UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

CURSOS DE SISTEMAS DE INFORMAÇÃO

JOÃO PEDRO SOUTO MAIOR DE LIMA VELÔSO

DESAFIOS RELACIONADOS À PRIVACIDADE NA ERA DA INTELIGÊNCIA ARTIFICIAL: UMA REVISÃO SISTEMÁTICA

Recife
2025

JOÃO PEDRO SOUTO MAIOR DE LIMA VELÔSO

DESAFIOS RELACIONADOS À PRIVACIDADE NA ERA DA INTELIGÊNCIA ARTIFICIAL: uma revisão sistemática

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de bacharel em Sistemas de Informação.

Orientador (a): Frederico Luiz Gonçalves de Freitas

Recife
2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Velôso, João Pedro Souto Maior de Lima.

Desafios relacionados à privacidade na era da inteligência artificial: uma revisão sistemática / João Pedro Souto Maior de Lima Velôso. - Recife, 2025.

38 p.

Orientador(a): Frederico Luiz Gonçalves de Freitas

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2025.

1. Privacidade. 2. Proteção de Dados. 3. Inteligência Artificial. I. de Freitas, Frederico Luiz Gonçalves. (Orientação). II. Título.

000 CDD (22.ed.)

JOÃO PEDRO SOUTO MAIOR DE LIMA VELÔSO

DESAFIOS RELACIONADOS À PRIVACIDADE NA ERA DA INTELIGÊNCIA ARTIFICIAL: uma revisão sistemática

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de bacharel em Sistemas de Informação.

Aprovado em: 07/04/2025

BANCA EXAMINADORA

_____

Prof. Dr. Frederico Luiz Goncalves de Freitas (Orientador) Universidade Federal de Pernambuco - UFPE

_____

Profª. Drª. Carla Taciana Lima Lourenço Silva (Examinador Interno) Universidade Federal de Pernambuco - UFPE

Resumo

A crescente adoção da Inteligência Artificial (IA) tem gerado avanços em diversas áreas, mas também intensificado preocupações sobre privacidade e proteção de dados pessoais. A falta de transparência nos controles técnicos e legais para o cumprimento das regulamentações mundiais representa um risco significativo à privacidade dos usuários. Este estudo realizou uma revisão sistemática da literatura, analisando 42 artigos provenientes de bases científicas relevantes, com o objetivo de identificar as consequências do descumprimento das boas práticas e as obrigações legais previstas nas regulamentações de privacidade. Os resultados destacaram sanções financeiras e danos reputacionais como os principais impactos negativos mais citados, seguido da importância de técnicas que acompanhem desde criação do sistema até a posterior transparência sobre os processos e políticas de proteção de dados existentes.

Palavras-chave: desafios; privacidade; inteligência artificial; práticas legais;proteção de dados

Abstract

The increasing adoption of Artificial Intelligence (AI) has driven advancements in various fields but has also heightened concerns about privacy and personal data protection. The lack of transparency in technical and legal controls for compliance with global regulations poses a significant risk to user privacy. This study conducted a systematic literature review, analyzing 42 articles from relevant scientific databases, aiming to identify the consequences of non-compliance with best practices and the legal obligations outlined in privacy regulations. The results highlighted financial penalties and reputational damage as the most frequently cited negative impacts, followed by the importance of techniques that monitor systems from creation to post-deployment transparency regarding data protection processes and policies.

Keywords: challenges; privacy; artificial intelligence; legal practices; data protection.

1 Introdução

Desde a promulgação do Regulamento Geral de Proteção de Dados (General Data Protection Regulation - GDPR), a proteção de dados pessoais tornou-se um tema central nas discussões sobre direitos fundamentais em um ambiente digital cada vez mais complexo [EP17]. No entanto, a ascensão das tecnologias de Inteligência Artificial (IA) trouxe desafios adicionais à implementação das boas práticas estabelecidas por legislações como o GDPR e a Lei Geral de Proteção de Dados (LGPD) [EP33]. Com o uso crescente de algoritmos de aprendizado de máquina em atividades cotidianas, a falta de conhecimento sobre o tratamento desses dados tem gerado resistência no cumprimento dos direitos legais dos indivíduos, ampliando os riscos associados à privacidade.

Este trabalho tem como objetivo investigar como a literatura científica aborda os desafios relacionados à privacidade no contexto da Inteligência Artificial (IA), destacando as inovações e perspectivas apresentadas pelos pesquisadores. A crescente adoção de sistemas baseados em IA tem gerado debates significativos sobre a proteção de dados pessoais, especialmente diante da complexidade técnica e regulatória envolvida. Nesse cenário, é essencial compreender como os estudos acadêmicos têm explorado questões como as implicações legais, a transparência no uso de dados e as estratégias para garantir a privacidade conforme os estudos de [EP13] e [EP05].

A revisão sistemática realizada neste estudo busca identificar tendências na literatura, analisando os principais tópicos abordados pelos pesquisadores, como regulamentações de proteção de dados, técnicas de preservação de privacidade e frameworks para avaliação de riscos. Além disso, o trabalho examina as visões existentes nos estudos e propõe reflexões sobre as práticas atuais no campo da IA.

2 Referencial Teórico e Trabalhos Relacionados

Com a modernização da sociedade para o mundo digital, as instituições globais, pouco a pouco, saíram do meio físico. Essa mudança fez com que os cidadãos, antes conhecidos apenas por seus documentos físicos, se transformassem em usuários digitais, aumentando a disseminação de dados pessoais. A privacidade, por ser um direito fundamental discutido desde 1948 com a Declaração Universal dos Direitos Humanos (DUDH), influenciou a urgência pela criação de legislações e normas que garantissem o cumprimento desse direito Peck Pinheiro (2022).

Nos últimos anos, a chamada era da inteligência artificial trouxe consigo outros fatores que agravam a problemática da proteção de dados dos indivíduos, necessitando de uma análise do panorama atual dos estudos relacionados ao tema.

2.1 Privacidade

Privacidade é um conceito multidimensional que se refere ao direito de um indivíduo de controlar o acesso e o uso de suas informações pessoais. De acordo com Westin (1967), a privacidade pode ser definida como "a reivindicação de indivíduos, grupos ou instituições de determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outros". Essa definição enfatiza a autonomia do indivíduo sobre suas informações pessoais.

No contexto da era digital, Solove (2006) evolui o conceito de privacidade para incluir a proteção contra a coleta, armazenamento e uso indevido de dados pessoais por sistemas de informação. Ele argumenta que a privacidade não é apenas um direito individual, mas também uma questão de justiça social, pois a falta de privacidade pode levar à discriminação e ao abuso de poder.

Já Morgulis (2023), com uma abordagem moderna, define a privacidade da informação como a capacidade do indivíduo de controlar informações sobre si próprio. Com o passar do tempo, o conceito de privacidade tornou-se mais maduro, englobando os aspectos de

liberdade, não-repúdio e a busca pela não exposição dos cidadãos, respeitando seu direito constitucional.

2.2 Proteção de Dados

O Regulamento Geral de Proteção de Dados (GDPR), introduzido pela União Europeia em 2016, define dados pessoais como qualquer informação sobre um indivíduo identificado ou identificável. Como um tópico dentro do conceito de privacidade, a proteção de dados refere-se às práticas, políticas e regulamentações que visam garantir que os dados pessoais sejam coletados, armazenados, processados e compartilhados de maneira segura e ética. A abordagem de Bygrave (2002) define a proteção como: "o conjunto de normas e procedimentos que visam proteger os dados pessoais contra acesso não autorizado, uso indevido, alteração ou destruição".

