Um *framework* conceitual para criação e implementação de proteção de dados

Jean Fellipe Barkoczy
Mackenzie Presbyterian University
São Paulo, Brazil
jeean.fellipe.b@gmail.com

Guilherme Heck Lara
Mackenzie Presbyterian University
São Paulo, Brazil
guihecklara@gmail.com

Solange Duarte Palma de Sá Barros
Mackenzie Presbyterian University
São Paulo, Brazil
solange.barros@mackenzie.br

Everton Knihs
Mackenzie Presbyterian University
São Paulo, Brazil
tomspsp@gmail.com

Ismar Frango Silveira
Mackenzie Presbyterian University
São Paulo, Brazil
ismarfrango@gmail.com

***Abstract*—This work was developed with the aim of exposing what is necessary to create data protection, observing a conceptual framework that meets the legal standards of data protection and privacy. In the search for a reference that encompasses the topics researched, it is clear that there is a need for instruction and support to navigate between the legal standards that guide the topic. Therefore, a conceptual framework in the form of an ontology is proposed to indicate the steps necessary to adapt current regulations, serving to instruct the technical and legal measures necessary for data protection.**

***Keywords*—Data protection; framework; ontology**

***Resumo* — Este trabalho foi desenvolvido com o objetivo de expor o que é necessário criar para proteção de dados, observando um framework conceitual que atenda as normas legais de proteção de dados e privacidade. Com a busca de uma referência que englobasse os temas pesquisados, percebe-se a necessidade de instrução e suporte para navegar entre as normas legais que orientam o tema. Sendo assim, propõe-se um framework conceitual em forma de ontologia, para indicar as etapas necessárias para adequar as normas vigentes, servindo para instruir as medidas técnicas e legais necessárias para a proteção de dados.**

***Palavras-chave*—Proteção de dados; framework; ontologia.**

I. Introdução

A proteção de dados pessoais é um direito e segue alguns princípios, sendo eles: finalidade; escolha; livre acesso; segurança e transparência [8], a proteção de dados é aplicada tanto ao setor público quanto privado. Diante das inovações tecnológicas e do aumento de consumo de dados, novas utilizações e fins para os dados pessoais foram criados, sendo necessário "regulamentar qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado" [3].

Com uma sociedade cada vez mais conectada, podemos observar uma tendência no ordenamento jurídico no que tange o tratamento dos dados pessoais, com o desenvolvimento das leis de proteção de dados foi formada a base para considerarmos a proteção de dados um direito fundamental [8]. Episódios de vazamento de dados têm sido cada vez mais recorrentes nos dias de hoje, um dos mais famosos é o Caso Cambridge Analytica em que dados de mais de 50 milhões usuários do Facebook foram utilizados sem consentimento com fins de propaganda política [9]. Esses casos de vazamentos reativaram as propostas de medidas regulatórias o que acabou gerando a Lei Geral de Proteção de Dados Pessoais (LGPD). No Brasil, algumas normas já regulavam o direito à privacidade e à inviolabilidade da intimidade e da vida privada como a Constituição Federal(art. 5º, X) e o Marco Civil da Internet [4] que regulamenta e orienta para usuários e provedores os procedimentos do uso da Internet no Brasil [8].

Neste contexto, a pergunta que será respondida nesta pesquisa é: “Quais os aspectos necessários envolvidos a ser considerado na elaboração de uma ferramenta computacional para cumprir os requisitos de adequação legal e tecnológica às normas nacionais vigentes?”

Este trabalho tem como objetivo estudar normas legais sobre proteção de dados e privacidade no âmbito nacional, levantar os principais conceitos necessários para estarem contidos em uma ferramenta computacional, no intuito de desenvolver um *framework* utilizando uma ontologia desenvolvida no software Protégé para representar o conhecimento da Lei Geral de Proteção de Dados (LGPD) [3]. Um estudo sobre este assunto pode ser considerado

complicado porque são documentos jurídicos, são documentos diversos, que precisam ser interpretados e aplicados por profissionais da área de tecnologia, sendo um assunto que se torna cada vez mais necessário no cenário profissional atual. Desse modo, nasce a necessidade de criar algo que simplifique a aplicação da legislação, sem prejuízo da lei, com uma interpretação simplificada da norma, representando este conhecimento para a área de tecnologia.

