
Proteção da Propriedade Intelectual: Uma revisão da segurança dos dados digitais e seus desafios

Protection of Intellectual Property: A review of digital data security and its challenges

José dos Santos Machado^{1*}, Francisco Sandro Rodrigues Holanda², Luiz Diego Vidal Santos², Arilmara Abade Bandeira¹, Aduino Cavalcante Menezes³, Toniclay Andrade Nogueira¹

RESUMO

Considerando que inovações tecnológicas e científicas estão sendo adotadas para a segurança dos dados armazenados digitalmente e que, assim como os demais dados os ativos de Proteção da Propriedade Intelectual (PPI) também requerem proteção, o presente estudo teve por objetivo identificar e analisar quais medidas e soluções estão sendo tomadas para a segurança dos dados armazenados por meio digital, no sentido de garantir a Proteção da Propriedade Intelectual (PPI) e os seus desafios futuros. Foi realizada uma revisão *Scoping Review*, usando critérios do *Cochrane Systematic Reviews* associados ao PRISMA, na base Scopus. Foram identificados 400 registros, usando os descritores: *data security*, *digital data*, *digital security*, *intellectual property*. Por meio dos métodos de seleção e classificação foram analisados 26 artigos. Os resultados sinalizam que os desafios mais relevantes para a PPI voltados à segurança dos dados digitais foram: desenvolvimento e disponibilidades de serviços de armazenamento na *Cloud Computing* exclusivo para a PPI, uso da Inteligência Artificial para a segurança de dados digitais, adesão a métodos de criptografias de dados e adoção de uma política de *cybersecurity*.

Palavras-chave: Armazenamento digital; Proteção de dados; Segurança cibernética; Segurança de rede.

ABSTRACT

Considering that technological and scientific innovations are being adopted for the security of stored data like other digital data and that, as well as the Protection of Intellectual Property (PIP) they also require protection, the present study aimed to identify and analyze the measures As solutions are being taken for the security of data stored by digital means, in order to guarantee the Protection of Intellectual Property (PIP) and its future challenges. A Scoping Review was performed, using criteria from the Cochrane Systematic Reviews associated with PRISMA, in the Scopus database. 400 records were identified, using the descriptors: *data security*, *digital data*, *digital security*, *intellectual property*. Through selection and classification methods, 26 articles were analyzed. The most relevant signs for digital data protection are Intellectual Property challenges unique to digital data protection (PIP use of Artificial Intelligence for digital data security), adherence to data encryption and adoption of a cyber security policy.

Keywords: Digital storage; Data protection; Cybersecurity; Network security.

¹ Instituto Federal de Sergipe - IFS

* E-mail: jsmac18@hotmail.com

² Universidade Federal de Sergipe - UFS

³ Instituto Federal do Amapá - IFAP

INTRODUÇÃO

Com o vigoroso desenvolvimento do *big data* e da inteligência artificial, a Proteção da Propriedade Intelectual (PPI) é parte essencial do atual desenvolvimento científico e tecnológico, e assim os dados relacionados à Propriedade Intelectual (PI) crescem em progressão geométrica (WANG, 2021), portanto, a demanda por espaço de armazenamento de dados da PI também está aumentando a cada dia. No entanto, essa tecnologia também pode ser explorada e levar a problemas de segurança, como crimes físicos e digitais. Infelizmente, as violações de segurança estão aumentando em complexidade e frequência, tornando as contramedidas atuais insuficientes para evitá-las (YU; KIM; KIM, 2021).

Propriedade Intelectual (PI) pode ser compreendida como o direito de pessoa, física ou jurídica, sobre um bem incorpóreo móvel (ARAÚJO, 2010). Assim, a propriedade intelectual corresponde ao direito sobre criações intelectuais, por determinado período, estabelecido segundo os preceitos legais (SINGH; SETHI, 2021).

As criações do intelecto humano são protegidas pela Propriedade Intelectual (YULIANI; ROSIYADI, 2016). Nesse sentido, o principal objetivo da PI é preservar os interesses dos criadores intelectuais, fornecendo-lhes um conjunto relevante de direitos para proteger a exploração de suas criações. Propriedade Intelectual é uma locução ampla que abrange tanto o direito autoral quanto à propriedade industrial (BARATÈ, 2015). Os direitos autorais incluem obras literárias e artísticas, como filmes, poemas e obras musicais, enquanto a propriedade industrial considera invenções (patentes), marcas, desenhos industriais e indicações geográficas de origem (SUN, 2020). O direito autoral nasceu como um “direito de cópia” e tem sua origem pela possibilidade de reprodução e pela necessidade de regular o exercício desse direito (HOU, 2018).

A Propriedade Intelectual (PI) está protegida por um conjunto de normas jurídicas que garantem que uma obra, criação ou invenção pertence exclusivamente aos seus criadores (BARBOSA 2013). É nesse sentido, que a utilização intensiva da ciência, tecnologia e inovação numa economia, conforme evidencia a literatura, permite a elevação da capacidade de competir, criando empreendimentos, empresas, empregos e marcas comerciais (MATIAS-PEREIRA, 2011).

Como incentivo à inovação tecnológica e para colher os benefícios do investimento, é essencial possuir proteção dos dados à Propriedade Intelectual em todas as inovações (SINGH; SETHI, 2021), porém, no rápido desenvolvimento da

disseminação de informações em rede atualmente, cada vez mais atos de violação de direitos de PI têm sido realizados por meio da internet (XU, 2012).