Como uma resposta à crescente coleta de dados e ao processamento de informações pessoais na era digital, o objetivo da Proteção de Dados é garantir a segurança e a integridade de dados pessoais, uso indevido, perda ou destruição.

2.2.1 Legislação para Proteção de Dados

A governança de dados abrange políticas, procedimentos e controles que visam garantir a segurança, a integridade e a privacidade dos dados ao longo de seu ciclo de vida. Nesse contexto, algumas legislações foram criadas para fortalecer a prática da proteção de dados. Entre as mais relevantes, é possível destacar a Regulamentação Geral de Proteção de Dados (General Data Protection Regulation - GDPR) da União Europeia e a Lei Geral de Proteção de Dados (LGPD) do Brasil.

2.3 Inteligência Artificial

Charmet et al. (2022) define Inteligência Artificial (IA) como a prática de programar computadores para terem intelecto comparável ao dos humanos e a capacidade de emular o comportamento humano. Ela se baseia em máquinas e utiliza estratégias de resolução de problemas e aprendizado para compreender atividades com altos graus de aspectos inspirados nos humanos, tomada de decisões e ciclos emocionais. A IA permite que sistemas executem etapas complexas, superando a capacidade humana, aprendendo e se treinando automaticamente ao longo do tempo usando Aprendizagem de Máquina (ML). O ML é um componente da IA que possibilita o desenvolvimento de Sistemas de Tomada de Decisão Algorítmica (ADSs)[EP04].

Existem diversos tipos e funções para classificação de uma IA. De forma geral, classificando por funcionalidade, [EP23] inclui em suas distinções:

- IA fraca ou limitada: Projetada para executar tarefas específicas e pré-definidas, como os assistentes virtuais (Siri da Apple e Alexa da Amazon), processamento de linguagem natural, recomendação de produtos.
- IA forte ou geral: Projetada para ser um tipo hipotético com capacidade intelectual de um ser humano, capaz de aprender e aplicar o conhecimento em diversas tarefas. É um conceito ainda em desenvolvimento.

A partir dos conceitos de Inteligência Artificial por funcionalidades, após o surgimento do ChatGPT, Copilot, um dos tipos se popularizou, a Generativa (Generative AI - Gen AI). IA Generativa, segundo [EP09], se concentra na geração de novos dados que se assemelham aos dados de treinamento, podendo gerar vários tipos de conteúdo como produto. No entanto, [EP12] destaca a necessidade de um vasto conjunto de dados para treinar o modelo de forma efetiva para uso.

2.4 Trabalhos Relacionados

Foi realizada uma busca na base de dados Google Scholar, utilizando a string de busca:

“systematic review” AND (“privacy” OR “data protection”) AND (“artificial intelligence” OR “machine learning”) AND (“ethics” OR “transparency”) AND (“GDPR" OR "LGPD”)”

Utilizando o filtro dos últimos 5 anos, foi encontrado apenas um estudo relacionado com a abordagem deste trabalho. Em suma, os outros estudos abordaram temas mais amplos do que a proteção de dados ou privacidade, além de não terem foco nos aspectos de desafios à privacidade no contexto da IA.

O estudo de Giordano et al. (2022) analisou o uso de técnicas de IA para mitigar vulnerabilidades relacionadas à privacidade em sistemas de IoT. No entanto, a linha de raciocínio seguia para análise da utilização de técnicas que melhorem a privacidade nas bases de dados que os sistemas utilizavam. Em contrapartida, o presente trabalho busca identificar impactos legais, técnicos e de conformidade para garantir a privacidade no uso dos sistemas baseados em inteligência artificial. A combinação dessas abordagens e a dificuldade em encontrar uma literatura focada nesses aspectos, aumenta a importância do presente estudo.

3 Metodologia

Com base nos conceitos apresentados no referencial teórico, que exploraram as dimensões da privacidade, proteção de dados e os desafios impostos pela Inteligência Artificial (IA), torna-se evidente a necessidade de uma abordagem estruturada para investigar as questões levantadas. A literatura revisada destacou a complexidade do tema, abrangendo aspectos técnicos, legais e éticos, o que reforça a importância de um método sistemático para identificar os principais desafios e soluções relacionados à privacidade no contexto da IA.

Dessa forma, este estudo adota a Revisão Sistemática da Literatura (RSL) como metodologia principal. Essa escolha se justifica pela capacidade da RSL de organizar e

sintetizar o conhecimento existente na área, permitindo uma análise abrangente das evidências científicas disponíveis. A seguir, detalham-se as etapas metodológicas empregadas para garantir rigor e consistência na condução da pesquisa.

A metodologia de Kitchenham e Charters (2007) é composta por sete etapas distintas:

1. Planejamento
2. Protocolo de pesquisa
3. Definição e aplicação de filtros
4. Qualificação dos estudos
5. Seleção de artigos
6. Coleta de evidências
7. Análise e síntese dos dados

As etapas foram utilizadas para consolidar os dados que fundamentam este estudo, conforme ilustrado na Figura 1.

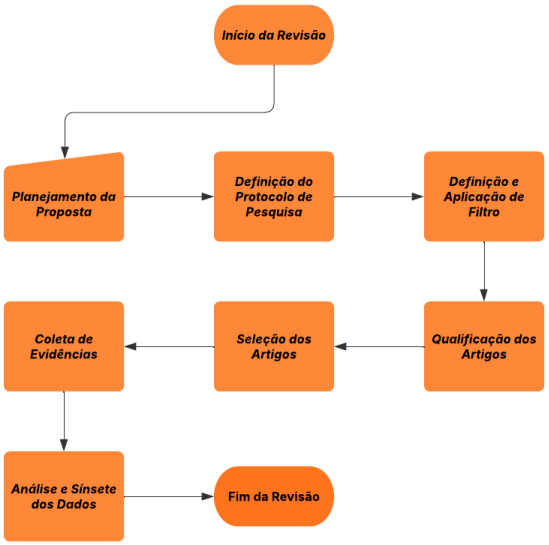

Figura 1: Etapas da Metodologia

Nas primeiras etapas, o problema central de pesquisa, assim como as perguntas de pesquisa são definidas. Seguidas das definições de quais bibliotecas digitais serão pesquisadas e da criação da string de busca, além dos critérios de inclusão e exclusão para validar o protocolo. Em seguida, são realizadas buscas sistemáticas em bases de dados científicas para identificar estudos relevantes, aplicando critérios de seleção e avaliando a qualidade dos estudos escolhidos. Em seguida, os dados são extraídos e sintetizados para responder às perguntas da pesquisa. A última fase é a documentação dos resultados encontrados.

A aplicação desta metodologia possibilitou a organização de conceitos e a compreensão das principais problemáticas relacionadas à privacidade no contexto da inteligência artificial.

3.1 Questões de Pesquisa

O objetivo geral desta pesquisa é investigar os principais desafios relacionados à privacidade impostos pela inteligência artificial (IA) no processamento de dados pessoais. O estudo do estado da arte do tema é necessário para identificar as evidências científicas existentes, as principais áreas de pesquisa que envolvem IA e privacidade, e elencar as principais dificuldades na proteção de dados. Visando a concordância com essas temáticas, a pesquisa tem como questão central: “Quais são os principais desafios relacionados à privacidade impostos pelo uso da IA para o processamento de dados pessoais?”. A partir da questão central, foram elaboradas três questões específicas para concretizar e aprofundar o tema, vistas na tabela 1 abaixo:

ID	**Questão de Pesquisa**	**Motivação**
QP1	Quais as implicações legais para o não cumprimento das boas práticas de proteção de dados?	Identificar as medidas legais que poderiam impactar indivíduos ou organizações que não buscam medidas para a proteção de dados.

