

Proteção de Dados e Conformidade Legal: Uma revisão de Ferramentas, Práticas de Segurança e Direções Futuras

Camilla C. B. Quincozes¹, Ketrin Vargas¹, Silvio E. Quincozes^{1,2},
César Murilo Silva Jr.², Rafael D. Araújo², Vagner E. Quincozes³

¹LEA, Universidade Federal do Pampa (UNIPAMPA) – Alegrete, Brasil.

²PPGCO, Universidade Federal de Uberlândia (UFU) – Uberlândia, Brasil.

³Instituto de Computação, Universidade Federal Fluminense (UFF) – Niterói, Brasil.

{camilaquincozes, ketrinvargas}@aluno.unipampa.edu.br

{sequincozes, cesarsj, rafael.araujo}@ufu.br

vequincozes@midia.com.uff.br

Abstract. *The digitalization of personal data has increased concerns about privacy and the protection of sensitive information. With more than 80% of global companies facing data breaches, compliance with data protection regulations has become crucial. This paper reviews the literature and available tools to ensure this compliance, analyzing the functionalities of automated tools and highlighting their capabilities and limitations. The results show that, although effective tools exist, significant gaps remain. The study emphasizes the importance of adaptive approaches in the face of rapid technological changes and emerging cyber threats. It is recommended that future research integrates emerging technologies with data protection regulations, developing more robust solutions. Practical guides and detailed strategies are offered to overcome challenges in implementing compliance.*

Resumo. *A digitalização de dados pessoais aumentou as preocupações com a privacidade e a proteção de informações sensíveis. Com mais de 80% das empresas globais enfrentando violações de dados, a conformidade com regulamentações de proteção de dados tornou-se crucial. Este trabalho revisa a literatura e as ferramentas disponíveis para garantir essa conformidade, analisando as funcionalidades de ferramentas automatizadas e destacando suas capacidades e limitações. Os resultados mostram que, embora existam ferramentas eficazes, ainda há lacunas significativas. O estudo enfatiza a importância de abordagens adaptativas frente às rápidas mudanças tecnológicas e ameaças cibernéticas emergentes. Recomenda-se que futuras pesquisas integrem tecnologias emergentes com regulamentações de proteção de dados, desenvolvendo soluções mais robustas. Guias práticos e estratégias detalhadas são oferecidos para superar desafios na implementação de conformidade.*

1. Introdução

As leis de proteção de dados são fundamentais para o cenário atual onde a digitalização acelerada de informações resultou em uma explosão de dados: a quantidade global de

dados gerados e armazenados atingiu 64.2 *zettabytes* em 2020 e continua a crescer exponencialmente [McGovern 1964]. Com isso, a preocupação com a privacidade e a proteção de informações sensíveis tem aumentado e vários setores precisam se preocupar com a proteção de dados.

Relatórios recentes indicam uma crescente ocorrência de ataques e também custos associados. Apenas na indústria da saúde, os custos de violações de dados aumentaram 53,3% desde 2020, resultando em um custo médio de USD 10,93 milhões por violação [IBM 2023]. Além disso, os ambientes de nuvem se tornaram alvos frequentes para atacantes em 2023. De acordo com o relatório de investigações de violação de dados [Verizon Business 2024] 82% das violações envolveram dados armazenados na nuvem, destacando a necessidade de soluções que forneçam visibilidade e proteção abrangente em ambientes híbridos. Já no relatório de custo de violação de dados de 2023, da IBM [IBM 2023], esse tipo de violação incorreram em custos acima da média de USD 4,75 milhões.

Isso ressalta a necessidade de compreender as ferramentas disponíveis no mercado para garantir a conformidade com a LGPD. A conformidade legal não é apenas uma exigência, mas também uma necessidade essencial para preservar a privacidade dos indivíduos e garantir a integridade das operações. No entanto, a literatura sobre ferramentas de conformidade com a LGPD foca principalmente nos aspectos técnicos e legais, mas apresenta limitações significativas. Primeiramente, carece de orientação prática detalhada, dificultando a implementação de soluções específicas pelas empresas. Além disso, não considera a rápida evolução das tecnologias e ameaças cibernéticas, resultando em soluções potencialmente obsoletas [Messias and Alves 2023, Quincozes et al. 2023].

Este estudo examina a literatura e as ferramentas para garantir a conformidade com as regulamentações de proteção de dados, visando identificar lacunas e sugerir direções futuras. Serão analisadas fraquezas na literatura e soluções de mercado, considerando mudanças tecnológicas e ameaças cibernéticas. Orientações detalhadas e estratégias específicas serão oferecidas para superar desafios na implementação de soluções de conformidade, contextualizando as descobertas no cenário normativo atual e nas demandas crescentes por proteção de dados.