A proteção de inovações e informações comerciais pode ser definida como um sistema de medidas legais, econômicas, organizacionais e técnicas que proporcionam segurança da informação das inovações (MINGALEVA e MIRSKIKH, 2018). A política de informação proporciona o uso racional de informações confidenciais e segurança econômica. Existem diferentes ameaças de uso indevido de informações, como internas ou externas, ativas e passivas, intencionais e não intencionais (MACHADO, 2014). Com o rápido desenvolvimento da tecnologia da informação, o design de informações de marca d'água para proteger a Propriedade Intelectual de mídia digital e a segurança da informação está se tornando cada vez mais significativo (SHUGU, 2017).

Existem inúmeros desafios no campo da segurança digital, incluindo replicação de dados, consistência, escalabilidade limitada, falta de confiabilidade, disponibilidade não confiável de recursos de nuvem, portabilidade devido à falta de padrão de provedor de nuvem, segurança e privacidade (SU, 2017). Privacidade refere-se a informações pessoais que uma pessoa não gostaria que outras pessoas soubessem sem autorização e ao direito de uma pessoa estar livre da atenção de outros - Declaração dos Direitos Humanos da ONU, 1948, (ARUMUGAM; SULEKHA, 2016).

O desenvolvimento da Internet tornou o problema da cópia não autorizada e dos dados distribuídos potencialmente devastadores para os direitos de Propriedade Intelectual (TSAI, 2013). Várias soluções foram propostas para lidar com Trojans em nível de design, com vários níveis de cobertura, mas trabalhos anteriores não forneceram uma estrutura prática e integrada para a engenharia dessas soluções (WAKSMAN; SETHUMADHAVAN; EUM, 2013).

De acordo com Kumar, Juhi e Vikrama, (2019), na literatura, pesquisadores têm introduzido inúmeras técnicas que abordam a questão da modificação e reprodução ilegal de dados, e as técnicas de ocultação de informações são algumas delas. Segundo Arora et al. (2018), as técnicas de ocultação de informações podem ser categorizadas como: esteganografia, criptografia e marca d'água.

Conforme o estudo de Farrand (2018), é definida a Estratégia de Cibersegurança como às salvaguardas e ações que podem ser utilizadas para proteger o domínio cibernético, tanto no domínio civil como militar, das ameaças associadas ou que podem prejudicar a sua interdependência de redes e infraestrutura de informação. No campo da

cibersegurança, o combate ao cibercrime constitui uma área de atuação principal, complementando as ações de combate às atividades categorizadas como ciberespionagem e ciberguerra (PENNAFORTE; RAMOS, 2020). Mais do que nunca, a crescente quantidade de trocas de conteúdo digital exige técnicas eficientes e práticas para proteger os direitos de Propriedade Intelectual (URVOY, 2014).

Conforme evidenciado na literatura atual a Proteção da Propriedade Intelectual (PPI), através da segurança dos dados digitais no mundo conectado é de grande importância para economia e crescimento de um país, sendo um campo de pesquisa de enorme relevância para pesquisadores do mundo inteiro. Este trabalho teve como objetivo identificar e analisar quais medidas e soluções estão sendo tomadas para a segurança dos dados armazenados por meio digital, para garantir a Proteção da Propriedade Intelectual (PPI) e os seus desafios futuros.

MATERIAIS E MÉTODOS

A revisão de escopo (RE) em documentos acadêmicos pode atingir esse objetivo, já que é projetada para coletar evidências que atendam aos critérios de elegibilidade pré-especificados buscando a compreensão de lacunas existentes no assunto proposto (MUNN et al., 2018). Para identificar, avaliar e interpretar os resultados relevantes das revisões sistemáticas em trabalhos acadêmicos publicados, conforme os princípios das regras empíricas relacionadas aos levantamentos bibliométricos na literatura, atualmente são amplamente adotados e aceitos os procedimentos de classificação, descrição e qualificação de documentos que adotam princípios metodológicos, tais como as revisões do Cochrane (CHANDLER et al., 2021).

Neste artigo foram adaptadas as recomendações do *Cochrane Handbook for Systematic Reviews of Interventions* (HIGGINS et al., 2020), adotando como procedimentos deste estudo: formulação da pergunta e rodadas: (i) localização dos estudos (artigos), (ii) elegibilidade dos estudos, (iii) qualificação dos artigos e extração dos dados e (iv) síntese da revisão interpretação dos dados.

Os Dados foram dispostos no repositório de dados abertos OSF sob o DOI: [10.17605/OSF.IO/A9FNR](https://doi.org/10.17605/OSF.IO/A9FNR)

Para este estudo foi atribuído o seguinte questionamento: Quais inovações tecnológicas e científicas estão sendo adotadas, para a segurança dos dados armazenados digitalmente em relação à Proteção da Propriedade Intelectual (PPI).

Rodada 1: Extração dos estudos

Inicialmente foi realizada uma busca com descritores primários nas bases de dados Scopus. Os descritores foram trabalhados na língua inglesa vinculados por operadores booleanos, seguindo as regras descritas por Slamet et al., (2016), por meio de artigos publicados entre os anos de 2012 a 2022. O critério de inclusão e exclusão para esta rodada das recomendações aceitou apenas artigos completos, escritos na língua inglesa apresentando os descritores primários nos seguintes campos: título (*title*), resumo (*abstract*) e palavras-chave (*keywords*). Para a base Scopus foi utilizado a seguinte string de busca: (TITLE-ABS-KEY (*data security*) AND TITLE-ABS-KEY (*digital data*) AND TITLE-ABS-KEY (*digital security*) AND ALL (*intellectual property*)) PUBYEAR > 2011.