QP2	Quais as principais	Fazer um levantamento
	consequências da falta de transparência sobre como as IAs utilizam dados pessoais?	sobre as dores que os usuários estão suscetíveis com a falta de transparência dos sistemas de IA.
QP3	Quais são as principais medidas tomadas para garantir a privacidade no uso da IA?	Entender quais são as boas práticas utilizadas para garantir a privacidade no contexto da IA.

Tabela 1: Questões de Pesquisa

3.2 String de Pesquisa

Para garantir uma cobertura abrangente e relevante da literatura científica, foi desenvolvida uma string de busca detalhada, adaptada especificamente para a RSL.

(("privacy" OR "data protection" OR "personal data" OR "sensitive data") AND
("artificial intelligence" OR "AI" OR "machine learning" OR "deep learning") AND
("transparency" OR "ethics" OR "accountability" OR "data governance") AND
("compliance" OR "best practices" OR "legal frameworks" OR "regulatory practices") AND
("challenges" OR "limitations" OR "legal implications" OR "policy")) AND ("systematic review" OR "literature review")

Posteriormente, visando uma abordagem mais objetiva e prática, que fosse assertiva e refinasse a coleta com os estudos mais relevantes de privacidade e inteligência artificial, foi definida uma versão final simplificada dessa string.

("privacy" OR "data protection") AND ("artificial intelligence" OR "machine learning") AND ("ethics" OR "transparency") AND ("GDPR" OR "LGPD")

Além de trazer as palavras-chaves com relação a todas as perguntas de pesquisa, alguns temas foram escolhidos por sua abrangência, enriquecendo a seleção de estudos com abordagens de vários campos de estudo. As siglas relacionadas às legislações foram adicionadas para selecionar estudos que fizessem menção às leis, trazendo pontos jurídicos relevantes para as implicações legais.

3.3 Seleção dos Estudos

Com a finalização das questões de pesquisa e definição da string de busca, foi necessário selecionar as bibliotecas digitais que garantiriam a qualidade e relevância dos resultados obtidos. Foram selecionadas três bases científicas que contemplam áreas tecnológicas e jurídicas relacionadas ao tema, sendo elas: IEEE Xplore Digital Library, ACM Digital Library e Elsevier Science Direct. Após a primeira consulta, foram encontrados 916 estudos, dos últimos 5 anos.

Biblioteca Digital	**Quantidade de Estudos**
IEEE	218
ACM	317
Science Direct	391

Tabela 2: Quantidade dos Estudos na primeira busca

3.4 Critérios de Seleção

A pesquisa focou na seleção de critérios que favorecessem a relação com o tema principal. Os estudos teriam que abordar privacidade, governança, IA ou legislações. Para desfavorecer um dos pontos de ameaça à validade, requisitos como linguagem de escrita, tempo de publicação e temática foram ajustados. Esses critérios estão apresentados na tabela abaixo.

ID	**Critério de Inclusão**
CI1	Artigos que mencionam privacidade, governança ou IA.
CI2	Artigos que mencionam LGPD ou GDPR.
CI3	Artigos em Inglês ou português.
CI4	Artigos de revisão e Journals.
ID	**Critério de Exclusão**
CE1	Artigos que não mencionem governança, privacidade ou IA
CE2	Artigos publicados há mais de 6 anos.
CE3	Artigos com menos de 5 páginas
CE4	Artigos com mais de 30 páginas
CE5	Artigos que não estejam em ingles ou portugues
CE6	Artigos que não tenham informações relacionadas aos critérios de inclusão

Tabela 3: Critérios de Inclusão e Exclusão

A lista atualizada de artigos foi gerada após aplicação dos critérios, ressaltando a extensão no período de publicação dos artigos, para agrupar aqueles que fossem baseados na Lei de Proteção de Dados (LGPD). Primeiramente, foi realizada a seleção pela leitura dos títulos, seguida da leitura dos resumos dos estudos restantes. Até a aplicação do critério CE5, existiam 312 artigos, com a inclusão desse critério, restaram 160. Essa etapa foi importante para remover os estudos que não tinham informações conclusivas e poderiam enviesar o resultado.

Biblioteca Digital	**Quantidade de estudos**	**Quantidade de exclusões após filtro**	**Quantidade de artigos restantes nessa etapa**
IEEE	218	114	104
ACM	317	153	154
Science Direct	391	337	54

Tabela 4: Quantidade de Estudos no Processo de Inclusão e Exclusão

3.5 Avaliação de Qualidade

Os estudos selecionados após os filtros iniciais passaram por uma avaliação qualitativa que avaliava a aderência com a temática central, a presença de informações sobre pontos positivos e de impacto para a validade, além do impacto da pesquisa. De acordo com Kitchenham e Charters (2007), essa etapa de avaliação é crucial para garantir a qualidade do estudo. Como medida de cálculo, foram definidas as pontuações e suas respectivas categorias. Os critérios foram pontuados seguindo os valores das diretrizes de Kitchenham e Charters (2007):

- Nota 0 caso o artigo não atenda ao critério
- Nota 0,5 caso o artigo atenda parcialmente ao critério

- Nota 1 caso o artigo atenda totalmente

ID	Questões de Avaliação de Qualidade
AQ1	Existe um contexto claro do tema a ser abordado?
AQ2	A metodologia de pesquisa é bem definida?
AQ3	Existe aplicação prática dos aspectos de privacidade no contexto da IA?
AQ4	Existe uma discussão relevante sobre privacidade ou governança no uso da IA?
AQ5	As limitações e ameaças são comentadas?

Tabela 5: Questões de Avaliação da Qualidade dos Estudos

Sendo, portanto, 5, a nota máxima possível na pontuação total para a avaliação do artigo. Aqueles que obtiveram notas inferiores a 3 foram excluídos. No fim, a lista final tinha 42 artigos selecionados.

Base de Dados	Filtros de Seleção	Análise de Qualidade	Resultado final
IEEE	104	34	34
ACM	154	0	0
Science Direct	54	8	8
Total	312	42	42

Tabela 6: Quantidade de Estudos da Lista Final

ID	Título	Autores	Ano de Publicação

EP01	Trustworthy AI in the Age of Pervasive Computing and Big Data	A. Kumar; T. Braud; S. Tarkoma; P. Hui	2020
EP02	Understanding Surveillance Societies: Social Cognition and the Adoption of Surveillance Technologies	J. R. Schoenherr	2020
EP03	Ethical Principles and Governance Technology	Wu, Wenjun; Huang, Tiejun; Gong, Ke	2020

	Development of AI in China		
EP04	Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)	A. Adadi; M. Berrada	2020
EP05	AI Ethics: Algorithmic Determinism or Self-Determination ? The GPDR Approach	M. Milossi; E. Alexandropoulou-Egyptiadou; K. E. Psannis	2021
EP06	Regulatory Framework of Artificial Intelligence in Healthcare	P. H. García; D. Simunic	2021