Este trabalho está organizado como segue: Na Seção 2, apresenta-se uma visão geral das leis de proteção de dados. Na Seção 3, discutem-se os trabalhos relacionados. Na Seção 4, aborda-se o impacto das regulamentações sobre inteligência artificial e pequenas empresas, com destaque para guias, checklists, frameworks e ferramentas disponíveis para garantir a conformidade. Na Seção 5, discute-se as práticas de segurança em banco de dados e estratégias de proteção de dados em empresas de desenvolvimento de software. Na Seção 6, são apresentadas as ferramentas de mercado, destacando suas funcionalidades, aplicabilidades e como elas auxiliam na conformidade com a LGPD e outras regulamentações. Na Seção 7, são identificados os desafios e oportunidades futuros, como a adaptação às mudanças rápidas nas regulamentações e o alto custo de implementação em pequenas empresas. Finalmente, na Seção 8, são apresentadas as considerações finais.

2. Leis de Proteção de Dados

A proteção de dados pessoais é uma questão de crescente importância no mundo digital moderno. Diversos países implementaram leis para assegurar que os dados pessoais dos

cidadãos sejam coletados, armazenados e processados de maneira segura e transparente. Neste contexto, discutiremos algumas das principais legislações de proteção de dados, com foco na LGPD, mas mencionando também outras relevantes no cenário global.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que estabelece regras claras para a coleta, armazenamento, processamento e compartilhamento de dados pessoais por organizações e empresas no Brasil. Entrou em vigor em setembro de 2020 e visa garantir a privacidade e a proteção dos dados pessoais dos cidadãos brasileiros, além de promover a transparência no uso dessas informações [Brasil 2018].

Similarmente, o Regulamento Geral sobre a Proteção de Dados (GDPR), em vigor desde 25 de maio de 2018, é uma legislação da União Europeia que protege a privacidade e os dados pessoais dos cidadãos da UE e do Espaço Econômico Europeu (EEE). A GDPR é considerada uma das legislações mais rigorosas do mundo em termos de proteção de dados, impondo obrigações significativas às empresas que coletam ou processam dados pessoais de residentes na UE [European Union 2016].

Nos Estados Unidos, a Lei da Privacidade do Consumidor da Califórnia (CCPA), que entrou em vigor em 1º de janeiro de 2020, concede aos residentes da Califórnia direitos específicos sobre suas informações pessoais. A CCPA impõe obrigações às empresas que coletam, processam ou vendem dados pessoais, permitindo que os consumidores saibam quais informações estão sendo coletadas, para que fins, e com quem são compartilhadas [California State Legislature 2018].

Além dessas leis principais, existem outras legislações de proteção de dados pelo mundo que merecem destaque. Por exemplo, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) do Canadá estabelece que as organizações devem obter consentimento explícito dos indivíduos antes de coletar seus dados pessoais [Canada 2000]. A Lei de Proteção de Dados da Índia (PDPL) exige que as organizações nomeiem um oficial de proteção de dados responsável por garantir a conformidade com a lei [India 2019]. A Lei de Proteção de Dados da África do Sul (POPIA) impõe que as organizações implementem medidas técnicas e organizacionais para proteger os dados pessoais [South Africa 2013].

Essas leis compartilham objetivos comuns de proteger a privacidade dos indivíduos e assegurar que os dados pessoais sejam tratados com responsabilidade e segurança. No entanto, cada legislação tem suas especificidades que refletem as diferentes necessidades e contextos culturais e econômicos dos países que as implementam.

3. Trabalhos Relacionados

Nesta seção, são apresentados trabalhos que analisam ferramentas e metodologias para conformidade com legislações de proteção de dados. São discutidas as contribuições e limitações de cada estudo em relação ao presente trabalho, que visa mapear soluções automatizadas de conformidade com diversas legislações de proteção de dados.

O trabalho de [Ryan et al. 2021] analisa ferramentas de conformidade com a GDPR aplicando fatores de sucesso das chamadas tecnologias reguladoras (do inglês, *Regulatory Technology* – RegTechs), que incluem governança de dados, automação, interoperabilidade e um quadro regulatório proativo. *RegTech* refere-se ao uso de tecnologias para facilitar o cumprimento de requisitos regulatórios de maneira eficiente e automati-

zadas são organizações que desenvolvem tecnologias, especialmente no setor financeiro. A conclusão dos autores é de que apesar das ferramentas disponíveis, muitas organizações ainda enfrentam dificuldades para cumprir as exigências da GDPR devido à falta de apoio integrado dos reguladores para facilitação da conformidade digital automatizada.