A seguir, será realizado um estudo da norma sobre proteção de dados, apresentando seus principais fundamentos e objetivos, bem como o referencial teórico sobre o tema. Após o referencial teórico, na seção 3, é apresentada a metodologia utilizada neste trabalho, com os métodos e etapas realizadas durante a pesquisa, explicando todas as ações a serem desenvolvidas nos métodos. A Seção 4, será apresentado o Framework e todos os aspectos que englobam a sua confecção. A Seção 5 é responsável por mostrar as limitações deste estudo e por fim, a Seção 6, realiza a conclusão e mostra o trabalho futuro desta pesquisa.

II. Referencial Teórico

Com o rápido crescimento da internet e a geração de informações, tornou-se necessário o debate acerca da proteção de dados pessoais e privacidade. Em 2012 começou a ser idealizado pela Comissão Europeia a revisão das regras estabelecidas sobre proteção de dados, porém, somente no ano de 2016, foi promulgado o adote do Regulamento 2016/679 e posteriormente, em 25 de maio de 2018 foi implementada a *General Data Protection Regulation (GDPR)*[1]. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) veio posteriormente, inspirando-se na *General Data Protection Regulation* (GDPR). Inspirada na lei europeia, a lei brasileira tem finalidade de realizar a proteção dos dados pessoais de pessoas físicas, ou seja, dados de organizações não estão contemplados, mas sim, os dados de pessoas físicas que são coletados, tratados e armazenados por pessoas jurídicas. Apesar da Lei Geral de Proteção de Dados Pessoais (LGPD) ser amplamente conhecida, ela não é a única que trata a proteção de dados no Brasil, legislações anteriores como o Marco Civil da Internet [4] já abordavam garantias, direitos e deveres para o uso da internet no Brasil.

No âmbito internacional temos algumas regulamentações importantes para este estudo, como a Lei Francesa de Proteção de Dados Pessoais de 1978 que tange o processamento automatizado de dados e o Regulamento Geral de Proteção de Dados da União Europeia que serviu como base para elaboração do projeto de lei brasileiro é o considerado a norma mais completa e estrutura como devem ser tratados os dados pessoais [Lorenzon 2021]. Uma das bases legais para a norma europeia é a necessidade do consentimento inequívoco dos usuários para a operacionalização do uso dos dados e também o reconhecimento da importância da proteção de dados pessoais;expansão do entendimento dos dados e quaisquer dados possíveis que permitam identificar o usuário; expansão dos direitos dos titulares dos dados; direito ao esquecimento e portabilidade;sanções a desrespeito do regulamento e o reporte obrigatório de incidentes à Autoridade de Controle relativo aos dados pessoais [OMAR et al. 2021].

A Lei Geral de Proteção de Dados Pessoais é um marco importante na legislação brasileira, considerada um grande avanço devido sua abrangência e especificidade e tem como fundamentos: o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão; de informação; de comunicação e de opinião; a inviolabilidade da intimidade; da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais [3].

A. Procedimentos de adaptação à GDPR e LGPD

A partir de quando a lei entra em vigor, as organizações buscam as suas exigências para se adequarem, seguindo a experiência de adequação da GDPR[1], foram utilizadas majoritariamente as seguintes práticas; montar um time ou responsável para garantir a conformidade, realizar treinamentos anuais de privacidade e segurança para todos os funcionários da organização, criar e atualizar as políticas internas e outros documentos para garantir a conformidade constante, implementar processos de resposta a incidentes e planos de recuperação, implementar uma política para dispositivos móveis com o objetivo de garantir a segurança e restringir a utilização de informações confidenciais. investir em certificações *Privacy Shield* , implementar um programa de segurança e privacidade para Fornecedores. [15].