EP07	Remote biometric identification systems and ethical challenges: The case of facial recognition	M. Milossi	2021
EP08	AI Ethics in the Public, Private, and NGO Sectors: A Review of a Global Document Collection	D. Schiff; J. Borenstein; J. Biddle; K. Laas	2021
EP09	What's up with Requirements Engineering for Artificial Intelligence Systems?	K. Ahmad; M. Bano; M. Abdelrazek; C. Arora; J. Grundy	2021
EP10	Ethics of Artificial Intelligence in Medicine and Ophthalmology	Abdullah, Yasser Ibraheem; Schuman, Joel S.; Shabsigh, Ridwan; Caplan, Arthur;	2021
		Al-Aswad, Lama A.	
EP11	An Introduction to the Principle of Transparency in Automated Decision-Making Systems	L. G. Rendón	2022

EP12	Investigating Organizational Factors Associated with GDPR Noncompliance using Privacy Policies: A Machine Learning Approach	A. -J. Aberkane; S. V. Broucke; G. Poels	2022
EP13	Responsible and Regulatory Conform Machine Learning for Medicine: A Survey of Challenges and Solutions	E. Petersen; Y. Potdevin; E. Mohammadi; S. Zidowitz; S. Breyer; D. Nowotka; S. Henn; L. Pechmann; M. Leucker; P. Rostalski; C. Herzog	2022
EP14	From ethics to standards – A path via responsible AI to cyber-physical production systems	Mezgár, István; Váncza, József	2022
EP15	Ethical implications of AI in robotic surgical training: A Delphi consensus statement	Collins, Justin W.; Marcus, Hani J.; Ghazi, Ahmed; Sridhar, Ashwin; Hashimoto, Daniel; Hager, Gregory; Arezzo, Alberto; Jannin, Pierre; Maier-Hein, Lena; Marz, Keno; Valdastri, Pietro;	2022

		Mori, Kensaku; Elson, Daniel; Giannarou, Stamatia; Slack, Mark; Hares, Luke; Beaulieu, Yanick; Levy, Jeff; Laplante, Guy; Ramadorai, Arvind; Jarc, Anthony; Andrews, Ben; Garcia, Pablo; Neemuchwala, Huzefa; Andrusaite, Alina; Kimpe, Tom; Hawkes, David; Kelly, John D.; Stoyanov, Danail	
EP16	A survey on federated learning for security and privacy in healthcare applications	Coelho, Kristtopher K.; Nogueira, Michele; Vieira, Alex B.; Silva, Edelberto F.; Nacif, José Augusto M.	2023
EP17	Data Privacy Threat Modelling for Autonomous Systems: A Survey From the GDPR's Perspective	N. Azam; L. Michala; S. Ansari; N. B. Truong	2023
EP18	A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle	S. Shahriar; S. Allana; S. M. Hazratifard; R. Dara	2023

EP19	Designing a Framework for Explainable Health Recommender System Based on the Ecuadorian	B. Jaramillo; E. Loza-Aguirre; L. Terán	2023

	Data Protection Regulations		
EP20	From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy	M. Gupta; C. Akiri; K. Aryal; E. Parker; L. Praharaj	2023
EP21	Automated Transparency Evaluation of Knowledge Graphs for Clinical Risk Governance	M. Basereh; M. Ward; U. Geary; U. Healy; M. Fogarty; A. Caputo; R. Brennan	2023
EP22	Security and Privacy Challenges of Participatory Sensing in Natural Disaster Management	M. Alswailim	2023
EP23	Bias Detection for Customer Interaction Data: A Survey on Datasets, Methods, and Tools	A. Donald; A. Galanopoulos; E. Curry; E. Muñoz; I. Ullah; M. A. Waskow; M. Dabrowski; M. Kalra	2023

EP24	Stores are Liable for Their Robots!? An Empirical Study on Liability in HRI with an Anthropomorphic Frontline Service Robot	P. Busch; J. Kirchhoff; J. S. Heinisch; K. David; O. v. Stryk; J. Wendt	2023
EP25	A survey on federated learning for security and privacy in healthcare applications	Coelho, Kristtopher K.; Nogueira, Michele; Vieira, Alex B.; Silva, Edelberto F.; Nacif, José Augusto M.	2023
EP26	Data-Driven Learning for Data	Xu, Jimin; Hong, Nuanxin; Xu,	2023

	Rights, Data Pricing, and Privacy Computing	Zhening; Zhao, Zhou; Wu, Chao; Kuang, Kun; Wang, Jiaping; Zhu, Mingjie; Zhou, Jingren; Ren, Kui; Yang, Xiaohu; Lu, Cewu; Pei, Jian; Shum, Harry	
EP27	Possibilities and challenges for artificial intelligence and machine learning in perioperative care	Meijden, S. L. van der; Arbous, M. S.; Geerts, B. F.	2023
EP28	Unveiling the black box: A systematic review of Explainable Artificial Intelligence in medical image analysis	Muhammad, Dost; Bendechache, Malika	2024

EP29	Towards a Responsible AI Metrics Catalogue: A Collection of Metrics for AI Accountability	B. Xia; Q. Lu; L. Zhu; S. U. Lee; Y. Liu; Z. Xing	2024
EP30	International Insights on AI Risk: Comparative Analysis of International Organizations	S. I. Aksoy Ercan; O. Akin	2024
EP31	Why Do Companies Employ Prohibited Unethical Artificial Intelligence Practices?	M. Méndez-Suárez; M. d. l. M. de Obesso; O. C. Márquez; C. M. Palacios	2024
EP32	Securing Personally	I. Makhdoom; M. Abolhasan; J.	2024

	Identifiable Information: A Survey of SOTA Techniques, and a Way Forward	Lipman; N. Shariati; D. Franklin; M. Piccardi	
EP33	Privacy and Security Concerns in Generative AI: A Comprehensive Survey	A. Golda; K. Mekonen; A. Pandey; A. Singh; V. Hassija; V. Chamola; B. Sikdar	2024
EP34	The Ethics of AI in Games	D. Melhart; J. Togelius; B. Mikkelsen; C. Holmgård; G. N. Yannakakis	2024

EP35	Designing and Evaluating an Interactive Learning Technology to Foster Privacy Literacy	J. Doria; P. Grimm; M. Hohendanner; S. Kuhnert	2024
EP36	Privacy and Copyright Protection in Generative AI: A Lifecycle Perspective	D. Zhang; B. Xia; Y. Liu; X. Xu; T. Hoang; Z. Xing; M. Staples; Q. Lu; L. Zhu	2024
EP37	A Qualitative Analysis Framework for mHealth Privacy Practices	T. Cory; W. Rieder; T. -M. Huynh	2024
EP38	Resolving Ethics Trade-offs in Implementing Responsible AI	C. Sanderson; E. Schleiger; D. Douglas; P. Kuhnert; Q. Lu	2024
EP39	Explainable Artificial Intelligence Model for Predictive Maintenance in	M. Kisten; A. E. -S. Ezugwu; M. O. Olusanya	2024
	Smart Agricultural Facilities		
EP40	Privacy protection strategies in mobile crowdsensing from the framework perspective	X. Han; X. Niu; L. Chen; S. Qin	2024

EP41	Theoretical Framework of Digital Ethics Concerns for Public Services: Electronic Voting Use Case	N. Andreasyan; D. Buson; J. Rüst; E. Portmann; L. Terán	2024
EP42	Security Considerations in AI-Robotics: A Survey of Current Methods, Challenges, and Opportunities	S. Neupane; S. Mitra; I. A. Fernandez; S. Saha; S. Mittal; J. Chen; N. Pillai; S. Rahimi	2024

Tabela 6: Lista final de estudos primários selecionados.

3.7 Ameaças à Validade

Durante a construção das etapas da pesquisa, alguns pontos podem ser uma ameaça à validade da pesquisa, de acordo com os vieses definidos por Kitchenham e Charters (2007).

