

Ketylen Suelen dos Anjos Dias

suelenanjos16@gmail.com.br
<http://orcid.org/0000-0001-8870-9716>

Universidade Federal de Sergipe
São Cristóvão, Sergipe, Brasil

Cristiane Toniolo Dias

cristonidias@gmail.com
<http://orcid.org/0000-0002-7204-8930>

Universidade Federal de Sergipe,
São Cristóvão, Sergipe, Brasil

Marcelo de Paula

marcelop@ufob.edu.br
<http://orcid.org/0000-0003-0234-727>

Universidade Federal de Sergipe, São
Cristóvão, Sergipe, Brasil.

Privacidade e inteligência artificial: uma análise exploratória

RESUMO

Devido à evolução da inteligência artificial e as violações de direito autoral, se faz necessário refletir os mecanismos e implicações do processo de coleta de dados. O objetivo deste trabalho consiste em entender as preocupações quanto à privacidade, dados de direitos autorais, analisar as práticas atuais e propor medidas baseadas na revisão de literatura e análise qualitativa. Neste estudo, encontramos algumas lacunas referentes à regulamentação e ética, além disso, encontramos desafios para proteger direitos autorais e propriedade intelectual usando inteligência artificial. Conclui-se, por fim, que é indispensável a implementação de uma regulamentação de longo prazo voltada à proteção dos direitos autorais.

PALAVRAS-CHAVE: big data, aprendizado de máquina, direitos autorais, ética, proteção de dados

INTRODUÇÃO

A Inteligência Artificial (IA) está cada vez mais presente entre indivíduos e empresas (Mariani, Dwivedi, 2024). Para Lyreskog *et al.* (2023), com a expansão das IAs, aumentam as preocupações em relação à privacidade de dados dos usuários que estão disponíveis na Internet. Como se trata de um tema recente e em constante evolução, ainda é difícil compreender plenamente como os dados serão utilizados. Entre as maiores preocupações estão a manipulação desses dados, a falta de transparência no controle sobre eles e o risco de roubo por indivíduos mal-intencionados. Além disso, existem questões éticas quanto à propriedade desses dados. Segundo os estudos de Xu *et al.* (2024), com a expansão desta tecnologia, os desenvolvedores estão utilizando aprendizado de máquina para fazer com que o sistema gere imagens a partir de *big data*. Esta técnica possibilita a criação de recursos úteis, mas também ameaça a privacidade de dados e os direitos autorais, além de gerar brechas na legislação vigente para lidar com esse tipo de tecnologia (Hadzovic *et al.*, 2024).

Com base nas discussões de Mariani e Dwivedi (2024), uma das categorias da inteligência artificial é o *insight* cognitivo, que envolve a interpretação e detecção de padrões em grandes volumes de dados por meio da aplicação de algoritmos de aprendizado de máquina. Nesse contexto, Meszaros e Ho (2021) ressaltam a dificuldade em acessar esses dados, uma vez que é necessário obter autorização dos proprietários para compor bancos de dados.

Os modelos mais comuns de IA generativa utilizam conjuntos de dados com grandes volumes de informações que não possuem classificação ou rótulos individuais para cada dado. Dessa forma, a máquina pode estar sendo alimentada com informações de dados privados ou que contém direitos autorais, sem que o proprietário desses dados seja devidamente informado ou aceite voluntariamente que seus dados sejam utilizados para o treinamento de programas de inteligência artificial. Há uma técnica chamada "*data scraping*" ou "*web crawling*", que consiste na extração automatizada de conteúdo de sites. Esse processo pode ser utilizado para coletar grandes volumes de dados rapidamente, muitas vezes sem respeitar as políticas de privacidade estabelecidas pelos sites, mesmo que essas regras estejam claramente expostas. Para executar essa técnica, geralmente há a necessidade de um intermediário humano que configure e supervisione o processo, extraia e processe os dados, e, em alguns casos, os utilize em grandes bases de dados (*big data*) com a finalidade, intencional ou não, de treinar algoritmos de aprendizado de máquina. Os tipos de dados utilizados podem incluir imagens, vídeos, textos e até informações pessoais, desde que estejam publicamente disponíveis na internet. No entanto, é difícil rastrear como e por quem essas informações estão sendo usadas, especialmente porque algumas empresas, como a OpenAI, nem sempre fornecem detalhes claros sobre o uso e tratamento desses dados (Garcia-Pomareda, 2024).