O compliance é um dos pilares de segurança na adequação das medidas regulatórias de proteção de dados pessoais como a Lei geral de proteção de dados (LGPD) e a Regulamento Geral sobre a Proteção de Dados(GDPR), compliance pode ser definido como um conjunto de instruções ou procedimentos que tenham como escopo aderir às normas legais, criar e gerir políticas internas [16] fazer o papel de controles internos para evitar inconformidades com as medidas regulatórias.

[1]

Um item que ambas leis implementaram foi necessidade de haver 3 papeis específicos em organizações co mais de 250 funcionários, esses papeis são os: Data Protectio Officer (DPO) ou encarregado, controladores e operadores.

Na GDPR, controladores e operadores possuem a mesma responsabilidade, na LGPD define-se controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais e o encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) [3].

III. Metodologia

Neste trabalho, o início foi a definição do tema de pesquisa e discussões com os professores orientadores para projetar uma pesquisa. Após a definição do tema, o próximo passo foi a fase de levantar o problema de pesquisa assim a fim de viabilizar a bibliografia que servirá como base para a construção desse trabalho, a bibliografia teve como objetivo levantar as informações sobre privacidade e proteção de dados pessoais na era tecnológica, normas legais e internacionais que tange a proteção desses dados, *privacy by design*, compliance e documentação de apoio para construção de um framework conceitual.

Este estudo terá a construção de um framework que contará com os parâmetros legais que servirá como instrução para adequação para a LGPD, onde será usada uma ferramenta online para criação de uma ontologia. A natureza da pesquisa desenvolvida se identifica como aplicada, pois é proposto a criação de um framework para construção de uma ferramenta tecnológica para compliance, já a abordagem é qualitativa, visto que busca o desenvolvimento de um framework para servir de instrução, a finalidade é classificada como metodológica, pois o framework servirá como um fluxograma de trabalho para servir como instrução de uma ferramenta tecnológica para atender o compliance, por isso a pesquisa também é propositiva, os meios dessa pesquisa são definidos em dois, sendo eles; Estudo de caso: Estudo investigando casos de organizações e instituições para levantar os problemas enfrentados na adequação de normas nacionais e internacionais e que será utilizado na implementação do framework; Bibliográfica: É utilizado uma bibliografia que contém artigos, livros, estudos, notícias, etc sobre o tema pesquisado.

IV. Framework Conceitual Proposto

O framework conceitual deverá evidenciar as instruções e conceitos contidos na pesquisa [AZEVEDO, 2016]. O framework conceitual deve ter um objetivo específico pode ser em texto, em formato de tabela informativa ou fluxograma. Para construir um framework conceitual devemos pensar na praticidade e usabilidade do framework, levando em conta os principais aspectos técnicos. Segundo Leung e Cockburn (2021) além de pensar na praticidade devemos levar em consideração os problemas e realizar as seguintes perguntas: Parâmetros - Como podemos especificar o framework de forma visual e objetiva numa forma que os computadores e usuários podem interpretar o framework e suas instruções indubitavelmente; Estrutura - Qual o relacionamento entre os elemento? Como eles harmonizam entre si ou podem ser aplicados em uma Design de interface de usuário(UI)? Problemas na implementação - Como as ferramentas gráficas podem ser usadas para atingir os requisitos? Adequação ao propósito - Como as técnicas existentes podem ser descritas? Que combinações de técnicas podem ter sido deixadas de lado do referencial teórico?

A. Proteção de Dados e Privacy by Design

A proteção de dados pessoais é um direito e segue alguns princípios, sendo eles: finalidade; necessidade; adequação; escolha; livre acesso; segurança e transparência [8], a proteção de dados é aplicada tanto ao setor público quanto privado, na Lei Geral de Proteção de Dados Pessoais [3], tem como fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão; de informação; de comunicação e de opinião; a inviolabilidade da intimidade; da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Diante das inovações tecnológicas e do aumento de consumo de dados, novas utilizações e fins para os dados pessoais foram criados, sendo necessário "regulamentar qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado" [Lei No 13.709/2018].