No processo da revisão sistemática, o viés de seleção se manifestou de duas formas: algumas bibliotecas digitais não aceitam strings de busca grandes, que conseguem abordar todo o campo de estudo requerido. Analogamente, a concentração de pesquisa em poucas áreas da sociedade relacionadas a proteção de dados de usuários na era da inteligência artificial, limitando a diversidade dos resultados. Para contornar esses pontos, foi feita a síntese da string de busca com as palavras chaves mais utilizadas, retiradas das questões de pesquisa. Além disso, a delimitação de tempo para filtro dos estudos colabora para que a investigação seja relevante, unindo os estudos mais atuais após a promulgação das principais legislações de proteção de dados. Outro ponto importante foi a facilidade de coleta dos estudos nas bibliotecas digitais, a ACM mostrou-se engessada no processo, tendo todos os estudos após o filtro descartados, podendo impactar no viés da pesquisa.

Por ser um tema em constante evolução, o viés de medição é identificado, principalmente depois da popularização das inteligências artificiais generativas, os estudos podem ficar

ultrapassados ou incompletos em um futuro próximo. Como estratégia de mitigação, é entendível que uma futura mudança na string de busca e especificidade dos temas centrais de pesquisa favoreceria a adaptação do estudo ao longo do tempo.

4 Resultados

A seleção dos artigos resultou em 42 artigos aderentes a string de busca e aos critérios de qualidade. A aplicação dos critérios de exclusão pôde eliminar boa parte dos estudos que não tinham relação direta com a temática e proporcionou uma lista de estudos relevantes para a resposta das questões de pesquisa. A análise também evidenciou que a maioria dos artigos selecionados foram publicados no ano de 2024, seguido pelo ano de 2023. Esses dados sugerem que a temática encontra-se em expansão, expressando uma crescente conscientização sobre os impactos e os resultados relacionados ao tema. A Figura 2 apresenta a quantidade de estudos selecionados ao longo dos anos.

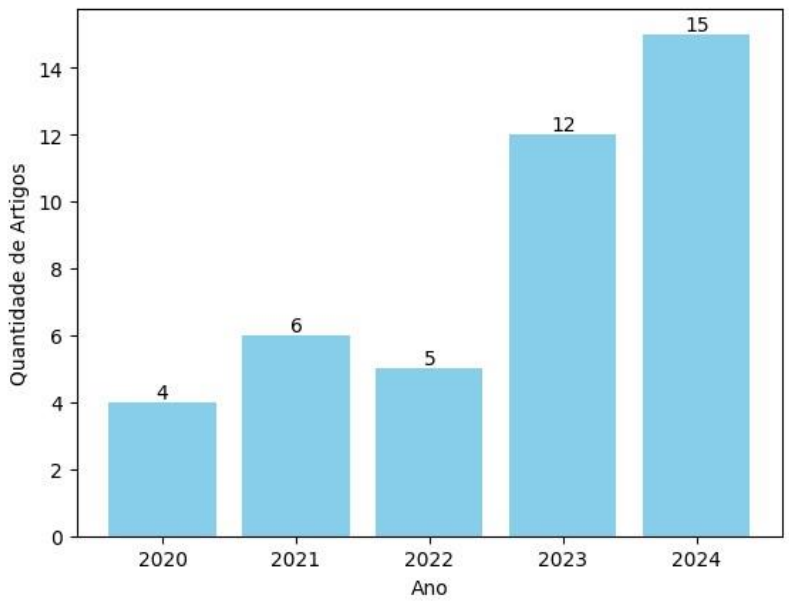

Figura 2: Distribuição de artigos por ano

Apesar da ACM ter começado com a maior quantidade de artigos, a IEEE mostrou ter os resultados mais relevantes após a aplicação dos filtros, com uma presença maior que 70% da lista de artigos, conforme a Figura 3.

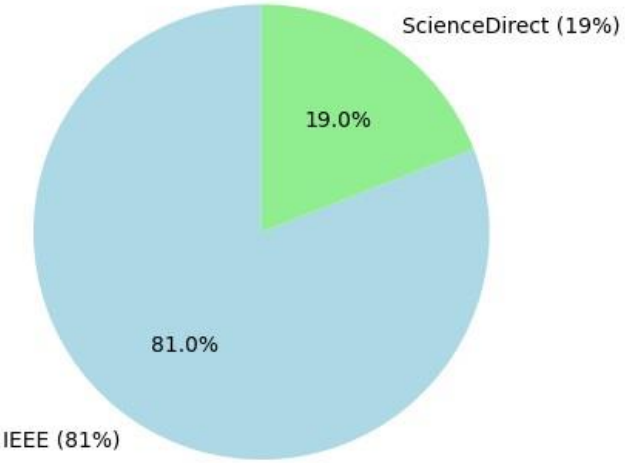

Figura 3: Percentual de artigos por base de dados

Fazendo uma análise dos títulos dos estudos selecionados, foi possível compreender uma tendência na presença em conjunto de duas palavras: Inteligência Artificial e Privacidade. A combinação dessas palavras demonstra a orientação dos estudos com a revisão atual. Além disso, expressa que menos de 50% das citações estão relacionadas com os impasses e requisitos legais da privacidade dos usuários, corroborando com a importância de revisões da literatura para mostrar as inovações na área e apresentar novas perspectivas.

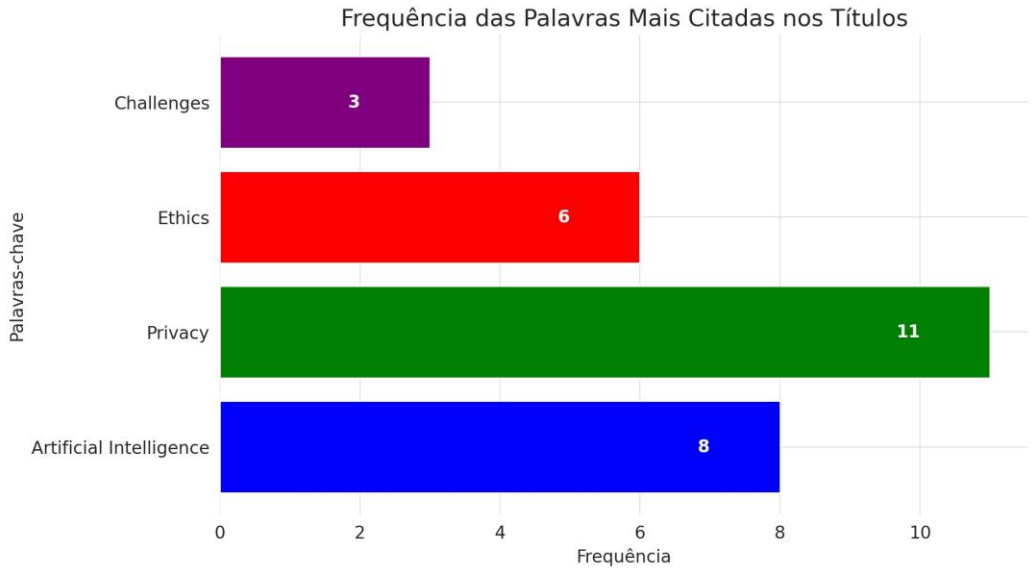

Figura 4: Palavras mais citadas nos títulos dos artigos.

QP1 Quais as implicações legais para o não cumprimento das boas práticas de proteção de dados?