O objetivo deste trabalho é explorar e analisar, por meio de um estudo qualitativo e uma revisão da literatura, as preocupações, práticas atuais e propostas relacionadas à privacidade de dados pessoais e proteção de materiais protegidos por direitos autorais, além de sua conexão com o uso de Inteligência Artificial.

METODOLOGIA

Este trabalho adotou uma abordagem metodológica fundamentada no conceito de Grant e Booth (2009), utilizando a revisão bibliométrica para identificar lacunas na proteção de dados, inteligência artificial e direitos autorais. Além disso, empregou o método qualitativo para a análise e interpretação dos dados, conforme Mihás (2023).

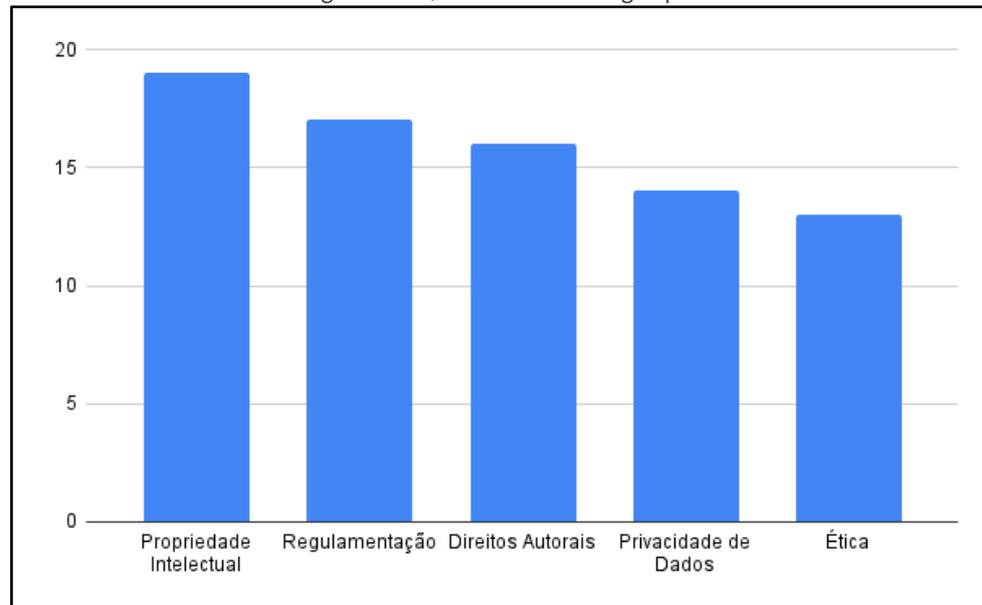
Para a análise dos artigos, foram adotados os seguintes critérios de inclusão e exclusão durante a seleção: artigos que tratam diretamente de temas relacionados à proteção de dados, inteligência artificial ou direitos autorais; e artigos de pesquisa publicados nos últimos 6 anos, incluindo o ano atual (2024), em periódicos conceituados.

