Um panorama bibliométrico da proteção de dados e da privacidade em contexto de avanço da inteligência artificial

A bibliometric overview of data protection and privacy in the context of the advance of artificial intelligence

AIRES JOSÉ ROVER

Universidade Federal de Santa Catarina, Facultad de Derecho, aires.j.r@ufsc.br

Resumen

Durante el proceso de establecimiento de una nueva sociedad, surgen varios temas dignos de análisis y reflexión, destacando entre ellos el papel de la inteligencia artificial, especialmente el aprendizaje automático y sus aplicaciones predictivas. Aunque se ha explorado ampliamente la protección de datos personales y la privacidad en la literatura científica, existe una notable ausencia de estudios que conecten este análisis con las últimas técnicas de inteligencia artificial. En este sentido, proponemos llevar a cabo un mapeo más cuantitativo que cualitativo de las publicaciones científicas más influyentes que abordan estos temas interrelacionados. Para cumplir con este objetivo, hemos optado por utilizar un enfoque bibliométrico, llevado a cabo durante los meses de marzo y abril de 2024, empleando un método de análisis inductivo y adoptando el procedimiento de estudio de caso.

Palabras clave: Revisiones bibliográficas. Protección de datos. Privacidad. Inteligencia artificial.

Abstract

A new societal landscape is taking form, marked by a myriad of emerging themes warranting thorough examination. Chief among these discussions is the pivotal role of artificial intelligence (AI), particularly machine learning and its predictive applications. Despite extensive exploration of issues pertaining to personal data protection and privacy across scientific literature, there remains a conspicuous dearth of studies integrating this analysis with the latest AI methodologies. Hence, this study endeavors to undertake a predominantly quantitative mapping of the most influential scientific works addressing these interconnected themes. Our approach, conducted over the span of March and April 2024, employs a bibliometric methodology, prioritizing an inductive analysis framework and adopting the case study methodology to fulfill this objective.

Keywords: Bibliographic reviews. Data protection. Privacy. Artificial intelligence.

1. Introdução

Uma nova sociedade está sendo moldada, e nesse processo emergem diversos temas que merecem análise e reflexão. No centro dessas discussões está o papel da inteligência artificial, com destaque para o machine learning e suas aplicações preditivas. Embora as questões relacionadas à proteção de dados pessoais e privacidade tenham sido amplamente exploradas em várias publicações científicas, é evidente a falta de estudos que conectem essa análise com o uso das mais recentes técnicas de inteligência artificial.

Assim, este estudo propõe-se a realizar um mapeamento, mais quantitativo do que qualitativo, das publicações científicas mais influentes que abordam esses temas interligados. Para atingir esse propósito, optamos por adotar uma abordagem bibliométrica, conduzida ao longo dos meses de março e abril de 2024, utilizando um método de análise indutiva e adotando o procedimento de estudo de caso.

2. Progresso técnico, riscos e desafios na sociedade contemporânea

A técnica ou tecnologia não são novidades na trajetória da humanidade; elas acompanham o homem desde tempos imemoriais. A emergência da técnica decorre da limitação sensorial inerente ao ser humano. Carente de sentidos, o homem depende da adaptação inteligente do ambiente natural para superar suas deficiências (Gehlen, 1980). A tecnologia, definida como qualquer instrumento artificial que visa controlar a natureza em contraste com o mundo dos homens, é, portanto, uma construção cultural cujos objetos não são encontrados na natureza e têm por objetivo expandir os limites físicos e sensoriais do ser humano.

As demandas da sociedade moderna são extremamente exigentes, demandando a rápida elaboração de grandes quantidades de informações. Anteriormente, havia tempo para assimilar novas informações, permitindo uma aprendiza-

gem interna. No entanto, atualmente, esse processo de interiorização tornou-se inviável. Não é de se estranhar, portanto, que as relações entre as pessoas estejam se tornando cada vez mais superficiais. Tudo acontece em uma velocidade vertiginosa, e todos os processos sociais exigem um número crescente de decisões em intervalos de tempo cada vez mais curtos. A tecnologia, a economia e, por extensão, os demais sistemas sociais, refletem claramente essa revolução. Uma revolução caracterizada por um novo paradigma, composto por um conjunto de inovações técnicas, organizacionais e administrativas interrelacionadas, cujo fator-chave são os insumos baratos de informação decorrentes dos avanços em microeletrônica e telecomunicações, marcados pela redução dos custos relativos e pela disponibilidade universal (Castells, 1999, p. 54).