A crescente importância da Inteligência Artificial (AI) e do tratamento de dados pessoais em diversos setores torna crucial a discussão sobre as implicações legais para as organizações que negligenciam as boas práticas legais. O não cumprimento dessas práticas pode acarretar em uma série de consequências legais que variam dependendo da legislação e do contexto que ocorreu a infração. A análise da literatura selecionada pode revelar um panorama abrangente e complexo, mostrando a presença dessa preocupação em algumas áreas com contextos sensíveis, como a saúde digital, a governança e a criação de sistemas digitais.

Um dos marcos regulatórios centrais que estiveram presentes nos estudos, é o Regulamento Geral de Proteção de Dados (GDPR), referenciado por estudos como os [EP16], [EP31], [EP08], [EP11], [EP12], . O não cumprimento do GDPR pode acarretar sanções financeiras substanciais, chegando a multas de até 20 milhões de euros ou até 4% do faturamento global anual das empresas infratoras, dependendo da gravidade da violação. Além disso, legislações nacionais e regionais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e leis específicas em países como o Argentina e Equador, também estabelecem requisitos rigorosos para o tratamento de dados pessoais, especialmente em contextos com dados sensíveis.

O estudo de [EP37], no setor da saúde, mostrou que com o crescimento das aplicações móveis (mHealth) e sistemas baseados em IA, surgem implicações legais significativas relacionadas à proteção de informações pessoalmente identificáveis (PII) e informações protegidas de saúde (PHI). O compartilhamento inadequado desses dados para terceiros sem consentimento explícito ou sem base legal válida, configura violação direta das leis aplicáveis. Além disso, divergências entre práticas declaradas nas políticas de privacidade e as práticas efetivamente observadas nos aplicativos configuram violações adicionais por falta de transparência adequada.

O direito à informação e à transparência são princípios do GDPR que destacam-se por impor várias obrigações legais críticas que visam garantir a proteção dos titulares de dados. Esses direitos exigem que os indivíduos sejam claramente informados sobre como seus dados são processados, sendo que a ausência dessa transparência pode levar a questionamentos legais. Apesar de debates sobre sua natureza explícita no GDPR, o direito à explicação impõe a obrigação de fornecer informações significativas sobre a lógica envolvida em decisões automatizadas, cuja falta pode acarretar responsabilizações legais. Além disso, o GDPR assegura o direito à contestação, permitindo que os indivíduos questionem decisões automatizadas; a ausência de mecanismos eficazes para isso pode gerar implicações jurídicas. Outro princípio essencial é o direito à não discriminação, que proíbe o uso enviesado ou discriminatório de dados pessoais, sendo que sistemas algorítmicos que não mitigam vieses podem resultar em sanções legais. Por fim, operações de alto risco devem realizar Avaliações de Impacto à Proteção de Dados (DPIA) adequadas, sendo que a não realização ou execução inadequada dessas avaliações implica responsabilidade legal. Esses princípios são fundamentais para garantir que as práticas de tratamento de dados estejam alinhadas às exigências regulatórias e aos direitos dos indivíduos.

A literatura [EP17], [EP11] ainda aponta desafios no contexto tecnológico. A implementação e o uso de sistemas com IA envolvida, levantam questões especialmente no quesito proteção de dados e governança. O princípio da responsabilidade no GDPR exige que os controladores de dados demonstrem que implementaram medidas eficazes para proteger os dados pessoais. A incapacidade de demonstrar a adesão a boas práticas de proteção de dados em sistemas de IA pode levar à responsabilização legal em caso de incidentes de segurança ou privacidade.

A falta de capacidade de detecção e mitigação de vieses em sistemas de Inteligência Artificial (IA) pode resultar em implicações legais significativas, especialmente por violar princípios fundamentais como justiça e não discriminação, conforme destacado por [EP23]. Esses problemas são agravados quando os modelos de IA são treinados com dados enviesados, o que pode levar a decisões discriminatórias, particularmente em contextos que envolvem atributos sensíveis [EP31]. Assim, o cuidado no treinamento dos modelos é essencial para evitar que sistemas baseados em IA reforcem desigualdades ou violem regulamentações de proteção de dados.

Em sistemas autônomos, como veículos autônomos ou sistemas inteligentes de vigilância, a modelagem adequada das ameaças à privacidade é essencial para garantir a conformidade regulatória [EP17]. Nesse contexto específico, baseado em sete princípios fundamentais, como "Privacidade como Configuração Padrão" e "Privacidade Incorporada ao Design", o framework Privacy By Design busca minimizar riscos ao priorizar a coleta mínima de dados, o uso de pseudonimização e anonimização, e a implementação de tecnologias que garantam segurança ao longo do ciclo de vida dos dados. No contexto da IA, esses princípios são cruciais para garantir conformidade com regulamentações como o GDPR e para fortalecer a confiança dos usuários nos sistemas autônomos. Por exemplo, técnicas como criptografia e privacidade diferencial podem ser incorporadas desde as fases iniciais do desenvolvimento para evitar violações de dados pessoais. Assim, o framework não apenas promove conformidade legal, mas também contribui para a criação de sistemas mais éticos e centrados no usuário.

No âmbito acadêmico, a forma como os dados são coletados, processados e utilizados para pesquisa e desenvolvimento de IA também possui implicações significativas. [EP18], [EP16] e [EP39] abordaram pontos importantes sobre anonimização, consentimento e segurança, princípios e técnica abordados como base nas legislações de privacidade mais famosas. As leis de proteção de dados frequentemente exigem os cuidados com: anonimização de dados ou pseudonimização - que são técnicas para desassociar um indivíduo de um dado -, consentimento informado e específico dos titulares para a coleta dos seus dados, garantia de acesso não autorizado ou vazamentos, se houver a transferência internacional de dados, as adequações aos requisitos de transferência devem ser seguidas. Nesse contexto, foi possível elencar, abaixo, os principais pontos de falha que podem levar a uma medida jurídica ou legal.

1. Falha ou não aplicação de métodos eficazes de anonimização
2. Ausência de consentimento válido
3. Ausência de medidas técnicas de segurança para proteção dos dados
4. A não adequação ou cumprimento com as medidas específicas quando existe a transferência internacional de dados.

De acordo com [EP30], diversas organizações internacionais (EU, UNESCO, IEEE, ISO) estão desenvolvendo frameworks e diretrizes para a governança ética da IA, com foco na proteção dos direitos fundamentais e valores humanos. Esses marcos regulatórios buscam estabelecer diretrizes claras para garantir que os sistemas baseados em IA sejam desenvolvidos e implementados com responsabilidade ética e jurídica. Ponto favorável para a evolução e criação de entidades que acompanhem o cumprimento legal do direito constitucional dos indivíduos.

Por fim, a negligência das obrigações legais relacionadas à proteção de dados não apenas resulta em sanções financeiras significativas como também gera danos reputacionais às organizações e perda da confiança pública nos sistemas tecnológicos implementados. A complexidade dessas implicações exige uma compreensão aprofundada das leis de proteção de dados aplicáveis e a implementação de práticas robustas para garantir a conformidade em todas as fases do ciclo de vida do tratamento de dados.

QP2 Quais as principais consequências da falta de transparência sobre como as IAs utilizam dados pessoais?

O objetivo desse tópico é elucidar as principais consequências negativas (dores) para os indivíduos, atreladas a falta de transparência na coleta, processamento e utilização de dados pessoais por sistemas de IA.