Durante os meses de agosto e setembro de 2024, foram conduzidas buscas avançadas por artigos de pesquisa e de revisão, publicados entre os anos de 2019 a 2024, através das bases de dados: *Scimedirect* e *Web of Science*. A lista de palavras-chave usadas incluiu: (*Privacy*); (*Generative Artificial Intelligence*); (*Intellectual Property*); (*Copyright*); (*Big Data*); (*AI*); (*Ethics*); (*Generative Artificial Intelligence*); (*Copyright; Regulation; Generative Artificial Intelligence*). Para a pesquisa na *Web of Science*, foi necessário refinar os resultados para assegurar sua relevância e alinhamento com o tema da investigação, utilizando os seguintes tópicos: (*Computer Science Information Systems*); (*Computer Science Theory Methods*); (*Computer Science Software Engineering*); (*Ethics*); (*Computer Science Cybernetics*); (*Statistics Probability*). A busca na *ScienceDirect* identificou 321 estudos, dos quais 47 foram selecionados para uma revisão preliminar de conteúdo. Desses, 11 artigos foram incluídos na revisão de literatura e na análise qualitativa detalhada deste trabalho. Na *Web of Science*, 142 artigos foram encontrados, com 21 selecionados após a refinação de conteúdo para compor a revisão de literatura.

RESULTADOS

Por meio da revisão da literatura, foram identificados 32 artigos que abordavam especificamente temas como privacidade de dados, propriedade intelectual, direitos autorais e inteligência artificial generativa. Para melhor compreensão, foi gerado um gráfico que analisou a relevância de cada tópico, com base na frequência com que esses temas surgiram nas pesquisas realizadas nos bancos de dados. A análise gráfica permitiu visualizar as tendências predominantes, destacando a ênfase maior em propriedade intelectual, direitos autorais e regulamentação, enquanto questões de ética e privacidade de dados apresentaram menor recorrência. Essa distribuição oferece insights sobre as áreas de maior atenção acadêmica e prática no cenário atual. A figura 1 mostra a quantidade de artigos por assunto.

Figura 1 – Quantidade de artigos por assunto



Com base na Figura 1, é possível observar as seguintes tendências:

Propriedade Intelectual: Como pode ser observado na Figura 1, este foi o tema mais citado entre os 19 artigos selecionados, evidenciando a preocupação com a propriedade intelectual.

Regulamentação: O tema aparece em 17 artigos, enfatizando propostas de soluções por meio de regulamentações legislativas.

Direitos Autorais: Citada em 16 artigos, levanta questões sobre o uso indevido de criações autorais em tecnologias de aprendizado de máquina e seus impactos sobre os autores.

Privacidade de Dados: Pouco mencionado, aparecendo em 14 artigos, levanta questões sobre a coleta indevida de dados e a segurança na internet.

Ética: O tema menos citado, aparecendo em 13 artigos, revela uma lacuna em discussões sobre inteligência artificial, além de refletir preocupações morais sobre o uso de dados no treinamento de inteligência artificial.

É possível constatar a relevância e a preocupação em relação aos assuntos abordados. Em consonância com Kempeneer (2021), foram observados poucos estudos oferecendo soluções práticas, no que se diz respeito à resolução do problema. O quadro 1 mostra o resumo dos resultados encontrados após a análise de cada artigo selecionado.