O trabalho [Delagustini 2021] analisa e avalia ferramentas de mapeamento de dados para identificar qual delas melhor adere à norma ABNT NBR ISO/IEC 27701 e a LGPD. As principais contribuições incluem a definição de critérios, métricas e casos de testes específicos para a avaliação das ferramentas *Talend Open Studio*, *Pentaho Kettle* e *CloverDX*. Conclui-se que ferramentas de mapeamento de dados usadas para extração, transformação e carregamento não são adequadas para conformidade com essas normas.

Em [Chhetri et al. 2022] há o desenvolvimento de uma ferramenta escalável para verificação automatizada de conformidade com a GDPR, baseada em consentimento informado modelado semanticamente. As principais contribuições incluem a implementação de um processo de *regulation-to-code* que transforma regulamentos em metas de proteção e medidas técnicas organizacionais, além do uso de tecnologia semântica para garantir interoperabilidade de dados e um modelo de consentimento consistente.

O trabalho de [Jackson 2018] fornece uma visão geral das ferramentas disponíveis para avaliar, implementar e manter a conformidade com o GDPR. Ele destaca diversas soluções, como *Snow Software GDPR Risk Assessment*, *IAPP* e *TRUSTe GDPR Readiness Assessment*, entre outras, cada uma oferecendo diferentes abordagens para a conformidade.

A Tabela 1 resume os trabalhos relacionados destacados acima. Tais trabalhos oferecem diversas abordagens para a conformidade com legislações de proteção de dados, focando principalmente no GDPR. Em contraste, o presente trabalho propõe uma revisão que mapeia não apenas ferramentas, mas também trabalhos científicos que abordam soluções automatizadas de conformidade com legislações de proteção de dados de forma mais abrangente. A principal diferença é que este trabalho abrange várias regulamentações, proporcionando uma análise mais inclusiva e completa.

Tabela 1. Comparação das Abordagens de Conformidade

Trabalho	Foco Principal	Ferramentas	Considerações
[Ryan et al. 2021]	GDPR	RegTech	Foco exclusivo na GDPR
[Delagustini 2021]	LGPD, ISO/IEC 27701	Talend, Pentaho, CloverDX	Foco em mapeamento de dados
[Chhetri et al. 2022]	GDPR	Ferramenta escalável	Aplicação limitada.
[Jackson 2018]	GDPR	Diversas ferramentas	Foco exclusivo no GDPR
Presente Trabalho	Várias regulamentações	Diversas ferramentas e artigos	Análise abrangente

4. Análise de Ferramentas Existentes

A conformidade com regulamentações de proteção de dados é um desafio constante para as organizações, especialmente no contexto brasileiro. As empresas precisam adaptar seus processos para atender às novas leis e garantir a segurança dos dados pessoais. Além disso, o impacto dessas regulamentações sobre a inteligência artificial e pequenas empresas deve ser considerado para desenvolver soluções eficazes e práticas. As ferramentas

existentes na literatura e no mercado exploram diferentes abordagens e oferecem diferentes funcionalidades. Nesta seção, serão exploradas as principais vertentes identificadas na literatura.

4.1. Guias, Checklists, Frameworks e Ferramentas

O diagnóstico da conformidade em organizações brasileiras revela diversas lacunas e desafios que precisam ser abordados para garantir a proteção de dados pessoais. O impacto socioeconômico das novas leis de proteção de dados é significativo, influenciando tanto a gestão de empresas quanto a percepção pública sobre privacidade. As contribuições e limites das regulamentações de proteção de dados para a regulação da inteligência artificial destacam a necessidade de regulamentações específicas para IA [Almada and Maranhão 2023]. O uso de *middleware* para garantir conformidade em pequenas empresas oferece uma solução prática e transparente, essencial para empresas com recursos limitados [Ferrão et al. 2021][Zerbielli et al. 2023].

Os guias, checklists e frameworks gerais são recursos valiosos para equipes de desenvolvimento e outras partes interessadas na conformidade com regulamentações de proteção de dados. Eles fornecem diretrizes práticas e estruturadas que ajudam a garantir que todos os aspectos relevantes da proteção de dados sejam considerados durante o desenvolvimento de projetos. Por exemplo, o trabalho [Quincozes et al. 2023] desenvolveu um checklist para avaliar a adequação do aplicativo móvel MedBe [Quincozes et al. 2022] com a LGPD. Este checklist traduz as exigências legais e os termos técnicos do desenvolvimento de sistemas, tornando-os mais acessíveis e aplicáveis na prática diária de desenvolvimento de software.