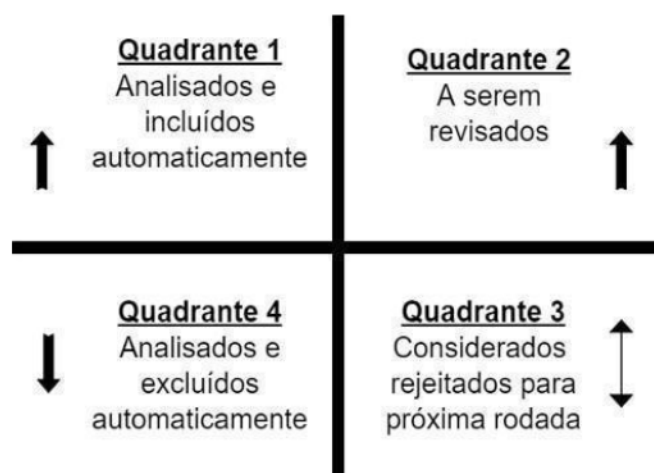
Rodada 2: Elegibilidade dos dados

Seleção automática

Pela possibilidade de se trabalhar com bancos de dados, a seleção inicial dos estudos foi realizada na sua primeira fase utilizando a busca por trabalhos duplicados a partir da seleção dos artigos únicos com o emprego do sistema StArt (LAPES, 2005). O método SCAS do sistema StArt foi adotado como classificador automático por pontuação, classificando os artigos utilizando duas fases. A primeira fase foi dividida em dois recursos, ou seja, por pontuação e por citação, e a segunda fase classificou nos seguintes quadrantes Q1 (3 pontos), Q2 (2 pontos), Q3 (1 ponto) e Q4 (0 pontos) (OCTAVIANO et al., 2015; OCTAVIANO et al., 2016). A Figura 1 apresenta os quadrantes adotados pelo Sistema.

Para completar a extração dos artigos classificados no Q2, foram lidos títulos, resumos e palavras-chave para verificação efetiva da inclusão ou exclusão.

Figura 1 – Quadrantes e categorias adotados no posicionamento hierárquico de pontos



Fonte: Santos et al., (2022)

Seleção manual dos artigos

Buscando mitigar possíveis artigos não relacionados ao tema proposto, foram selecionados os artigos que apresentaram valores maiores nos índices de inclusão quer para os índices de exclusão (Tabela 1) quanto para poder ser elegível na próxima rodada.

Tabela 1 – Critérios de Inclusão/Exclusão dos artigos observados

Critérios adotados	Grupo de Índices
Apresenta os dois descritores no título	Inclusão (I)
Periódico com Fator de impacto Internacional	Inclusão (I)
Correlação entre as duas áreas temáticas	Inclusão (I)
Não é trabalho sobre temas relacionados	Exclusão (E)
Não é trabalho sobre métodos inovadores	Exclusão (E)
Não apresenta solução inovadora	Exclusão (E)
Não apresenta possibilidade de replicação do experimento	Exclusão (E)
É uma revisão bibliográfica	Exclusão (E)
Pouca aderência aos descritores primários	Exclusão (E)

Fonte: Os autores (2022)

Os demais trabalhos foram considerados automaticamente inelegíveis para a próxima rodada. Todas as seleções nesta rodada foram realizadas por dois pesquisadores, independentemente, assim como restrita, de modo a evitar influência pessoal nos resultados. As discrepâncias observadas durante esta rodada foram resolvidas por consenso.

Rodada 3: Qualificação dos artigos e extração dos dados

Índice de qualidade dos artigos

Para classificação de qualidade dos artigos selecionados, foram adotados indicadores presentes na Tabela 2:

Tabela 2 — Indicadores adotados para descrição de qualidade dos artigos.

Siglas	Indicador	Grupo de Índice
DMS	Descreve o método/meios de segurança dos dados	Índices de qualidade
CSD	Apresenta a categoria da segurança dos dados digitais	Índices de qualidade
ACR	Apresenta capacidade de reprodução	Índices de qualidade
INV	Aparenta ser uma inovação	Índices de qualidade
TPI	Aplicação de uma tecnologia direcionada à proteção da PI	Índices de qualidade
DES	Apresenta descrição do procedimento metodológico	Índices de qualidade
TSD	Envolve tecnologia direcionada a área da segurança digital	Índices de qualidade

Fonte: Os autores (2022)

Foram atribuídos para cada indicador os valores: 0 para “não atende o indicador”, 0,5 “atende parcialmente o indicador” e 1 para “atende o indicador”, assim como os valores alcançados na classificação de prioridade (3 Muito alto, 2 Alto e 1 Baixo). Nesta fase foram excluídos os manuscritos que apresentavam grandes similaridades com os demais, e os que foram pontuados como prioridade baixa, mantendo o que apresentou maior pontuação dentre estes, assim como trabalhos que mantinham caráter de continuidade de uma pesquisa macro, pelos mesmos autores ou grupo de pesquisa.