Tópicos	Síntese	Referências
Preocupações	Poucos autores estudando aplicações práticas; É necessária uma grande quantidade de dados para treinar IA; Insegurança quanto à exposição dos dados; Uso antiético; Falta de consentimento; ainda não é possível avaliar o impacto em relação a direitos autorais e propriedade intelectual; Roubo de propriedade intelectual.	Kempeneer (2021); Ge <i>et al.</i> (2023);Tara <i>et al.</i> (2019); Ashok <i>et al.</i> (2019); Lederer <i>et al.</i> (2023); Xu <i>et al.</i> (2024);Chen <i>et al.</i> (2024); Zhang <i>et al.</i> (2022);Cardona (2024); Wang (2021); Vig (2024); Peng (2023); Yao (2023); Sabherwal <i>et al.</i> (2024); Olimid <i>et al.</i> (2024);
Práticas atuais	Criação de legislação para proteção de direitos autorais; Criação de normas para uso responsável de inteligência artificial.	Magliori (2024); Feng e Nie (2024); Riemer e Perter (2024); Hacker (2023); Laux <i>et al.</i> (2024); Zhang <i>et al.</i> (2024)
Propostas	Marca d'água baseados em gatilhos; Codificação anticulusão para garantir a verificação da propriedade; Abordagem de caracterização das ameaças à propriedade intelectual; Sistema de bloqueio denominado <i>M-LOCK</i> ; Criptografia e ocultação para prevenir a divulgação de informações sensíveis; Impressão digital; ActiveGuard, que utiliza impressão digital para gerenciar a autorização e a verificação de propriedade; emendas do Parlamento da União Europeia à Lei de IA; Transparência em relação aos termos de uso, especialmente no que se refere à inteligência artificial, propriedade intelectual e privacidade pessoal; Implementação de diretrizes éticas para o treinamento de IA generativa; Desenvolvimento de ferramentas abrangentes para auxiliar na detecção de materiais protegidos por lei.	Helberger (2024); Ruan <i>et al.</i> (2023); Fenwick e Jurcys (2023); Dwivedi <i>et al.</i> (2021); Lin <i>et al.</i> (2024); Luo <i>et al.</i> (2024); Peng <i>et al.</i> (2023); Ren <i>et al.</i> (2024); Lederer <i>et al.</i> (2023); Zhang <i>et al.</i> (2022); Liu <i>et al.</i> (2024); Xue <i>et al.</i> (2021); Lucchi (2023); Knott <i>et al.</i> (2023)

Quadro1 Visão geral das preocupações, práticas atuais e propostas de solução em IA

Preocupações

Conforme apontam Lederer *et al.* (2023), a pesquisa na área de aprendizado de máquina ainda está em fase inicial, além de não existir uma visão unificada sobre as vulnerabilidades tornando mais desafiador o desenvolvimento de abordagens abrangentes frente às crescentes ameaças e aos novos métodos de proteção e contra-ataques que estão sendo continuamente aperfeiçoados.

O primeiro ponto para entender o funcionamento da inteligência artificial é conhecer seu processo. *Big datas* são alimentadas pela quantidade de dados disponíveis na internet. No entanto, Kempeneer (2021) levanta o debate sobre a forma na qual os dados estão sendo coletados, interpretados e usados. Como não é possível treinar máquinas de aprendizagem sem usar *big data*, Ge *et al.* (2023) questiona a qualidade e a fonte desses dados. Diversas fontes, como Tara *et al.* (2019) e Ashok *et al.* (2019), destacam o uso antiético e o compartilhamento indevido de dados, frequentemente empregados na prática de crimes de pirataria e violações de direitos autorais.

A violação da privacidade se inicia quando as empresas optam por obter dados de maneira ilegal, infringindo a propriedade intelectual dos dados utilizados (Xu *et al.*, 2024) na internet. Zhang *et al.* (2022) abordam essa questão, enfatizando os riscos presentes em toda a cadeia de processamento de *big data*. Assim, essas empresas não apenas violam os direitos autorais, mas também comprometem a privacidade dos usuários da internet que não consentiram com o uso de seus dados para treinar sistemas de inteligência artificial. Wang (2021) questiona as lacunas na proteção da propriedade intelectual e alerta que isso pode comprometer o desenvolvimento da indústria da informação.

De acordo com a legislação indiana, Vig (2024) questiona a justiça de utilizar materiais protegidos por direitos autorais para treinar máquinas de aprendizado. Por outro lado, Peng (2023) argumenta que a utilização desses dados caracteriza roubo de propriedade intelectual. Cardona (2024) ressalta que o avanço tecnológico não deve comprometer a democracia da sociedade, enquanto Yao (2023) propõe a criação de um sistema jurídico adequado para mitigar as ameaças que a inteligência artificial generativa representa para a humanidade.

A preocupação com a privacidade dos dados abrange uma discussão mais ampla. Sabherwal *et al.* (2024) questionam a qualidade dos modelos generativos e a veracidade dos resultados que eles produzem, além das implicações regulatórias necessárias para controlar essas questões. Essa perspectiva ressalta a importância de enfatizar princípios éticos na regulamentação da inteligência artificial e na proteção de dados pessoais (Olimid *et al.*, 2024).