A adoção de frameworks e ferramentas específicas é essencial para que as empresas possam garantir a conformidade com as regulamentações de proteção de dados. Esses frameworks e ferramentas devem abordar aspectos como governança, segurança, privacidade e transparência, proporcionando uma base sólida para a implementação de práticas de proteção de dados. A revisão sistemática [Canedo et al. 2021] investiga a percepção das equipes ágeis sobre o impacto da LGPD em suas atividades de desenvolvimento de software. Um fato que é possível de ser observado em tais estudos consiste na constatação de que as equipes possuem conhecimento sobre legislação de privacidade, mas enfrentam desafios na implementação prática das técnicas propostas na literatura.

Há iniciativas que concentram-se em cenários específicos. No setor do agrobusiness, por exemplo, o trabalho [Lisboa et al. 2023] propõe um protocolo para auxiliar empresas desse ramo a se adequarem às regulamentações de proteção de dados, baseada no *Balanced Scorecard* (BSC), avalia o desempenho organizacional em processos, lei/norma, tecnologia e aprendizado. Já no contexto de empresas que utilizam *Big Data*, há a proposta de *frameworks* de *compliance* que são baseados em pilares como governança, segurança, privacidade, transparência e responsabilidade [Carvalho 2021].

Ferramentas automatizadas para verificação de conformidade com o GDPR, utilizando grafos de conhecimento, ajudam a identificar lacunas e recomendam ações corretivas [Tauqeer et al. 2022]. Guias e *frameworks* para implementar princípios de proteção de dados no desenvolvimento de software oferecem processos detalhados e *checklists* que garantem a conformidade de soluções de software e IoT [Rocha et al. 2023, Pereira et al. 2022].

4.2. Avaliação e Diagnóstico

A avaliação e o diagnóstico de conformidade são etapas fundamentais para identificar áreas de melhoria e garantir que as práticas de proteção de dados estejam alinhadas com as regulamentações vigentes. Ferramentas e métodos específicos podem facilitar esse processo e ajudar as organizações a se manterem em conformidade.

Na literatura há relatos de trabalhos que seguem tal abordagem. Por exemplo, em [Alves et al. 2022], uma pesquisa com 20 respondentes que avaliaram uma plataforma web de conformidade com regulamentações de proteção de dados mostrou que a plataforma é adequada para avaliar projetos de software à luz da legislação vigente.

Em geral, métodos e plataformas para a avaliação e diagnóstico de conformidade são essenciais para auxiliar organizações no processo de adequação às regulamentações. A conformidade de empresas brasileiras do setor químico foi avaliada utilizando um *framework* baseado em seis dimensões, demonstrando que o modelo pode ser útil para auxiliar as empresas no processo de adequação [Silva 2021].

5. Práticas e Avaliações de Segurança e Proteção de Dados

A segurança dos dados é um aspecto crucial da conformidade com as regulamentações de proteção de dados. As práticas de segurança devem ser integradas nos processos organizacionais para proteger dados sensíveis contra acessos não autorizados e outras ameaças.

5.1. Práticas de Segurança

Práticas de segurança em banco de dados incluem a identificação e categorização de dados pessoais, controle de acesso, criptografia, auditoria e backup. Estas práticas são essenciais para garantir a conformidade com regulamentações de proteção de dados [da Silveira 2022]. Estratégias de proteção de dados em empresas de desenvolvimento, abrangendo aspectos técnicos, culturais e jurídicos, são descritas em [Nardelli 2021]. Um exemplo de uso da tecnologia se dá no emprego de técnicas como o uso de *blockchain*, para o gerenciamento eficiente de consentimento de dados, o que proporciona maior controle aos usuários e garantem a auditabilidade e a conformidade com as leis de proteção de dados [Araújo and de Souza 2022].

Integrar a privacidade desde o início do desenvolvimento de software é crucial para garantir que as soluções finais estejam em conformidade com as regulamentações de proteção de dados. *Frameworks* específicos podem ajudar os desenvolvedores a incorporar práticas de privacidade de maneira eficaz e consistente. *Frameworks* para suportar a engenharia de requisitos com foco na proteção de dados foram propostos em [Da Silva et al. 2022] e [Miranda 2021]. Esses *frameworks* integram preocupações de privacidade diretamente no processo de desenvolvimento de software, destacando áreas potenciais de melhoria e garantindo a conformidade com regulamentações.

A análise de dados e as heurísticas cognitivas desempenham um papel importante na forma como os dados são compartilhados e protegidos. Entender esses aspectos pode ajudar a criar interfaces e sistemas que respeitem a privacidade dos usuários e estejam em conformidade com as regulamentações de proteção de dados. Fatores que influenciam a divulgação de dados de usuários do Facebook foram analisados em

[F. B. de Carvalho et al. 2022]. Heurísticas cognitivas foram identificadas como influentes na decisão dos usuários de revelar informações, destacando a necessidade de interfaces que protejam a privacidade.