Como usuários, os indivíduos que utilizam sistemas inteligentes ou que têm dados pessoais compartilhados com algum sistema baseado em IA, podem ter dificuldade de entender que existem possíveis riscos associados nessa prática. Para dar luz a essas dores, foi possível identificar nos estudos os principais pontos de relevância.

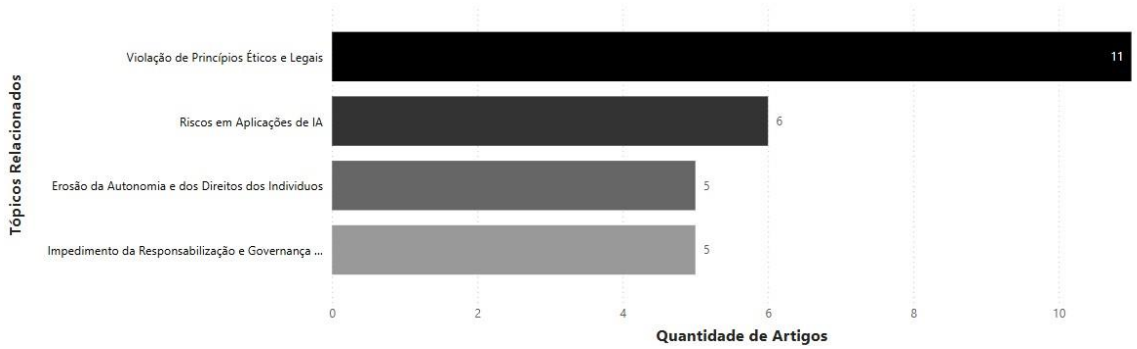

Figura 5: Quantidade de Estudos que Citam as Consequências

Falando de responsabilidade, focada nos controladores, primeiramente, destaca-se a violação direta dos princípios fundamentais estabelecidos por legislações de privacidade, que enfatizam licitude, lealdade e transparência no tratamento dos dados pessoais. Quando os usuários não conseguem compreender adequadamente como seus dados são utilizados, ficam impossibilitados de exercer plenamente seus direitos ou fornecer consentimento informado [EP08] e [EP13]. Direitos como acesso aos dados pessoais, exclusão ou oposição ao processamento tornam-se difíceis ou até impossíveis quando os usuários não dispõem das informações necessárias para identificar problemas ou solicitar correções adequadas.

Ao pensar na utilização de um sistema, é abstraída a responsabilidade dos usuários, principalmente em casos do serviço ser um SaaS. O criador ou fornecedor deve ter medidas técnicas, processuais e legais para garantir a proteção do serviço, imperando a confiança entre as duas partes envolvidas. No entanto, [EP18] discorre sobre como a opacidade dos sistemas de IA mina a confiança dos usuários. Quando os indivíduos não entendem como as decisões algorítmicas são tomadas com base em seus dados, torna-se difícil confiar na justiça e na equidade desses sistemas. Adicionalmente, a falta de transparência dificulta a accountability (responsabilização) dos controladores de dados e desenvolvedores de IA em caso de danos ou decisões injustas [EP07].

O direito à explicação abordado nos estudos de [EP07], [EP04] e [EP13] traz ênfase, também, a medidas que poderiam ser utilizadas a partir do momento que os usuários entendessem minimamente o risco ou a existência dele. O direito é implícito por legislações como a GDPR e existe uma crescente demanda por explicabilidade em sistemas de IA, refletindo a necessidade dos usuários compreenderem as razões acerca das decisões automatizadas que podem afetá-los. Esse impasse é presente em muitos

modelos complexos de IA, dificultando o provisionamento de informações significativas e, consequentemente, impede a capacidade dos usuários de contestar decisões consideradas injustas ou errôneas.

A opacidade algorítmica, do ponto de vista regulatório e técnico, cria barreiras significativas à auditoria independente e à supervisão regulatória eficaz. A ausência de mecanismos claros para auditoria independente limita a capacidade das autoridades regulatórias em detectar práticas inadequadas ou ilegais relacionadas ao tratamento dos dados pessoais por sistemas automatizados. É essencial que existam meios para validar o cumprimento das medidas prevista nas legislações, principalmente quando os usuários realizam uma Solicitação do Titular dos Dados, um direito garantido, reforçando que todo o contexto envolvido na falta de transparência pode ser prejudicial legalmente e ao princípio fundamental a liberdade dos indivíduos, elencado pela DUDH.

Finalmente, a falta de transparência também oculta riscos relacionados à segurança e privacidade dos dados pessoais utilizados pelas IAs. Sem informações claras sobre práticas adotadas para garantir segurança e proteção desses dados durante todo o ciclo operacional (coleta, armazenamento, processamento), vulnerabilidades ocultas podem aumentar as chances de incidentes envolvendo vazamentos ou acessos não autorizados.

Em suma, a ausência ou insuficiência da transparência no uso da inteligência artificial para tratamento de dados pessoais gera consequências negativas profundas e/ou desconhecidas para os usuários: desde violações éticas fundamentais, manipulação indevida, perda da autonomia individual e aumento significativo da exposição a riscos cibernéticos.

QP3 Quais são as principais medidas tomadas para garantir a privacidade no uso da IA?

A garantia da privacidade no uso das IAs é um desafio que abrange desde a utilização, concepção, implementação e monitoramento contínuo de sistemas. A dependência crescente por dados para treinar e operar modelos, e pela inserção de dados por usuários em sistemas, aumenta as preocupações sobre violações de dados.

Os estudos analisados contribuíram com várias abordagens, que foram agrupadas pela quantidade de incidência na Tabela 7.

Tópico de referência	Número de artigos que citam	Porcentagem do total
Regulamentações de Proteção de Dados	10	29%
Técnicas de Preservação de Privacidade	14	40%
Avaliação de Risco e Modelagem de Ameaças	5	14%
Transparência e Explicabilidade	6	17%
Privacidade por Design	3	9%
Segurança em IA	7	20%

Tabela 7: Quantidade de Tópicos de Referência Abordados Pelos Estudos Selecionados

- Regulamentações de Proteção de Dados: Refere-se à menção de leis e regulamentos como o GDPR, CCPA, PIPEDA e outras legislações que visam proteger os dados pessoais. Inclui também discussões sobre conformidade e não conformidade com tais regulamentos [EP18], [EP32], [EP22].

- Técnicas de Preservação de Privacidade: Abrange métodos técnicos utilizados para proteger a privacidade dos dados, como Differential Privacy (DP), Federated Learning (FL), Homomorphic Encryption (HE), Secure Multiparty Computation (SMC), Anonimização, Pseudonimização, e Minimização de Dados [EP16], [EP42], [EP33], [EP17].

- Avaliação de Risco de Privacidade e Modelagem de Ameaças: Inclui a identificação, análise e mitigação de riscos de privacidade no desenvolvimento de IA. Isso envolve o uso de frameworks como STRIDE, LINDDUN, Avaliações de Impacto à Privacidade (DPIA), e modelagem de ameaças em geral [EP17], [EP13], [EP32].

- Transparência e Explicabilidade: Refere-se à necessidade de tornar os sistemas de IA compreensíveis e de fornecer informações sobre como os dados são usados e as decisões são tomadas [EP08], [EP13], [EP01].
- Privacidade por Design: Envolve a integração de considerações de privacidade desde as fases iniciais do projeto e desenvolvimento de sistemas de IA [EP18], [EP40].
- Segurança em IA: Abrange medidas e técnicas para proteger os dados e sistemas de IA contra acesso não autorizado, violações e outras ameaças à segurança [EP19], [EP16], [EP22], [EP18], [EP21].