Os riscos éticos estão ligados à confiabilidade da ferramenta, à responsabilização pelo uso dos dados, ao viés algorítmico e à privacidade das informações (Chen e Esmailzadeh, 2024). Nesse contexto, Ali e Aysan (2024) enfatizam a integridade dos dados e suas implicações sociais. Por fim, Knott *et al.* (2023) sugerem que o desempenho dos classificadores deve ser testado em amostras de conteúdo gerado tanto por inteligência artificial quanto por humanos, que não foram utilizadas durante o treinamento, a fim de garantir a precisão e a confiabilidade dos sistemas de IA.

Práticas atuais

O gerenciamento da tecnologia de inteligência artificial enfrenta desafios significativos, como ressaltado por Magliori (2024), que destaca as regulamentações da União Europeia para proteger direitos autorais e garantir a segurança dos dados, promovendo maior transparência. Segundo Riemer e Perter (2024), alguns países impuseram restrições ao uso de dados, aumentando seu valor de mercado, levando empresas a optarem pelo uso de dados gratuitos. A ISO também publicou o documento ISO/IEC 4200 em 2023 para garantir privacidade de dados e legalidade no desenvolvimento de IA (Laux *et al.*, 2024). No entanto, Hacker (2023) argumenta que essas legislações não são suficientes a longo prazo.

Em regiões mais desenvolvidas, como a China, é possível observar o impacto positivo das regulamentações voltadas para a proteção da propriedade intelectual e das indústrias tecnológicas (Feng e Nie, 2024). No entanto, muitas empresas ainda violam a privacidade dos indivíduos durante a coleta e o processamento de dados, o que se torna uma questão prioritária. Embora algumas leis e regulamentações estejam sendo elaboradas, essa área ainda enfrenta diversos desafios, desde a resistência das empresas em se adequar até a falta de compreensão do público sobre essas questões (Zhang *et al.*, 2024).

Propostas

Para abordar a proteção da propriedade intelectual em modelos de inteligência artificial, diversos autores propuseram estratégias e destacaram desafios específicos. Helberger (2024) enfatiza a necessidade de esclarecer a procedência dos dados e definir estratégias antes de implementar soluções relacionadas à privacidade, direitos autorais e segurança. Fenwick e Jurcys (2023) sublinham a importância de responsabilizar legisladores e desenvolvedores para prevenir práticas ilegais viabilizadas pela IA. Dwivedi *et al.* (2021) destacam a criação de políticas públicas adequadas para acompanhar o rápido avanço da tecnologia, garantindo a segurança digital da população.

A primeira tentativa de proteger a propriedade intelectual envolve mecanismos de marca d'água baseados em gatilhos (Ruan *et al.*, 2023). Essa abordagem é semelhante à proposta de Lin *et al.* (2024), que também sugere um protocolo baseado em marca d'água, mas incorpora o mapeamento de caos logístico para assegurar que modelos sem a marca d'água não sejam classificados. Por sua vez, Luo *et al.* (2024) propõem a utilização de codificação anticodificação para garantir a verificação da propriedade, sem comprometer a precisão do modelo. Segundo Peng *et al.* (2023), essas abordagens podem ser categorizadas como proteção passiva e ativa para redes neurais profundas.

Além disso, Lederer *et al.* (2023) propuseram uma abordagem inovadora no aprendizado de máquina, centrada na caracterização das ameaças à propriedade intelectual. Em contraste, Ren *et al.* (2024) desenvolveram um sistema de bloqueio denominado *M-LOCK*, que proporciona proteção ativa aos modelos de propriedade intelectual. Zhang *et al.* (2022) já destacavam a relevância das técnicas de criptografia e ocultação para prevenir a divulgação de informações sensíveis.