6. Ferramentas do Mercado

Empresas importantes de diversos setores e reconhecidas nacionalmente utilizam plataformas de gestão e conformidade com as regulamentações de proteção de dados.

A Didomi [Didomi 2024] é uma plataforma de consentimento e preferências que ajuda empresas a coletar, gerenciar e documentar o consentimento dos usuários de forma eficaz e em conformidade com as regulamentações de privacidade, incluindo a LGPD. A plataforma Didomi oferece diversas funcionalidades essenciais para proteger a privacidade dos usuários e garantir a conformidade legal. Didomi ajuda as empresas a obter consentimento válido e em conformidade com os requisitos específicos da LGPD e outras regulamentações de privacidade, garantindo que as empresas estejam em conformidade com as leis aplicáveis.

A OneTrust oferece uma ampla gama de soluções de conformidade, incluindo ferramentas para gerenciamento de consentimento, mapeamento de dados, avaliação de riscos e resposta a solicitações de privacidade. A ferramenta ajuda as organizações a operacionalizar os requisitos da LGPD, gerenciando todo o ciclo de vida do processamento de dados pessoais, desde a coleta até o encerramento e a exclusão. Em seu site, a empresa fornece um documento intitulado “OneTrust para a Lei Geral de Proteção de Dados (LGPD) do Brasil” [OneTrust 2023], onde explica com mais detalhes seus serviços.

Já a LGPD Azul é uma startup totalmente brasileira e oferece um software como serviço para gestão e governança da conformidade com a LGPD [LGPD Azul nd]. A empresa se descreve como uma “PrivacyTech”, um tipo de mercado que começou a surgir entre 2016 e 2017, e que, como o nome sugere, é focado na prestação de serviços voltados para privacidade e proteção de dados de seus clientes [DeParis 2020]. Ou seja, as empresas OneTrust e a LGPD Now, já mencionadas, também fazem parte desse mercado. Aliás, em seu blog, a LGPD Azul apresenta um artigo em que lista vários fornecedores de softwares para adequação à LGPD, incluindo a OneTrust e a LGPD Now [Azul 2023]. A seguir, serão apresentados mais alguns desses fornecedores e seus softwares.

A ECOMPLY surgiu em 2017, na Alemanha, para auxiliar empresas europeias no processo de conformidade com a GDPR. Em 2020, a empresa se expandiu para o Brasil, tendo a partir de então uma representação de vendas em São Paulo, pronta para oferecer serviços para adequação à LGPD, que acabava de entrar em vigor. Em 2022, seu software estava na versão 4.0, com suporte a dashboards, delegação, gerenciamento de processos, armazenamento de arquivos refinado, entre outras funcionalidades [ECOMPLY 2023].

Em seu site oficial, a Securiti¹ informa ter vários clientes importantes, dentre os quais a Cisco e a Dell Technologies. Seu produto de destaque é o Data Command Center, uma plataforma centralizada que possibilita o uso seguro de dados e inteligência artificial generativa (GenAI). No entanto, eles também oferecem a PrivacyOps, uma plataforma focada na gestão da privacidade. A PrivacyOps permite criar formulários Web personalizados com a marca da empresa a fim de aceitar pedidos verificados de direitos dos

¹<https://securiti.ai/>

titulares de dados. Além disso, também permite automatizar o tratamento de solicitações de acesso ao titular, verificar gráficos de dados de pessoas, atender à conformidade com cookies, monitorar e acompanhar o consentimento, e medir a postura da organização em relação aos requisitos da LGPD, entre outras funções [securiti.ai 2023].

Voltando ao mercado brasileiro, além da LGPD Azul, também há a Riosoft com seu sistema chamado LGPD Advance. Esse sistema reúne um conjunto de soluções para adequação da empresa à LGPD. Facilita a gestão de dados e auxilia nas etapas de mapeamento de dados (*Data Mapping*) e de riscos. O produto também inclui assessoria, dividida em etapas e com especialistas, além de treinamento por meio da plataforma, manuais, tutoriais e modelos pré-formatados de documentos [Riosoft 2023].

Estas foram algumas das ferramentas do mercado encontradas. As empresas citadas oferecem plataformas de gerenciamento de dados e privacidade com muitas funcionalidades em comum mas com seus diferenciais, quais cabe os interessados avaliarem melhor qual dos produtos se encaixa melhor em seus orçamentos e lhe traz mais garantia de segurança. Vale lembrar que outras empresas oferecem softwares apenas para gestão de *cookies* ou para aprendizagem.