Nota-se a presença de dois temas centrais, corroborando com o que foi abordado nos outros tópicos da pesquisa, a tendência dos estudos em regulamentações e medidas técnicas para proteger o dado utilizado em inteligências artificiais em sua forma bruta. Juntos, esses temas estão presentes na maioria dos estudos da seleção final de artigos.

Primeiramente, falando sobre os riscos que podem ter mitigados com requisitos técnicos, o aprendizado federado surge como uma técnica promissora, com sua relevância principalmente em sistemas de saúde, permitindo que várias organizações trabalhem no treinamento de um modelo de IA global sem a necessidade de centralizar dados sensíveis [EP06] e [EP16]. Esse ponto aborda a necessidade de melhorar os sistemas, sem tirar a obrigação legal com o cuidado com os dados pessoais sensíveis, evitando o compartilhamento e a utilização em treinamentos.

[EP40] abordou algumas tecnologias, como a privacidade diferencial, que adicionam ruído aos dados para limitar a capacidade de identificar indivíduos, mantendo a utilidade dos dados para análise. A computação multipartidária segura permite que várias partes computem conjuntamente uma função sobre seus dados privados sem revelar as entradas umas às outras. Outras técnicas como anonimização e pseudonimização buscam remover ou mascarar informações que poderiam identificar um indivíduo, respeitando o princípio da minimização de dados, previsto no GDPR, que enfatiza a coleta dos dados estritamente necessários para um propósito específico.

Os estudos de [EP32], [EP35], [EP18] abordaram a importância de incorporar princípios de Privacy by Design desde as fases iniciais do desenvolvimento de sistemas de IA. Isso

significa considerar a privacidade não como um adendo, mas como um requisito fundamental, integrando mecanismos de proteção em toda a arquitetura do sistema. Por exemplo, o uso de metadados para rastrear o acesso, a utilização e o armazenamento de dados pode aumentar a integridade e a transparência. A ideia de "contestabilidade por design" em sistemas de tomada de decisão automatizada (ADM) permite que usuários especializados questionem e analisem o funcionamento dos algoritmos, promovendo a transparência [EP11].

Citando os marcos regulatórios, além de enfatizar a necessidade de cumprir com os princípios que compõem as leis, as organizações precisam implementar medidas apropriadas para identificar e mitigar riscos com antecedência, como a Avaliação de Impacto a Proteção de Dados (DPIA).

Fazendo uma junção dos estudos de [EP39] e [EP28] foi possível entender que a Inteligência Artificial Explicável (XAI) visa tornar os modelos de IA mais compreensíveis para humanos, abordando a "caixa preta" de muitos algoritmos de aprendizado de máquina. Diferentes tipos de explicações podem ser necessárias para diferentes partes interessadas, como desenvolvedores, profissionais de saúde e pacientes. A transparência pode ser alcançada através de modelos intrinsecamente interpretáveis ou por meio de técnicas pós-hoc que fornecem explicações para modelos complexos [EP13]. A criação de "FactSheets" para sistemas de IA, contendo informações relevantes sobre os dados, o modelo e o uso pretendido, pode aumentar a transparência [EP18].

[EP17] faz alusão a um framework de identificação e mitigação de ameaças à privacidade dentro do ciclo de vida da IA. Técnicas de modelagem de ameaças, como o LINDDUN, ajudam a identificar vulnerabilidades relacionadas à linkabilidade, identificabilidade, não repúdio, detectabilidade e divulgação de informações. Em sistemas autônomos, como veículos conectados, a modelagem de ameaças à privacidade apresenta desafios adicionais devido à complexidade das arquiteturas e à confidencialidade de certas informações. A utilização de frameworks como tema da avaliação de riscos e modelagem de ameaças corrobora com a concepção de um produto robusto e que respeita os princípios legais, é mais adaptável a mudanças e menos suscetível a violações de dados.

5 Conclusão e Trabalhos Futuros

O presente estudo buscou entender os principais pontos abordados pela literatura na perspectiva de que privacidade no uso de inteligência artificial é um tema essencial e necessita de pesquisa sobre o seu impacto nessa área. Alguns estudos destacam-se por refletir sobre a confiança dos usuários no uso das IAs, [EP18]. A criação das regulamentações, novas em comparação com a maioria das leis, quase que prediz a expansão dos sistemas baseados em IA, sendo ponto importante para a garantia do direito dos indivíduos. No entanto, [EP37], [EP31] e [EP23], discorrem sobre a presença das implicações, mas a popularização do não cumprimento das necessidades legais vai em contrapartida com as necessidades apontadas pelos estudos. Os resultados mostraram que a falta de conformidade com boas práticas acarretam, principalmente, em multas de valores significativos, sanções administrativas, congelamento de atividades de tratamento de dados e má reputação da marca.

Por outro lado, foram identificadas medidas eficazes para mitigar esses desafios. Primeiramente, citando a questão cultural, os estudos falam sobre tornar a preocupação com as implicações legais e de transparência dos sistemas fator presente desde as fases iniciais da sua concepção. Para apoiar essa iniciativa, [EP13], [EP17], [EP33] e [EP40] citam a utilização de medidas como as técnicas de anonimização, aprendizado federado e Privacy by Design para mitigação de riscos. Além disso, a criação de frameworks como o LINDDUN, destacaram-se como ferramentas úteis para modelar ameaças à privacidade ao longo do ciclo de vida da IA, permitindo identificar vulnerabilidades relacionadas à identificabilidade e divulgação indevida de informações. Esses pontos reforçam a visão de que privacidade e proteção de dados são aspectos que devem ter sua importância discutida em todas as fases de criação de um sistema de Inteligência Artificial. Pensando em uma maior adequação com os princípios da transparência, minimização e responsabilidade, a adoção aos cuidados citados contribui na construção de uma documentação que favorece esses princípios.

Urge, portanto, que as pesquisas sobre os aspectos éticos na utilização dos sistemas de IA, principalmente aqueles que recebem dados pessoais ou que são treinados com bases de dados pessoais, continuem com sua expansão. Que haja uma atenção especial na criação de novos modelos que utilizem privacy by design na sua construção e que respeitem os

princípios de transparência, minimização e anonimização, fazendo com que essa preocupação abordada nos estudos seja amenizada. Como futuro do estudo, a adição de mais bibliotecas digitais pode agrupar novas categorias de impasses e medidas tomadas atualmente, além de ter um escopo maior para questionar sobre quais ações de auditoria são utilizadas e viram notícia mundo afora.

6 Referências

Charmet, F., Tanuwidjaja, H.C., Ayoubi, S. et al. Explainable artificial intelligence for cybersecurity: a literature survey. Ann. Telecommun. 77, 789–812 (2022). https://doi.org/10.1007/s12243-022-00926-7.

Kitchenham, B. and Charters, S. (2007). "Guidelines for performing Systematic Literature Reviews in Software Engineering". EBSE Technical Report, EBSE-2007-01. Disponível em: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

MORGULIS, Rafael. Privacidade da Informação: Uma Abordagem Moderna. São Paulo: Editora Digital, 2023.

PECK, Patricia. Proteção de Dados Pessoais: Comentários à Lei 13.709/2018. 3. ed. São Paulo: Saraiva, 2022.

SOLOVE, Daniel J. A taxonomy of privacy. University of Pennsylvania Law Review, v. 154, n. 3, p. 477-560, 2006. DOI: https://doi.org/10.2307/40041279.

WESTIN, Alan F. Privacy and Freedom. New York: Atheneum, 1967.