Extração e síntese dos dados

A última rodada foi responsável pela classificação da qualidade dos trabalhos selecionados. Para identificar os artigos mais relevantes considerando as pontuações e classificações de toda a revisão, foi estabelecido um valor de corte correspondente a 85% do somatório dos critérios de classificação de escore por valor, obtidos na seleção dos estudos. O limite de 85% do somatório foi baseado no postulado de Pareto, afirma que, a maioria do efeito se origina de um pequeno número de causas (PARETO, 1964). No contexto desta pesquisa, este postulado afirma que os artigos com maior pontuação representarão a maior parte do reconhecimento científico no conjunto bibliográfico atual (AZEVEDO; ENSSLIN; JUNGLES, 2014).

Os dados a serem extraídos seguiram as seguintes classificações: classificação da atividade da segurança digital na Propriedade Intelectual (dados armazenados na computação em nuvem, dados governamentais, da indústria e pessoais) e a área de

estudo/pesquisa (segurança digital, inovações na segurança de dados, Proteção da Propriedade Intelectual).

RESULTADOS E DISCUSSÃO

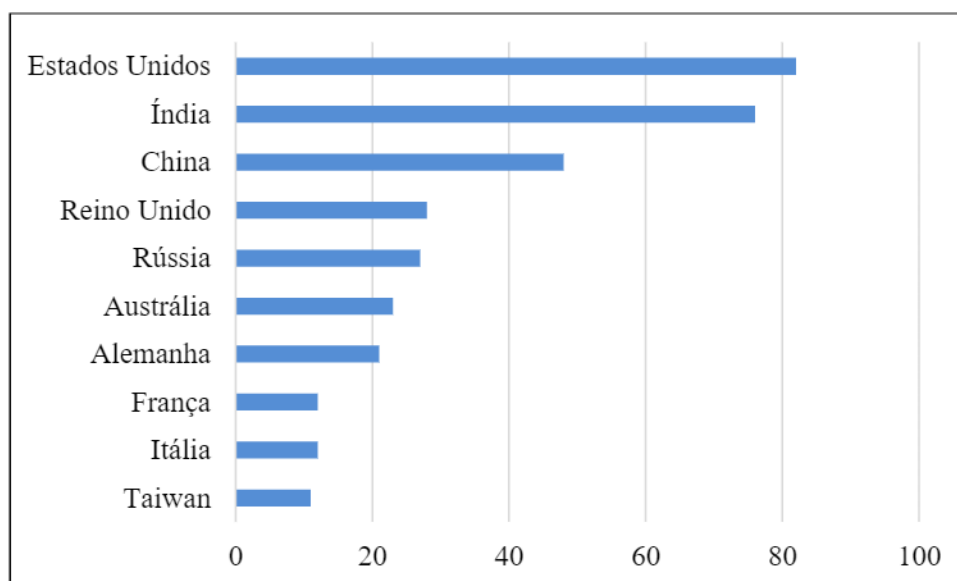
Inicialmente a busca na base de dados resultou em 400 artigos na Scopus, e destes estudos encontrados somente 2 artigos foram considerados duplicados e 4 arquivos eram notas explicativas de artigos já presentes, excluídos do corpus de artigos selecionados. Os artigos selecionados contam com 56 documentos escritos por apenas um autor e 344 em conjunto, índice de colaboração de 2,98. No corpo textual selecionado foram observados 883 autores apresentando uma média de 0,38 documentos por autores e 2,76 em coautoria com índice de colaboração de 2,95. Todos os artigos não duplicados minerados nos bancos de dados que emergiram utilizando os descritores de busca, foram inicialmente considerados elegíveis para avançar para a rodada 3, sendo a seleção dos estudos.

Bibliometria dos artigos selecionados

Observando as publicações identificadas no universo desta pesquisa a maioria dos artigos foi publicada em periódicos internacionais, sendo eles do tipo *Journal* (49,75%), *Conference Proceeding* (34,25%), *Book Series* (10,25%) e *Book* (5,75%). As principais fontes dos títulos foram; *IEEE Access* (3,25%), *ACM International Conference Proceedings Series* (3%) e *Advances in Intelligent Systems and Computing* (2,5%).

Analisando mais detalhadamente as palavras-chave mais citadas na base de dados da pesquisa realizada, foram destacadas: *Digital Storage* (81), *Security of Data* (79), *Cryptography* (61), *Digital Watermarking* (59) e *network security* (53). Foram também observados os países que mais publicaram sobre o tema, sendo que a maioria das publicações foram produzidas pelos Estados Unidos (20,5%), seguido de Índia (19%) e China (12%). A Figura 2 apresenta as publicações dos principais países identificadas nesta pesquisa.