7. Tendências, Desafios e Oportunidades

A análise dos estudos revisados revela a diversidade e complexidade das abordagens para a conformidade com regulamentações de proteção de dados. Entre os principais enfoques, destacam-se métodos de aprendizado de máquina para a detecção de fraudes, *frameworks* para *compliance* em *Big Data*, e ferramentas de verificação automatizada de conformidade. Essas soluções oferecem contribuições valiosas para diferentes contextos organizacionais, porém, há áreas que ainda necessitam de maior desenvolvimento e refinamento.

No contexto das pequenas e médias empresas, exemplificadas pelo estudo de caso no agronegócio, o protocolo PDAGRO [Lisboa et al. 2023], baseado no BSC, se mostra uma abordagem promissora para avaliação do desempenho organizacional em múltiplas dimensões. A utilização desse protocolo pode ser estendida para incluir novas métricas e métodos de avaliação, especialmente considerando a evolução das leis de proteção de dados e as necessidades específicas do setor agroindustrial. Futuras pesquisas podem explorar a implementação de tecnologias emergentes, como IoT e blockchain, para melhorar ainda mais a conformidade e a gestão de dados nesse setor.

Além disso, a aplicação de *frameworks* de *compliance* para empresas que utilizam Big Data destaca a importância de abordar a governança, segurança, privacidade, transparência e responsabilidade. Para expandir esses *frameworks*, é essencial considerar a integração com sistemas de inteligência artificial, assegurando que as práticas de proteção de dados acompanhem o rápido avanço tecnológico. Estudos futuros devem investigar como essas tecnologias podem ser harmonizadas com as regulamentações existentes, desenvolvendo guias práticos e estratégias de implementação que sejam aplicáveis a diversos setores da economia.

Outra área crítica é a implementação de ferramentas de verificação automatizada de conformidade, como as que utilizam grafos de conhecimento para identificar lacunas e recomendar ações corretivas. Essas ferramentas podem ser aprimoradas com a inclusão de algoritmos de aprendizado contínuo, que se adaptem automaticamente às mudanças

nas regulamentações e nos ambientes operacionais. Pesquisas emergentes podem focar na criação de sistemas inteligentes que não apenas identifiquem problemas de conformidade, mas também sugiram soluções proativas e customizadas para cada organização.

Para guiar futuras direções de pesquisa, sugere-se explorar os seguintes tópicos emergentes e interessantes:

- **Integração de IoT e Blockchain:** Investigar como a combinação dessas tecnologias pode fortalecer a conformidade com regulamentações de proteção de dados em setores específicos, como agronegócio e saúde.
- **Inteligência Artificial e Compliance:** Desenvolver frameworks que utilizem IA para monitorar, detectar e corrigir automaticamente problemas de conformidade em tempo real.
- **Aprendizado Contínuo em Ferramentas de Conformidade:** Criar sistemas de verificação automatizada que se adaptem às mudanças nas leis e nas práticas de proteção de dados, utilizando aprendizado contínuo e análise preditiva.
- **Impacto das Tecnologias Emergentes em Pequenas Empresas:** Estudar a aplicabilidade e os desafios da implementação de tecnologias avançadas de conformidade em pequenas e médias empresas, identificando soluções viáveis e econômicas.
- **Interfaces de Usuário para Privacidade:** Desenvolver interfaces intuitivas que ajudem os usuários a gerenciar suas preferências de privacidade de maneira eficaz, baseadas em heurísticas cognitivas identificadas em estudos anteriores.

Dessa forma, a combinação de métodos inovadores e tecnologias emergentes promete avanços significativos na proteção de dados, alinhando-se às exigências regulamentares e às necessidades operacionais das organizações.

8. Considerações Finais

Este trabalho realizou uma análise abrangente das ferramentas e metodologias disponíveis para garantir a conformidade com as regulamentações de proteção de dados. A pesquisa considerou as legislações relevantes, mapeando técnicas e ferramentas utilizadas para garantir a proteção de dados pessoais. Foram revisados diversos estudos e ferramentas, identificando suas aplicações práticas e limitações.

As principais descobertas revelam que, embora existam muitas ferramentas eficazes para a conformidade com a proteção de dados, ainda há lacunas significativas. Muitos estudos destacaram a importância de abordagens adaptativas que considerem as rápidas mudanças tecnológicas e as ameaças cibernéticas emergentes. As ferramentas analisadas demonstraram capacidades variadas, desde a detecção de fraudes até a gestão de consentimento e a auditoria de conformidade, mas também mostraram limitações, especialmente na implementação prática em pequenas empresas e na adaptação a tecnologias emergentes como IoT e blockchain.