Com base para o desenvolvimento do Framework, devemos considerar as condições para tornar-se legal a coleta de dados, tratamento, processamento e armazenamento conforme a Lei Geral de Proteção de Dados Pessoais(LGPD) :

V. Finalidade: Propósitos legítimos, específicos, explícitos e informados ao titular.´

VI. Adequação: O tratamento deve ser compatível com a finalidade.

VII. Necessidade: Processar o tratamento ao mínimo

necessário de acordo com a finalidade.

VIII. Livre acesso: Garantir ao Titular acesso facilitado e gratuito aos seus dados.Qualidade dos dados: Os dados devem ser exatos e atualizados.

IX. Transparência: Garantir ao Titular a exatidão e informações claras quanto aos tratamentos dos dados.

X. Segurança: Implementar medidas técnicas e administrativas para proteger os dados pessoais.

XI. Prevenção: Implementar medidas para prevenir as violações de segurança.

XII. Não discriminação: Proibido tratar os dados para fins discriminatórios, ilícitos ou abusivos.

XIII. Responsabilização: Adotar e demonstrar as medidas adotadas para conformidade e cumprimento das normas e suas eficiências.

Além das condições acima, deve-se considerar um conceito que foi desenvolvido nos anos 1990 para endereçar problemas cada vez mais complexos de sistemas de informação e de comunicação de dados em larga escala [Cavoukian,2009]. Este conceito evidencia que a privacidade e a proteção de dados não podem ser garantidos apenas por frameworks de compliance ou normas regulatórias e sim que a privacidade deve estar incorporada nas operações da instituição, desde desenvolvimento de novos produtos, serviços, processos e etc, deve estar no modus operandi da instituição. Portanto, conclui-se que depender apenas de uma ou algumas instruções para adequação de medidas regulatórias de privacidade não é o suficiente, e uma necessidade de um framework para unificar os conceitos atuais para que irá instruir a criação de uma ferramenta computacional para atender o direito de privacidade e melhores práticas no tratamento de dados.

B. Representação de recursos necessários e requisitos da LGPD

A tabela a seguir, foi desenvolvida está embasada nas considerações da Lei geral de Proteção de Dados Pessoais [3] e na referência bibliográfica que compõe este artigo. Foi levantado os principais requisitos para o desenvolvimento de uma aplicação e com base nos requisitos da Lei Geral de Proteção de Dados Pessoais [3] .

A tabela é composta por 26 requisitos centrais e 3 classificações, sendo assim, a estrutura da tabela é:

- Requisitos: Foram os requisitos levantados para a criação de uma ferramenta tecnológica seguindo a Lei geral de Proteção de Dados Pessoais(LGPD)
- Humano: Esta coluna indica se o requisito envolve alguma intervenção humana. Se marcada, é sugerido que a responsabilidade pela implementação do requisito cai sob responsabilidade de alguém da organização.
- Tecnológico: Esta coluna indica se o requisito envolve a utilização de tecnologia. Se marcada, é sugerido que haja implementação de soluções tecnológicas.
- Requisito Legal: Esta coluna indica se o requisito está mencionado explicitamente na Lei geral de Proteção de Dados Pessoais(LGPD).

Tabela 1. Representação de recursos necessários e requisitos da LGPD

Requisitos	Humano	Tecnológico	Requisito Legal
Consentimento do titular dos dados	X		X
Anonimização dos dados		X	X
Proteção e segurança dos dados	X	X	X
Notificar violação de dados	X	X	X
Nomear um Encarregado(Data Protection Officer)	X		X
Ter políticas de privacidades claras	X		X
Registrar e documentar atividades de tratamento de dados	X	X	X
Relatório de Impacto à Proteção de Dados	X		X
Limitar a coleta de dados		X	X
Limitação do uso, acesso e divulgação de dados	X	X	X
Possibilidade do titular solicitar revisão de decisões automatizadas	X	X	
Atender direitos dos titulares	X	X	X
Fornecer informação sobre a coleta de dados no momento da coleta	X		X
Implementar medidas de segurança, técnicas e administrativas para proteção dos dados	X	X	X