Figura 2 – Publicações por país

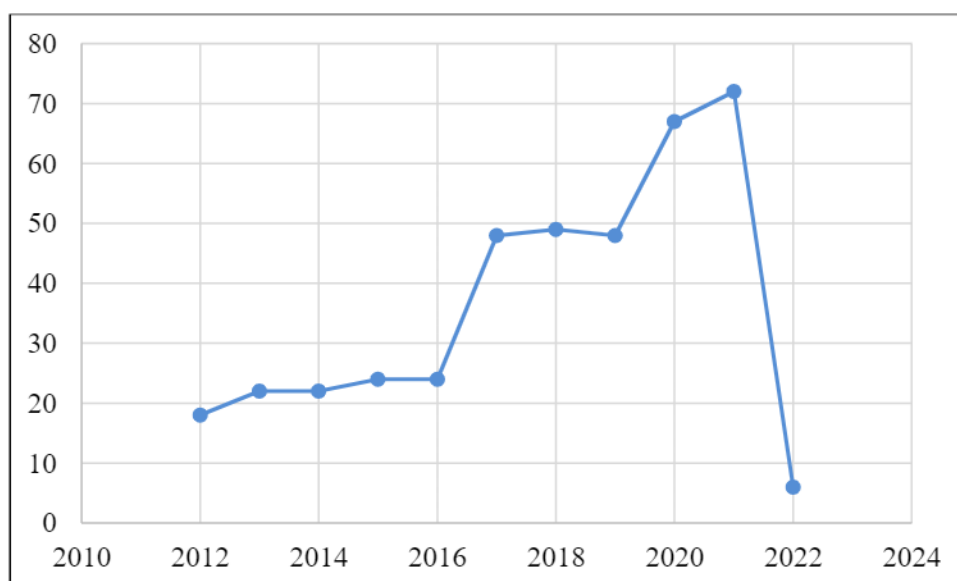


Fonte: Elaborado pelos autores, 2022

Outro fator importante a se observar são as publicações por ano, onde pode ser verificado um crescimento significativo de publicações relevantes ao tema (Figura 3), com destaque para o ano de 2012 com 18 publicações. Em 2021 foram registradas 72 publicações, apresentando um crescimento de 400%, demonstrando um significativo interesse por pesquisadores sobre o tema “segurança digital na PPT”.

A Figura 3 demonstra o crescimento das publicações no período pesquisado do ano de 2012 até a metade do mês de fevereiro do ano de 2022.

Figura 3 – Evolução das publicações por ano



Fonte: Elaborado pelos autores, 2022

Elegibilidade dos artigos

Seleção Automática de Citação e Pontuação

O sistema SCAS categorizou automaticamente 5 artigos no quadrante Q1, os quais foram aceitos automaticamente para a próxima rodada, que abordam majoritariamente métodos estratégicos ou inovações tecnológicas para segurança dos dados digitais, com ênfase na Proteção da Propriedade Intelectual voltada ao Governo ou instituição na área de inovação. Wang et al. (2021), propõem que com o desenvolvimento contínuo da computação em nuvem, a nuvem pode ser aplicada no gerenciamento de dados de Propriedade Intelectual.

Dos trabalhos categorizados no Q1, foi identificado que o principal artigo que atingiu 44 pontos pelo SCAS foi *Security-driven distributed platforms for intellectual property resource provision - a case study of TSITE IP* (Wang et al., 2021). Este trabalho apresenta uma estratégia de projeto para a Proteção da Propriedade Intelectual, com plataforma distribuída de serviço para segurança no armazenamento dos dados da Propriedade Intelectual e um modo de serviço de operação sob o contexto da era da informação em computação em nuvem. Para atender a esses requisitos para o desenvolvimento da plataforma operacional atual, os autores sinalizaram os seguintes desafios: A implementação da *Edge Computing*, para solucionar o problema do processamento e armazenamento dos dados na borda da rede; Engenharia do conhecimento para uma gestão de utilização da melhora e eficiência do recurso em todos os aspectos e *Cybersecurity* necessária para melhorar os recursos de monitoramento de segurança da plataforma. Igualmente contidos neste quadrante estão pesquisas que apresentaram ter como objetivo, analisar o status do legislativo da China e discute como manter a coordenação no futuro entre o fortalecimento das regras de aplicação da PI no ambiente digital e também a segurança de dados, apresentando recomendações específicas (XU, 2012). No trabalho de Singh et al., (2021), os autores apresentam uma pesquisa que visa estudar as questões de Propriedade Intelectual (PI) em relação à Inteligência Artificial (IA) em meio digital.

No Q3 e Q4 foram classificados 348 artigos e no quadrante Q4 313 artigos para classificação, sendo estes rejeitados para a próxima fase. Os artigos classificados no Q2 (47 artigos) que contavam com o escore de frequência de termos acima de 9 pontos foram conduzidos para seleção manual, buscando uma leitura mais aprofundada destes para

posterior pontuação, sendo aceitos 26 artigos do total. A Tabela 3 descreve mais detalhadamente a quantidade de artigos incluídos por critérios de maior relevância.

Tabela 3 – Quantidade de artigos incluídos por critérios de seleção

Crítérios adotados	Grupo de Índices	Q. de artigos
Apresenta os dois descritores no título	Inclusão (I)	8
Periódico com Fator de impacto Internacional	Inclusão (I)	6
Correlação entre as áreas temáticas	Inclusão (I)	7
Selecionado automaticamente pelo método SCAS	Inclusão (I)	5

Fonte: Os autores (2022)

Vários artigos foram excluídos, restando 26 artigos para as demais fases metodológicas deste estudo, visto que apresentavam pontuação relevante sobre a óptica de ocorrência dos descritores secundários no corpo textual e atenderam aos critérios propostos na fase de seleção. A Tabela 4 apresenta a quantidade de artigos excluídos por critérios de maior relevância.