Outra estratégia de proteção, além da marca d'água, é a impressão digital. Liu *et al.* (2024) criaram uma arquitetura que preserva tanto os dados quanto o processo de treinamento da inteligência artificial, resultando na geração de impressões digitais. Xue *et al.* (2021) introduziram o *ActiveGuard*, que utiliza impressão digital para gerenciar a autorização e a verificação de propriedade.

No que diz respeito às propostas legislativas, já existem algumas em discussão, como as emendas do Parlamento da União Europeia à Lei de IA. Lucchi (2023) argumenta que os repositórios devem garantir transparência em relação aos termos de uso, especialmente no que se refere à inteligência artificial, propriedade intelectual e privacidade pessoal. O autor também recomenda a implementação de diretrizes éticas para o treinamento de IA generativa, que incluem aspectos relacionados à coleta de dados, compensação aos proprietários, consentimento e transparência.

Além disso, é crucial o desenvolvimento de ferramentas abrangentes para auxiliar na detecção de materiais protegidos por lei (Knott *et al.*, 2023).

A discussão dos resultados sugere a necessidade de novos estudos para determinar a melhor abordagem para evitar a coleta indevida de dados protegidos por direitos autorais. Apesar dos resultados encontrados, a pesquisa destaca lacunas em relação a regulamentações, soluções a longo prazo e transparência na coleta de dados. Além de criar restrições e barreiras para evitar a violação de direitos autorais, como por exemplo, marca d'água, impressão digital e algumas ferramentas para detecção de uso de propriedade intelectual.

CONCLUSÕES

Esse estudo fornece uma revisão de estudos sobre privacidade de dados e inteligência artificial com foco em direitos autorais. Existe uma preocupação quanto aos dados expostos na Internet e como eles podem ser usados. Para restringir o uso antiético dos dados, propomos algumas recomendações para regulamentações que responsabilizam as empresas que não obtêm o consentimento dos indivíduos no desenvolvimento de inteligência artificial. Nem toda empresa utiliza dados de direitos autorais, no entanto existem diversas violações de propriedade intelectual e coleta indevida de dados pessoais para geração de conteúdo. No entanto, pesquisas adicionais são necessárias para entender o impacto da inteligência artificial na vida das pessoas e quais técnicas utilizar para proteger direitos de criação.

Privacy and artificial intelligence: an exploratory analysis

ABSTRACT

Due to the evolution of artificial intelligence and copyright infringements, it is necessary to reflect on the mechanisms and implications of the data collection process. The objective of this work is to understand the concerns regarding privacy, copyright data, analyze current practices and propose measures based on literature review and qualitative analysis. In this study, we found some gaps regarding regulation and ethics, in addition, we found challenges to protect copyright and intellectual property using artificial intelligence. Finally, we conclude that the implementation of long-term regulation aimed at protecting copyright is essential.

KEYWORDS: big data, machine learning, copyright, ethics, data protection

REFERÊNCIAS

Ali, H.; Aysan, A., F. **“Ethical dimensions of generative AI: a cross-domain analysis using machine learning structural topic modeling”**, International Journal of Ethics and Systems, 2024.

Ashok, M.; Madan, R.; Joha, A.; Sivarajah, U. **“Ethical framework for Artificial Intelligence and Digital technologies”**, International Journal of Information Management, Vol. 62, 2022.

Cardona, N., J. **“El 'uso Transformador' De Las Empresas De IA: Entre La Libertad Creativa Y Los Derechos De Propiedad Intelectual”**, Revista De Internet, Derecho Y Política. Vol. 40, pp. 1-11, 2024.

Chen, Y.; Esmailzadeh, P. **“Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges”**, J Med Internet Res, 2024.