Fornecer acesso fácil e gratuito sobre processamento	X	X	X
Realizar auditorias	X	X	X
Excluir dados após uso	X	X	X
Portabilidade	X	X	X
Transparência	X	X	X
Prevenção	X	X	X
Adequação Contratos	X		X
Treinamentos	X		
Resposta incidentes e recuperação	X	X	X
Resposta aos titulares e a Autoridade Nacional de Proteção de Dados (ANPD)	X	X	X
Revisão e atualização de políticas de privacidade e internos	X		X
Procedimentos de reclamações ou consultas	X	X	

Fonte: autores

C. Ontologia e Design Science Research

A ontologia de acordo com [5] é a possibilidade de representar a existência de objetos e eventos, assim como as suas relações, com esse conceito, o presente trabalho irá apresentar os requisitos técnicos das medidas legais e montar a suas relações com as regulamentações através de uma ontologia.

Os autores do termo Design Science, segundo [14] concordavam que era necessário ter uma abordagem mais sistematizada para representação de artefatos. No Design Science Research (DSR), um problema prático deve guiar a pesquisa e através desses problemas surgirão novos problemas e questionamentos sobre o conhecimento [14]. No presente trabalho, o Design Science Research (DSR)possui um papel metodológico para realizar o design do framework de forma sistematizada considerando uma área de conhecimento e um problema prático que a dificuldade em aderir a proteção de dados como medidas técnicas.

A ontologia deste presente trabalho indica-se que seja utilizada juntamente com a tabela de requisitos, Tabela 1, para melhor compreensão do conhecimento representado.

D. Protegé

A ferramenta utilizada para o desenvolvimento da ontologia é o Protégé, um software *open-source* e editor de ontologias, que inicialmente foi idealizado para aquisição de conhecimento, tornou-se um software para desenvolvimento e pesquisa de sistemas inteligentes baseados em conhecimento [12]. O Protégé possui diversas opções para desenvolvimento de modelos de conhecimentos, a sua principal é o Web Ontology Language(OWL), uma linguagem para instanciar ontologias conforme World Wide Web Consortium(W3C)[2].

As ontologias criadas no Protégé podem ser exportadas em diversos formatos como RDF\XML, OWL/XML, Turtle Syntaxes, entre outros.

Na ontologia há relacionamentos, definidos por *Object Properties*, entre classes do modelo e instâncias de classes e subclasses. Exemplos de relacionamentos para relacionar classes (Propriedades de Objeto), que foram implementadas na ontologia estão sendo mostrados na Figura 1 e 2, respectivamente.

Figura 1. Classes da ontologia no Protégé

Figura 2. Propriedade de Objeto da ontologia no Protégé

Com as classes, subclasses, relacionamentos e propriedade de objetos definidos, obtemos a seguinte ontologia que precisou ser divida em 4 figuras, Figuras 3, 4, 5 e 6 respectivamente, para apresentação do presente trabalho.

[2] Organização que padroniza a World Wide Web.

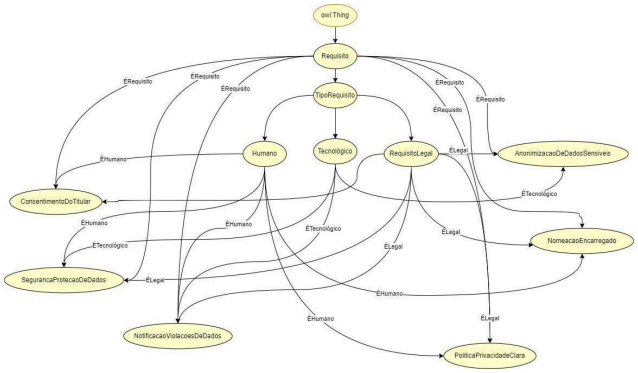

Figura 3. Primeira parte da ontologia.