Tabela 4 – Quantidade de artigos excluídos por critérios de seleção

Crítérios adotados	Grupo de Índices	Q. de artigos
Não é trabalho sobre temas relacionados	Exclusão (E)	6
Não apresenta os dois descritores no título	Exclusão (E)	3
Não apresenta solução inovadora	Exclusão (E)	4
Não apresenta possibilidade de replicação do experimento	Exclusão (E)	5
É uma revisão bibliográfica	Exclusão (E)	3
Pouca aderência aos descritores primários	Exclusão (E)	5
Selecionado pelo método SCAS	Exclusão (E)	348

Fonte: Os autores (2022)

Extração e síntese dos dados dos trabalhos selecionados

A partir das análises apresentadas anteriormente, partiu-se para uma síntese qualitativa mais minuciosa do material selecionado, sendo possível a classificação dos artigos por meio do somatório dos valores obtidos em todas as rodadas. A partir desse ponto foi realizado um corte correspondente a 85% do somatório de todos os critérios, sendo possível chegar a somente quatorze artigos, mas que expressam bem o perfil dos trabalhos que abordam a segurança dos dados digitais na Proteção da Propriedade Intelectual (PPI).

O presente estudo objetivou principalmente apresentar quais inovações tecnológicas e científicas estão sendo adotadas para a segurança dos dados armazenados digitalmente em relação à Proteção da Propriedade Intelectual (PPI) e seus desafios. A finalidade do objetivo proposto foi alcançada na análise dos artigos apresentados na Tabela 5.

Tabela 5 - Artigos com maior pontuação após somatório da síntese de qualidade

Pontuação	Título do artigo	Ano de publicação	Área de pesquisa	Inovação tecnológica
44	WANG, Yang. Security-driven distributed platforms for intellectual property resource provision-a case study of TSITE IP. Journal of Cloud Computing , v. 10, n. 1, p. 1-15.	2021	Cloud Computing	Serviços especializados para armazenamento visando PPI
33	XU, Xin. Coordination between the Intellectual Property Enforcement in the Digital Environment and the Data Security. In: 2012 Second International Conference on Business Computing and Global Informatization . IEEE, 2012. p. 804-807.	2012	Cloud Computing	Imposição de PPI no ambiente digital na segurança de dados
23	YU, Jin-Yong; KIM, Yujun; KIM, Young-Gab. Intelligent video data security: a survey and open challenges. IEEE Access , v. 9, p. 26948-26967.	2021	Vídeo Inteligente	Segurança inteligente de imagem de vídeo
19	SINGH, V. and SETHI, M.R. Digital Trade And Artificial Intelligence: Role Of Intellectual Property. NTUT Journal of Intellectual Property Law and Management , v. 10, p. 45-66.	2021	Inteligência Artificial (AI)	Segurança no comércio digital
17	ARORA, Shaifali M. et al. A DWT-SVD based robust digital watermarking for digital images. Procedia computer science , v. 132, p. 1441-1448.	2018	Imagem Digital	Técnica de <i>watermarking</i> para imagem digital
16	MINGALEVA, Zhanna; MIRSKIKH, Irina. The problems of digital economy development in Russia. In: The 2018 International Conference on Digital Science . Springer, Cham, 2018. p. 48-55.	2018	Economia Digital	Solução de problemas no desenvolvimento da economia digital
13	SU, Ziyi et al. Owner-stipulated data security and privacy for data accessing in Mobile Cloud context. In: 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICCT) . IEEE, 2017. p. 1-5.	2017	Mobile Cloud	Controle de nível de segurança e privacidade dos dados.

13	WAKSMAN, Adam; SETHUMADHAVAN, Simha; EUM, Julianna. Practical, lightweight secure inclusion of third-party intellectual property. IEEE Design & Test , v. 30, n. 2, p. 8-16.	2013	Hardware	Segurança em controlador de memória de chip
13	BARATÈ, Adriano et al. Managing intellectual property in a music fruition environment. IEEE MultiMedia , v. 23, n. 2, p. 84-94.	2015	Áudio Digital	Codificação conteúdos digitais
11	FARRAND, Benjamin. Combatting physical threats posed via digital means: the European Commission's developing approach to the sale of counterfeit goods on the Internet. European Politics and Society , v. 19, n. 3, p. 338-354.	2018	Impressão 3D	PPI no ambiente de impressão 3D
10	ARUMUGAM, G.; SULEKHA, V. Jane Varamani. IMR based anonymization for privacy preservation in data mining. In: Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society . 2016. p. 1-8.	2016	Mineração de Dados	Preservação da privacidade na mineração de dados
10	MISHRA, Kamta Nath. Aadhar based smartcard system for security management in South Asia. In: 2016 International Conference on Control, Computing, Communication and Materials (ICCCCM) . IEEE, 2016. p. 1-6.	2016	Biometria	Sistema de cartão inteligente
10	SUN, Wenyue et al. Blockchain and homomorphic encryption for digital copyright protection. In: 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom) . IEEE, 2020. p. 754-761.	2020	Criptografia	Uso de <i>blockchain</i> e criptografia homomórfica
10	BRANDMAN, Josh et al. A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems. Journal of Manufacturing Systems , v. 56, p. 202-212.	2020	Cybersecurity	Método para detectar ataques ciberfísicos

Fonte: Os autores (2022)

Conforme apresentado na Tabela 5 os principais desafios para a segurança dos dados na PPI nas instituições identificados foram:

- **Cloud Computing:** Desenvolvimento e disponibilidades de serviços de armazenamento de dados digitais na Cloud Computing exclusivo para a Proteção da Propriedade Intelectual (PPI).
- **Inteligência Artificial:** Uso da Inteligência Artificial para a segurança de dados digitais na detecção de ataques, invasões de sistemas e falsificação de marcas e produtos.
- **Criptografia:** Adesão a métodos de criptografias de dados para que se os dados digitais forem vazados o invasor não possa compreender sua leitura.
- **Cybersecurity:** Adoção de uma política de cybersecurity que esteja em uma constante atualização, pelo fato das medidas de segurança de hoje pode não servir em breve.