Dwivedi, Y., K.; Hughes, L.; Ismagilova, E.; Aarts, G.; Coombs, C.; Crick, T.; Duan, Y.; Dwivedi, R.; Edwards, J.; Eirug, A.; Galanos, V.; Ilavarasan, V.; Janssen, M.; Jones, P.; Kar, A., K.; Kizgin, H.; Kronemann, B.; Lal, B.; Lucini, B.; Medaglia, R.; Williams, M., D. **“Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy”**, International Journal of Information Management, Vol. 57, 2021.

Feng, Y.; Nie, C. **“The effect of government informatization construction on corporate digital technology innovation: New evidence from China”**, Business, Ethics, The Environment & Responsibility, 2024.

Fenwick, M.; Jurcys, P. **“Originality and the future of copyright in an age of generative AI”**, Computer Law & Security Review, Vol. 51, 2023.

Garcia-Pomareda, J. D. **“Inteligencia artificial generativa: un arma de doble filo para el metaverso”**, Revista e-mercatoria, Vol. 23, n. 2, pp. 295–323, 2024.

Ge, L.; Li, H.; Wang, X.; Wang, Z. **“A review of secure federated learning: Privacy leakage threats, protection technologies, challenges and future directions”**, Neurocomputing, Vol. 561, 2023.

Grant, M. J.; Booth, A. **“A typology of reviews: An analysis of 14 review types and associated methodologies”**, Health Information & Libraries Journal, Vol. 26(2), pp. 91-108, 2009.

Hacker, P. **“The European AI liability directives – Critique of a half-hearted approach and lessons for the future”**, Computer Law & Security Review, Vol. 51, 2023.

Hadzovic, S.; Becirspahic, L.; Mrdovic, S. **“It's time for artificial intelligence governance”**, Internet of Things, Vol. 27, 2024.

Helberger, N. **“FutureNewsCorp, or how the AI Act changed the future of news”**, Computer Law & Security Review, Vol. 52, 2024.

Kempeneer, S. **“A big data state of mind: Epistemological challenges to accountability and transparency in data-driven regulation”**, Government Information Quarterly, Vol. 38, 2021.

Knott, A.; Pedreschi, D.; Chatila, R.; Chakraborti, T.; Leavy, S.; Baeza-Yates, R.; Eysers, D.; Trotman, A.; Teal, P., D.; Biecek, P.; Russell, S.; Bengio, Y. **“Generative AI models should include detection mechanisms as a condition for public release”**, Ethics Inf Technol, Vol. 25(55), 2023.

Laux, J.; Wachter, S.; Mittelstadt, B. **“Three pathways for standardisation and ethical disclosure by default under the European union artificial intelligence act”**, Computer Law & Security Review, Vol. 53, 2024.

Lederer, I.; Mayer, R.; Rauber, A. **“Identifying Appropriate Intellectual Property Protection Mechanisms for Machine Learning Models: A Systematization of Watermarking, Fingerprinting, Model Access, and Attacks”**, Ithaca, 2023.

Leong, P.; Freeman, B. **“Riding the waves over generative AI in Malaysia: policies and responses”**, Communication Research and Practice, Vol. 10(3), pp. 362–374, 2024.

Lin, HJ.; Shen, SY.; Lyu, HJ. **“Protecting IP of deep neural networks with watermarking using logistic disorder generation trigger sets”**, Multimed Tools Appl, Vol. 83, pp. 10735–10754, 2024.

Lucchi, N. **“ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems”**, European Journal of Risk Regulation, 2023.

Luo, Y.; Li, Y.; Qin, S.; Fu, Q.; Liu, J. **“Copyright protection framework for federated learning models against collusion attacks”**, Information Sciences, Vol. 680, 2024.

Lyreskog, D. M., et al. **"The Ethics of Thinking with Machines: Brain-Computer Interfaces in the Era of Artificial Intelligence"**, International Journal of Chinese & Comparative Philosophy of Medicine, Vol. 21, no. 2, Centre for Applied Ethics, Hong Kong Baptist University, pp. 11–34, 2023.

Mariani, M.; Dwivedi, Y., K. **"Generative artificial intelligence in innovation management: A preview of future research developments"**, Journal of Business Research, Vol. 175, 2024.