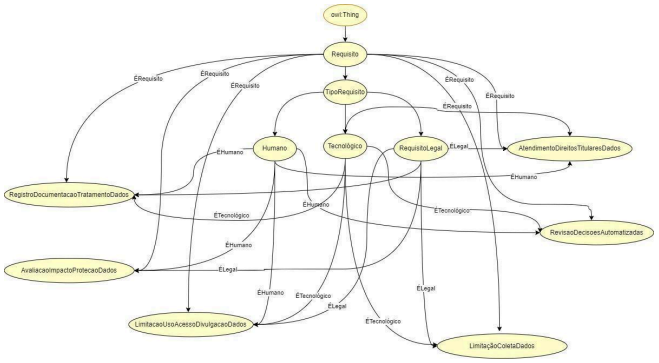

Figura 4. Segunda parte da ontologia

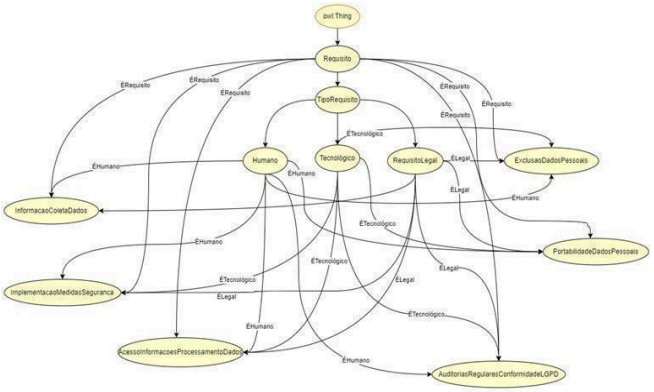

Figura 5. Terceira parte da ontologia

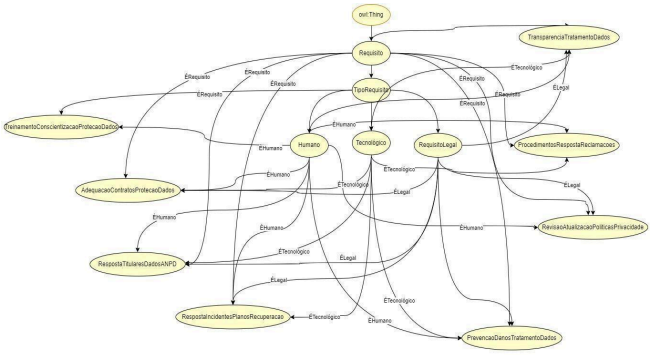

Figura 6. Quarta parte da ontologia

E. Limitações

As limitações deste trabalho foram o escopo, recursos e a não representação total e unificada da ontologia. A limitação de escopo se deve à complexidade e especificidade da Lei Geral de Proteção de Dados Pessoais (LGPD). A modelagem de uma ontologia é um processo complexo e desafiador, especialmente quando aplicada a novos cenários tecnológicos. A falta de ontologias comparáveis dificulta a criação e validação da ontologia. Devido a quantidade de requisitos não foi possível a representação total da ontologia, pois comprometeria a visibilidade.

V. Considerações Finais

O trabalho destaca a importância do framework proposto como uma referência prática para empresas que buscam conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). O estudo identificou e delineou medidas técnicas e administrativas essenciais para a proteção de dados, visando facilitar a adequação aos requisitos legais e a construção de ferramentas computacionais seguras e eficientes. Apesar das limitações enfrentadas, como a não validação do modelo proposto, o framework sugere um ponto de partida robusto para o desenvolvimento de soluções voltadas à proteção de dados e à privacidade.

Além disso, o trabalho contribui significativamente para o campo de compliance e segurança de dados, principalmente ao abordar os desafios enfrentados por empresas e instituições ao implementar a LGPD em um contexto prático. A proposta de um framework baseado em ontologias permite a representação estruturada das necessidades legais, técnica inovadora para traduzir regulamentações jurídicas em um formato compreensível e aplicável para profissionais de tecnologia e compliance. Esta

abordagem promove uma interpretação mais prática da LGPD, permitindo que organizações de diferentes portes e setores adequem suas operações às exigências legais sem comprometer a eficiência operacional.

