluções pontuais, mas exige uma abordagem integrada, capaz de incorporar os princípios legais diretamente na estrutura dos sistemas de informação.

Ao longo do trabalho, evidenciou-se que o banco de dados ocupa posição central na governança da informação, funcionando como o alicerce sobre o qual operam os demais mecanismos de tratamento de dados. Nesse sentido, o cuidado com a modelagem, o controle de acesso, a minimização da coleta e o planejamento para retenção e descarte dos dados são práticas indispensáveis para assegurar o respeito aos direitos dos titulares e a integridade dos sistemas institucionais.

A fundamentação teórica permitiu mapear os principais conceitos envolvidos na temática, como os princípios da LGPD, os papéis dos agentes de tratamento, os mecanismos de anonimização e pseudonimização, e os critérios normativos definidos por padrões como a ISO/IEC 27002 e 29134. Esse referencial sustentou a construção das boas práticas propostas, que foram sistematizadas em uma tabela de síntese para facilitar sua adoção por profissionais da área.

Dentre as práticas recomendadas, destacaram-se a minimização de dados desde a concepção do banco, o registro estruturado de consentimento, o uso de controle de acesso

baseado em perfis, a aplicação de técnicas de anonimização e mascaramento, e a implementação de mecanismos de auditoria e rastreabilidade. Cada uma dessas práticas responde a exigências legais específicas, mas também contribui para a construção de sistemas mais seguros, eficientes e confiáveis.

Foram também discutidos os principais desafios enfrentados na implementação da LGPD em ambientes de banco de dados, tanto do ponto de vista técnico quanto jurídico. A distinção entre anonimização e pseudonimização, os impactos em sistemas legados, a ausência de jurisprudência consolidada e a dificuldade de comunicação entre áreas técnicas e jurídicas revelam a complexidade dessa adequação. Tais desafios impõem a necessidade de formação continuada e de práticas colaborativas.

A integração entre arquitetura de banco de dados e governança da informação surgiu como fator crítico para o sucesso da conformidade. Essa integração pressupõe o envolvimento ativo de administradores de banco, analistas de segurança, juristas e gestores, numa atuação coordenada que transcende a especialização de cada setor. A LGPD, ao exigir transparência e responsabilização, convoca as instituições a desenvolverem soluções estruturais, e não meramente paliativas.

O monitoramento contínuo da conformidade, com auditorias regulares, uso de indicadores e aplicação de relatórios de impacto, foi apresentado como estratégia essencial para garantir a resiliência das organizações frente a mudanças tecnológicas e regulatórias. A conformidade, nesse contexto, deve ser vista como um processo cíclico e adaptativo, que responde à dinamicidade dos sistemas e ao amadurecimento institucional.

Além dos aspectos técnicos e legais, o artigo abordou as dimensões éticas e prospectivas da proteção de dados, ressaltando a importância de se repensar a modelagem de dados como prática socialmente orientada. Tecnologias emergentes, como inteligência artificial e data mesh, exigem que a arquitetura de dados seja guiada por princípios de transparência, explicabilidade e justiça, evitando reproduções de desigualdades ou abusos informacionais.

Diante disso, conclui-se que o alinhamento entre bancos de dados relacionais e a LGPD exige uma transformação cultural nas instituições, na qual a privacidade seja valorizada não apenas como uma exigência legal, mas como um compromisso ético com os indivíduos e a coletividade. O banco de dados deixa de ser apenas um instrumento técnico para se tornar um espaço sensível de mediação entre poder informacional e direitos fundamentais.

Por fim, espera-se que este estudo contribua para o fortalecimento de uma cultura de proteção de dados mais sólida, crítica e propositiva, incentivando desenvolvedores, pesquisadores e gestores a adotarem práticas estruturadas e alinhadas à legislação vigente. O caminho para a conformidade plena é árduo e contínuo, mas imprescindível para a consolidação de uma sociedade digital justa, transparente e centrada no ser humano.

9.Referências

ALMEIDA, Reinaldo dos Santos et al. LGPD: Lei Geral de Proteção de Dados Pessoais – Comentada artigo por artigo. São Paulo: Thomson Reuters Brasil, 2020.

ALVES, Gabriel de Araújo. Garantindo a conformidade com a LGPD: estratégias de mascaramento e anonimização de dados para ambientes de banco de dados. Goiânia: Pontifícia Universidade Católica de Goiás, 2024. Trabalho de Conclusão de Curso.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2022 – Segurança da informação, cibersegurança e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 29134:2020 – Segurança da informação – Diretrizes para avaliação de impacto de proteção de dados. Rio de Janeiro: ABNT, 2020.

DATE, C. J. Introdução a sistemas de banco de dados. 8. ed. Rio de Janeiro: Campus, 2003.

FREITAS JÚNIOR, Ailton; SOUZA, Leonardo Lima. Estudo sobre a aplicação de técnicas de anonimização de dados e a Lei Geral de Proteção de Dados (LGPD). Revista Brasileira de Computação Aplicada, v. 15, n. 1, 2023.

HEWAGE, Chaminda et al. Data Protection: The Wake of AI and Machine Learning. Cham: Springer Nature Switzerland, 2024.

KALIN, Roman Pascal. Digital Trade and Data Privacy: Cross-border Flows of Personal Data Between Data Protection and Data Protectionism. Cham: Springer Nature Switzerland, 2024.

KOHLS, Cleize; DUTRA, Luiz Henrique; WELTER, Neide. LGPD: Da teoria à implementação nas empresas. São Paulo: Revista dos Tribunais, 2021.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MENEZES VIGLIAR, José Marcelo. LGPD e a proteção de dados pessoais na sociedade em rede: dados de crianças e adolescentes na Internet, tratamento de proteção jurídica e desafios da regulação. São Paulo: Revista dos Tribunais, 2022.

REDECKER, Ana Cláudia et al. Proteção de dados: temas controvertidos. São Paulo: Revista dos Tribunais, 2021.

SILVEIRA, Kamilla Dória da. Segurança em banco de dados para adequação à LGPD. In: Anais do SIBGRAPI 2022 – Simpósio Brasileiro de Geometria Computacional, Aracaju-SE: Universidade Tiradentes, 2022.

USTARAN, Eduardo (Ed.). European Data Protection: Law and Practice. 3. ed. Portsmouth: IAPP, 2023.

WANG, Anyu. Data Security and Privacy Protection: A Comprehensive Guide. Singapore: World Scientific, 2025.