Meszaros, J.; Ho, Ch. **"AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?"**, Computer Law & Security Review, Vol. 4, 2021.

Mihas, P. **"Qualitative research methods: approaches to qualitative data analysis"**, International Encyclopedia of Education, pp. 302-313, 2023.

Migliorini, S. **"China's Interim Measures on generative AI: Origin, content and significance"**, Computer Law & Security Review, Vol. 53, 2024.

Olimid, A., P.; Georgescu, C., M.; Olimid, D., A. **"Legal Analysis of EU Artificial Intelligence Act (2024): Insights from Personal Data Governance and Health Policy"**, Access to Justice in Eastern Europe, 2024.

Peng, S.; Chen, Y.; Xu, J.; Chen, Z.; Wang, C.; Jia, X. **"Intellectual property protection of DNN models"**, World Wide Web Vol. 26, pp. 1877–1911, 2023.

Ren, G.; Wu, J.; Li, G. L.; Li, S. H.; Guizani, M. **"Protecting Intellectual Property With Reliable Availability of Learning Models in AI-Based Cybersecurity Services"**, IEEE Transactions on Dependable and Secure Computing, Vol. 21 (2), pp. 600-617, 2024.

Riemer, K.; Peter, S. **"Conceptualizing generative AI as style engines: Application archetypes and implications"**, International Journal of Information Management, Vol. 79, 2024.

Ruan, H.; Song, H.; Liu, B.; Cheng, Y.; Liu, Q. **"Intellectual property protection for deep semantic segmentation models"**, Front. Comput. Sci. Vol. 17, 2023.

Sabherwal, R.; Grover, V. **"The Societal Impacts of Generative Artificial Intelligence: A Balanced Perspective"**, Journal of the Association for Information Systems, Vol. 25(1), pp. 13-22, 2024.

Sun, T., Q.; Medaglia, R. **“Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare”**, Government Information Quarterly, Vol. 36, pp. 368-383, 2019.

Vig, S. **“Intersection of generative artificial intelligence and copyright: an Indian perspective”**, Journal of Science and Technology Policy Management, 2024.

Wang, Y. **“Security-driven distributed platforms for intellectual property resource provision - a case study of TSITE IP”**, Journal of Cloud Computing, Heidelberg, Vol. 10, n. 1 (12), 2021.

Xu, Q.; Jiang, X.; Sun, T.; Wang, W.; Meng, L.; Yan, H. **“Detecting Artificial Intelligence-Generated images via deep trace representations and interactive feature fusion”**, Information Fusion, Vol. 112, 2024.

Yao, L. **“Specifics of Regulatory and Legal Regulation of Generative Artificial Intelligence in the UK, USA, EU and China”**, Law Journal of the Higher School of Economics, n. 3, pp. 245-267, 2023.

Zhang, J.; Yang, A.; Shuaishuai, F. **“Data Protection of Internet Enterprise Platforms in the Era of Big Data”**, Journal of Web Engineering, Vol. 21(3), pp. 861-878, 2022.

Recebido: 2024-09-23

Aprovado: 2024-09-30

DOI: 103895/recit.v16n39.19181

Como citar: DIAS, Ketylen Suelen dos Anjos; DIAS, Cristiane Toniolo; PAULA, Marcelo de. Privacidade e inteligência artificial: uma análise exploratória R. Eletr. Cient. Inov. Tecnol, Medianeira, v. 16. n. 39, p. 36- 49, jan/abr, 2025 Disponível em: <<https://periodicos.utfpr.edu.br/recit>>. Acesso em: XXX.

Correspondência:

Ketylen Suelen dos Anjos Dias

Universidade Federal de Sergipe, São Cristóvão, Sergipe, Brasil.

Rosa Elze, São Cristóvão - SE, 49100-000

Direito autoral: Este artigo está licenciado sob os termos da Licença creativecommons.org/licenses/by-nc/4.0 Internacional.