Como trabalhos futuros, pretende-se desenvolver um estudo de caso a fim de produzir-se dados quantitativos e aprofundar-se na investigação sobre a integração de tecnologias emergentes com regulamentações de proteção de dados, buscando desenvolver soluções mais robustas e adaptáveis. Além disso, pretende-se explorar formas de tornar essas ferramentas mais acessíveis e custo-efetivas para pequenas e médias empresas. Finalmente, planeja-se trabalhar na criação de guias práticos e detalhados para a

implementação dessas ferramentas para ajudar as organizações a superar os desafios de conformidade de maneira mais eficiente e eficaz.

Referências

- Almada, M. and Maranhão, J. (2023). Contribuições e limites da lei geral de proteção de dados para a regulação da inteligência artificial no brasil. *Revista direito público*, 20:385–413.
- Alves, M. B., Costa, L. M. T., and Guimarães, R. F. (2022). LGPD compliance: aplicando checklist para avaliação de sistemas à luz da Lei geral de proteção de dados. B.S. thesis, Instituto Federal de Paraíba.
- Araújo, M. and de Souza, C. (2022). Personal blockchain: Uma estratégia de gerenciamento de consentimento de dados pessoais dirigida ao usuário. In *Anais Estendidos do XII Simpósio Brasileiro de Engenharia de Sistemas Computacionais*, pages 104–109, Porto Alegre, RS, Brasil. SBC.
- Azul, L. (2023). Lista dos fornecedores de software para adequação à lgpd. Disponível em: https://www.lgpdazul.com.br/fornecedores_software_lgpd. Acesso em: Dez. 2023.
- Brasil (2018). Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 Jun. 2024.
- California State Legislature (2018). California Consumer Privacy Act (CCPA), Civil Code Section 1798.100-1798.199. Disponível em: https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 15 jun. 2024.
- Canada (2000). Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5. Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/>. Acesso em: 15 jun. 2024.
- Canedo, E. D., Toffano Seidel Calazans, A., Cerqueira, A. J., Teixeira Costa, P. H., and Seidel Masson, E. T. (2021). Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil. In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pages 58–69.
- Carvalho, A. P. (2021). Proposta de um framework de compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): um estudo de caso para prevenção a fraude no contexto de Big Data. B.S. thesis, Universidade de Brasília.
- Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K., and Fensel, A. (2022). Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. *Sensors*, 22(7).
- Da Silva, P. H., Benitti, F., and Wingham, M. (2022). Framework for the development of computational solutions for the support of requirements engineering with a focus on data protection. In *Proceedings of the XXXVI Brazilian Symposium on Software Engineering*, SBES '22, page 419–424, New York, NY, USA. Association for Computing Machinery.

- da Silveira, K. D. (2022). Segurança em Banco de Dados para Adequação a LGPD. In *Anais do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 278–287, Porto Alegre, RS, Brasil. SBC.
- Delagustinhi, P. A. (2021). *Análise de Ferramentas de Mapeamento de Dados*. PhD thesis, Universidade de Caxias do Sul, Caxias do Sul. Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação.
- Deparis, A. L. (2020). O crescimento das privacytech. Disponível em: <https://www.migalhas.com.br/depeso/320896/o-crescimento-das-privacytech>. Acesso em: 15 ago. 2024.
- Didomi (2024). Didomi: Consent and Preference Management Platform. Disponível em: <https://www.didomi.io/>. Acesso em: 18 Jun. 2024.
- ECOMPLY (2023). Ecomply. about us. Disponível em: <https://www.ecomply.io/brasil/about-us>. Acesso em: 15 ago. 2024.
- European Union (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. European Parliament and Council of the European Union. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 15 jun. 2024.
- F. B. de Carvalho, D. F., N. Nobre, C., and T. Marques-Neto, H. (2022). Evaluating Cognitive Privacy Heuristics that Influence Facebook Users Data Disclosure. *Journal of Internet Services and Applications*, 13(1):66–81.
- Ferrão, S. É. R., Carvalho, A. P., Canedo, E. D., Mota, A. P. B., Costa, P. H. T., and Cerqueira, A. J. (2021). Diagnostic of data processing by Brazilian organizations—a low compliance issue. *Information*, 12(4):168.
- IBM (2023). Cost of a Data Breach Report. Technical report, IBM Corporation. Disponível em: <https://www.ibm.com/security/data-breach>.
- India (2019). Personal Data Protection Law (PDPL), Act No. 20 of 2019. Disponível em: <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>. Acesso em: 15 jun. 2024.
- Jackson, W. (2018). 14 top tools to assess, implement, and maintain GDPR compliance. CSO. Foundry (an IDG, Inc. company). Disponível em: <https://www.csoonline.com/article/563565/14-top-tools-to-assess-implement-and-maintain-gdpr-compliance.html>. Acesso em: Ago. 2024.
- LGPD Azul (n.d.). LGPD Azul. Disponível em: <https://www.lgpdazul.com.br/>. Acesso em: Dez. 2023.
- Lisboa, A. P. A., do AMARAL, E., and LAMPERT, V. d. N. (2023). PDAGRO: Uma ferramenta de diagnóstico de conformidade à LGPD. *Revista do CCEI*, 26(42):82–98.
- McGovern, P. (1964). International Data Corporation. Disponível em: <https://www.idc.com/>. Acesso em: Mai. 2024.
- Messias, d. S. L. M. and Alves, N. G. (2023). LGPD e Compliance: A efetivação dos direitos da personalidade nas relações de emprego. *Scientia Iuris*, 27(2):91–111.