Nesta revisão de escopo evidenciamos que existem muitas publicações direcionadas para a proteção de dados digitais, porém, poucas apresentam ênfase exclusivamente para a Proteção da Propriedade Intelectual (PPI), demonstrando haver necessidade de mais pesquisas nesta área.

CONCLUSÕES

Evidenciamos neste estudo que a segurança digital como técnica de criptografia dos dados atualmente é essencial e quando se trata da PPI esses cuidados têm que ser redobrados, podendo significar o fracasso ou sucesso de uma instituição.

Na literatura internacional surgem inúmeras ameaças em um curto espaço de tempo e as medidas de segurança tem que ser atualizadas e inovadas constantemente. Hoje as guerras entre Nações não ocorrem apenas no território terrestre com armas bélicas, e sim, no território digital com ataques cibernéticos, como no caso da guerra entre a Rússia e a Ucrânia.

A *Cloud Computing* neste cenário se mostra como um fator importante para PPI, pelo fato de cada vez mais os dados estão sendo migrados para esses serviços. A Inteligência Artificial também está nesse grupo, sendo que pode ser tanto usada para a segurança dos dados digitais como para atacar sistemas.

Inovar em segurança digital será sempre necessário, as instituições devem cada vez mais investir recursos em pesquisa e inovação para manter vigilante e protegida a Propriedade Intelectual.

REFERÊNCIAS

- ARORA, Shaifali M. et al. A DWT-SVD based robust digital watermarking for digital images. **Procedia computer science**, v. 132, p. 1441-1448, 2018.
- ARUMUGAM, G.; SULEKHA, V. Jane Varamani. IMR based anonymization for privacy preservation in data mining. In: **Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society**. 2016. p. 1-8.
- ARAÚJO, Elza Fernandes et al. Propriedade Intelectual: proteção e gestão estratégica do conhecimento. **Revista Brasileira de Zootecnia**, v. 39, p. 1-10, 2010.
- AZEVEDO, Rogério Cabral De; ENSSLIN, Leonardo; JUNGLES, Antônio Edésio. A Review of Risk Management in Construction: Opportunities for Improvement. **Modern Economy**, v. 05, n. 04, p. 367–383, 2014. DOI: 10.4236/me.2014.54036.
- BARATÈ, Adriano et al. Managing intellectual property in a music fruition environment. **IEEE MultiMedia**, v. 23, n. 2, p. 84-94, 2015.
- BARBOSA, Cláudio. Propriedade intelectual: introdução à propriedade intelectual como informação. **Elsevier Brasil**, 2013.
- BRANDMAN, Josh et al. A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems. **Journal of Manufacturing Systems**, v. 56, p. 202-212, 2020.
- CHANDLER, Jacqueline; CUMPSTON, Miranda; THOMAS, James; HIGGINS, Julian PT; DEEKS, Jonathan J.; CLARKE, Mike J. **Cochrane Capítulo I: Introdução | Treinamento**. 2021. Disponível em: <https://training.cochrane.org/handbook/current/chapter-i>.
- FARRAND, Benjamin. Combatting physical threats posed via digital means: the European Commission's developing approach to the sale of counterfeit goods on the Internet. **European Politics and Society**, v. 19, n. 3, p. 338-354, 2018.
- HIGGINS, Julian; THOMAS, James; CHANDLER, Jacqueline; CUMPSTON, Miranda; LI, Tianjing; PAGE, Matthew J.; WELCH, Vivian A. **Manual de Cochrane para Revisões Sistemáticas de Intervenções 6.1**. 2. ed. Oxford UK: Wiley-Blackwell, 2020. v. 1
- HOU, Jong-Uk et al. Copyright protections of digital content in the age of 3d printer: Emerging issues and survey. **IEEE Access**, v. 6, p. 44082-44093, 2018.
- KUMAR, Singh Arun; JUHI, Singh; VIKRAM, Singh Harsh. DCT-and DWT-Based Intellectual Property Right Protection in Digital Images. In: **First International Conference on Artificial Intelligence and Cognitive Computing**. Springer, Singapore, 2019. p. 507-513.
- LAPES, Laboratório de Pesquisa em Engenharia de Software. **StArt — LaPES - Laboratório de Pesquisa em Engenharia de Software** LaPES-Laboratório de Pesquisa em Engenharia de Software, 2005. Disponível em: http://lapes.dc.ufscar.br/tools/start_tool.

MACHADO, FELIPE NERY RODRIGUES. Segurança da informação: princípios e controle de ameaças. **Saraiva Educação SA**, 2014.

MATIAS-PEREIRA, José. A gestão do sistema de proteção à propriedade intelectual no Brasil é consistente?. **Revista de Administração Pública**, v. 45, p. 567-590, 2011.

MINGALEVA, Zhanna; MIRSKIKH, Irina. The problems of digital economy development in Russia. In: **The 2018 International Conference on Digital Science**. Springer, Cham, 2018. p. 48-55.