Para trabalhos futuros, recomenda-se a ampliação do framework com estudos de caso específicos, que poderiam validar e ajustar as recomendações para contextos diversos, como setores de saúde e finanças, onde a proteção de dados é ainda mais crítica. Adicionalmente, uma integração com tecnologias emergentes, como inteligência artificial e blockchain, poderia reforçar a automação e a precisão das medidas de compliance, tornando o framework aplicável para o cenário de dados cada vez mais complexo e dinâmico.

Por fim, o desenvolvimento de metodologias para auditorias automatizadas e monitoramento contínuo, baseadas nos princípios do framework, poderia assegurar uma conformidade proativa, minimizando riscos e antecipando possíveis vulnerabilidades. Com esses avanços, o framework proposto não apenas atenderia às necessidades regulatórias atuais, mas também se tornaria uma base para futuras normativas e práticas globais de proteção de dados, promovendo um ambiente de inovação seguro e conforme com os padrões de privacidade e segurança esperados no futuro.

Referências

1. D. Azevedo, "Revisão de Literatura, Referencial Teórico, Fundamentação Teórica e Framework Conceitual em Pesquisa – diferenças e propósitos," *Working paper*, 2016. Disponível em: https://unisinos.academia.edu/DeboraAzevedo/Papers. Acesso em: 17 de maio de 2023.
2. Brasil, "Constituição da República Federativa do Brasil, de 5 de outubro de 1988." Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 de maio de 2023.
3. Brasil, "Lei Geral de Proteção de Dados, Lei nº 13.709 de 2018." Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 de maio de 2023.
4. Brasil, "Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014," *Diário Oficial da União*, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html. Acesso em: 17 de maio de 2023.
5. M. L. A. Campos, L. M. Campos, e J. S. Medeiros, "A representação de domínios de conhecimento e uma teoria de representação: a ontologia de fundamentação," *Informação & Informação*, vol. 16, no. 2, pp. 140-164, 2011. DOI: 10.5433/1981-8920.2011v16n2p140.
6. A. Cockburn e J. Leung, "Design Framework for Interactive Highlighting Techniques," in *Foundations and Trends® in Human-Computer Interaction*, vol. 14, pp. 96-271, 2021. DOI: 10.1561/1100000084.
7. A. Covoukian, "Privacy by Design: The 7 Foundational Principles," 2009. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 17 de maio de 2023.
8. D. Doneda, "A proteção dos dados pessoais como um direito fundamental," *Espaço Jurídico Journal of Law*, vol. 12, no. 2, pp. 91–108, 2011.
9. "Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades," G1, 23 mar. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 17 de maio de 2023.
10. França, "La loi Informatique et Libertés (1978)." Disponível em: https://www.cnil.fr/fr/la-loi-informatique-et-liberte. Acesso em: 17 de maio de 2023.
11. GDPR, "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho," 2016. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1. Acesso em: 13 de março de 2024.
12. J. H. Gennari, M. A. Musen, R. W. Fergerson, W. E. Grosso, M. Crubézy, H. Eriksson, N. F. Noy, e S. W. Tu, "The Evolution of Protégé: An Environment for Knowledge-Based Systems Development," *International Journal of Human-Computer Studies*, vol. 58, pp. 89-123, 2003.
13. L. N. Lorenzon, "Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement," 2021. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/

article/view/83423/79192. Acesso em: 17 de maio de 2022.

14. D. D. Rodrigues, "Design Science Research como caminho metodológico para disciplinas e projetos de Design da Informação," *InfoDesign - Revista Brasileira De Design Da Informação*, vol. 15, no. 1, pp. 111–124, 2018. DOI: 10.51358/id.v15i1.564.
15. SC&H Group, "7 Ways That Your Company Can Adapt to GDPR Regulations Right Now," 2019. Disponível em: https://www.schgroup.com/resource/blog-post/7-ways-that-your-company-can-adapt-to-gdpr-regulations-right-now/. Acesso em: 20 de maio de 2023.
16. D. C. Silva e J. R. Covac, *Compliance como boa prática de gestão no ensino superior privado*, São Paulo: Saraiva, 2015, pp. 181-184.