- Miranda, E. E. C. d. (2021). *Um Framework Fundamentado na Engenharia de Requisitos para Apoiar a Conformidade Legal e Regulatória em Sistemas Computacionais*. Tese (doutorado em sistemas e computação), Centro de Ciências Exatas e da Terra, Universidade Federal do Rio Grande do Norte, Natal.
- Nardelli, C. (2021). Segurança da Informação e LGPD Aplicado no Desenvolvimento de Software. In *Anais da V Escola Regional de Engenharia de Software*, pages 169–178, Porto Alegre, RS, Brasil. SBC.
- OneTrust (2023). Soluções OneTrust para a LGPD. Disponível em: <https://www.onetrust.com/br/lgpd/>. Acesso em: Mai. 2024.
- Pereira, I., Mendes, J., Viana, D., Rivero, L., Ferreira, W., and Soares, S. (2022). Extending an LGPD Compliance Inspection Checklist to Assess IoT Solutions: An Initial Proposal. In *Congresso Brasileiro de Software: Teoria e Prática*, pages 28–31.
- Quincozes, V. E., Quincozes, S. E., Kreutz, D., Mansilha, R. B., and Kazienko, J. F. (2022). A Mobile Application for on-Demand Scheduling of Health Services. In *Proceedings of the XVIII Brazilian Symposium on Information Systems, SBSI '22*, New York, NY, USA. Association for Computing Machinery.
- Quincozes, V. E., Quincozes, S. E., Kreutz, D., Mansilha, R. B., and Kazienko, J. F. (2023). Sistema de Informação para Agendamento 4.0: Caracterização, UX e LGPD. *iSys-Brazilian Journal of Information Systems*, 16(1):5–1.
- Riosoft (2023). LGPD Advance. Disponível em: <https://www.lgpdadvance.com.br/>. Acesso em: Mai. 2024.
- Rocha, L. D., Silva, G. R. S., and Dias Canedo, E. (2023). Privacy compliance in software development: A guide to implementing the lgpd principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, pages 1352–1361.
- Ryan, P., Crane, M., and Brennan, R. (2021). GDPR Compliance Tools: Best Practice from RegTech. In Filipe, J., Śmiałek, M., Brodsky, A., and Hammoudi, S., editors, *Enterprise Information Systems*, pages 905–929. Springer International Publishing, Cham.
- securiti.ai (2023). Lei Geral de Proteção de Dados (ou LGPD): Revolucionando a conformidade com a LGPD por meio do PrivacyOps. Disponível em: <https://securiti.ai/pt-br/solutions/brazil-lgpd/>. Acesso em: Mai. 2024.
- Silva, R. H. (2021). Framework para identificar o nível de conformidade das empresas brasileiras do setor químico no processo de adequação à lei geral de proteção de dados pessoais. Disponível em: <https://repositorio.ufsc.br/handle/123456789/222071>. Acesso em: 15 ago. 2024. Acesso em: 15 ago. 2024.
- South Africa (2013). Protection of Personal Information Act (POPIA), Act No. 4 of 2013. Disponível em: <https://www.gov.za/documents/protection-personal-information-act>. Acesso em: 15 jun. 2024.
- Tauqeer, A., Kurteva, A., Chhetri, T. R., Ahmeti, A., and Fensel, A. (2022). Automated GDPR contract compliance verification using knowledge graphs. *Information*, 13(10):447.

Verizon Business (2024). 2024 Data Breach Investigations Report: Summary of Findings. Disponível em: <https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/>. Acesso em: 6 Mai. 2024.

Zerbielli, Y. M., Felicio, V. B., Solutchak, C., Kunzler, W., Peretti, G. S., de SP Ozório, G., Priesnitz Filho, W., and Neto, H. S. (2023). A Middleware Proposal Towards The Compliance of Small Business Databases with the LGPD. In *Anais do XX Congresso Latino-Americano de Software Livre e Tecnologias Abertas*, pages 146–149. SBC.