MISHRA, Kamta Nath. Aadhar based smartcard system for security management in South Asia. In: **2016 International Conference on Control, Computing, Communication and Materials (ICCCCM)**. IEEE, 2016. p. 1-6.

MUNN, Zachary; PETERS, Micah D. J.; STERN, Cindy; TUFANARU, Catalin; MCARTHUR, Alexa; AROMATARIS, Edoardo. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. **BMC Medical Research Methodology**, v. 18, n. 1, p. 1–7, 2018. DOI: 10.1186/S12874-018-0611-X/TABLES/1. Disponível em: <https://bmcmmedresmethodol.biomedcentral.com/articles/10.1186/s12874-018-0611-x>.

OCTAVIANO, Fábio R.; FELIZARDO, Katia R.; MALDONADO, José C.; FABBRI, Sandra C. P. F. Semi-automatic selection of primary studies in systematic literature reviews: is it reasonable? **Empirical Software Engineering**, v. 20, n. 6, p. 1898–1917, 2015. DOI: 10.1007/s10664-014-9342-8. Disponível em: <http://link.springer.com/10.1007/s10664-014-9342-8>.

OCTAVIANO, Fábio; SILVA, Cleiton; FABBRI, Sandra. Using the SCAS strategy to perform the initial selection of studies in systematic reviews: an experimental study. In: 2016, **Anais [...]**: Association for Computing Machinery, 2016. p. 1–10. DOI: 10.1145/2915970.2916000. Disponível em: <https://doi.org/10.1145/2915970.2916000>.

PARETO, Vilfredo. **Cours d'économie politique**. Librairie Droz, 1964. v. 1

PENNAFORTE, Charles; RAMOS, Thiago Kazuhira Hayasaka. Os Desafios da Cibersegurança Russa: Algumas Considerações: The Challenges of Cybersecurity Russian: Some Considerations. **Revista Intellector-ISSN 1807-1260-[CENEGRI]**, v. 17, n. 34, p. 47-61, 2020.

SANTOS, L. D. V.; HOLANDA, F. S. R.; OLIVEIRA, C. V. de S.; HOLANDA, V. de A. R.; CAMPOS, M. S.; MACHADO, J. dos S. Brand equity sustentável: levantamento teórico sobre marcas relacionadas a exploração florestal. **Concilium**, [S. l.], v. 22, n. 2, p. 169–183, 2022. DOI: 10.53660/CLM-106-127B. Disponível em: <https://clium.org/index.php/edicoes/article/view/106>. Acesso em: 13 mar. 2022.

SHUGUO, Yang; QINGLIANG, Liu. Image watermarking algorithm based on wavelet transform. In: **2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP)**. IEEE, 2017. p. 116-121.

SINGH, V. and SETHI, M.R. Digital Trade And Artificial Intelligence: Role Of Intellectual Property. **NTUT Journal of Intellectual Property Law and Management**, v. 10, p. 45-66, 2021.

SLAMET, Cepy; RAHMAN, Ali; RAMDHANI, Muhammad Ali; DARMALAKSANA, Wahyudin. Clustering the verses of the Holy Qur'an using K-means algorithm. **Asian Journal of Information Technology**, v. 15, n. 24, p. 5159–5162, 2016. Disponível em: <http://digilib.uinsgd.ac.id/5117/1/5159-5162> Clustering the Verses of the Holy Quran using K-Means Algorithm.pdf.

SU, Ziyi et al. Owner-stipulated data security and privacy for data accessing in Mobile Cloud context. In: **2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)**. IEEE, 2017. p. 1-5.

SUN, Wenyue et al. Blockchain and homomorphic encryption for digital copyright protection. In: **2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)**. IEEE, 2020. p. 754-761.

TSAL, Shu-Min. A robust zero-watermarking algorithm for audio based on LPCC. In: **2013 1st International Conference on Orange Technologies (ICOT)**. IEEE, 2013. p. 63-66.

URVOY, Matthieu; GOUDIA, Dalila; AUTRUSSEAU, Florent. Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. **IEEE Transactions on Information Forensics and Security**, v. 9, n. 7, p. 1108-1119, 2014.

WAKSMAN, Adam; SETHUMADHAVAN, Simha; EUM, Julianna. Practical, lightweight secure inclusion of third-party intellectual property. **IEEE Design & Test**, v. 30, n. 2, p. 8-16, 2013.

WANG, Yang. Security-driven distributed platforms for intellectual property resource provision-a case study of TSITE IP. **Journal of Cloud Computing**, v. 10, n. 1, p. 1-15, 2021.

XU, Xin. Coordination between the Intellectual Property Enforcement in the Digital Environment and the Data Security. In: **2012 Second International Conference on Business Computing and Global Informatization**. IEEE, 2012. p. 804-807.

YU, Jin-Yong; KIM, Yujun; KIM, Young-Gab. Intelligent video data security: a survey and open challenges. **IEEE Access**, v. 9, p. 26948-26967, 2021.

YULIANI, Asri Rizki; ROSIYADI, Didi. Copyright protection for color images based on transform domain and luminance component. In: **2016 International Conference on Information Technology Systems and Innovation (ICITSI)**. IEEE, 2016. p. 1-4.

Recebido em: 10/03/2022

Aprovado em: 15/04/2022

Publicado em: 23/04/2022