Esse processo de mediação tecnológica pode ser ainda mais radical, ultrapassando a visão clássica (prometéica) de domínio técnico da natureza, que mantém a fé no progresso material e na melhoria das condições humanas. Estamos potencialmente vivendo uma era fáustica da tecnociência, caracterizada por um impulso cego em direção ao domínio e à apropriação total da natureza, tanto externa quanto internamente ao corpo humano. Baseada em inteligência artificial e outras tecnologias disruptivas, a busca é pela transcendência do ser humano, uma verdadeira superação de suas limitações materiais, por meio da decifração do mistério da vida. Isso instaura uma forma de "biopoder", baseada na possibilidade de surgimento de "sociedades de controle" (Medeiros, 2003, p. 249).

Erros, falhas, riscos e perigos são inerentes a qualquer processo de transformação. Como Riobaldo, em "Grande Sertão: Veredas", afirmava, viver é perigoso. A inteligência humana permitiu a organização e a dominação por meio do trabalho, viabilizando o avanço da tecnologia. Esta se tornou um fator preponderante no processo de produção e transformação da humanidade, reduzindo os perigos, mas aumentando os riscos. O perigo é o risco que se concretiza. No entanto, a preocupação mais imediata é com a possível substituição ou domínio do ser humano por suas criações mecânicas. As máquinas certamente não substituirão o homem, mas o envolverão completamente, conferindo-lhe maior poder sobre a natureza e a sociedade. O verdadeiro risco reside nos processos que apenas as máquinas podem executar ou cujo controle humano é precário. A ameaça de falta de controle sempre estará presente. O que fazer então? Proibir simplesmente pesquisas que possam levar a essas situações? Ou arriscar até certo ponto e aprimorar os mecanismos de controle e vigilância?

A palavra-chave diante desses riscos é responsabilidade. Ela constitui o antídoto para transformar um risco em perigo. Quem são os agentes responsáveis pelas consequências de seus atos e omissões em diversos níveis? Definir esse cenário é uma tarefa regulatória complexa, uma vez que, cada vez mais, a responsabilidade das decisões recai sobre sistemas, e as pessoas tendem a se eximir dela. Não há mais ninguém para culpar em caso de falha: a culpa recai nos sistemas. Beck discute sobre uma sociedade que entra em uma fase de modernização reflexiva, tornando-se tema para si mesma e fonte de instabilidades e riscos provocados pelas novidades tecnológicas e organizacionais (2002, p. 21). Por exemplo, o princípio da precaução encontra seus limites nessa sociedade do risco, que demanda uma reflexão sobre si mesma. Assim, para ser contra o uso de determinada tecnologia, não é necessário possuir conhecimento, enquanto para ser a favor, é preciso possuir um entendimento profundo. O problema reside na polarização ideológica e na falta de conhecimento, o que dificulta a aplicação responsável desse princípio.

Portanto, é essencial aumentar a transparência na produção e distribuição de informações, facilitar a publicação de dados e proteger as informações de caráter privado. Essas são medidas de um regime aberto e de uma sociedade que se organiza de forma transparente e responsável. O avanço das tecnologias digitais pode impulsionar esse movimento. Como destacado por Rover (1995, p. 45), a humanidade há muito tempo almeja a utopia de um mundo universal, onde as pessoas possam estar mais conectadas sem perder sua autonomia, e onde o conhecimento, produto dessa autonomia, possa ser democratizado ao máximo.

Assim, o progresso técnico não é intrinsecamente bom nem mau, mas sim um instrumento cultural que, dependendo de seu uso, pode contribuir para o desenvolvimento humano em geral.

3. Privacidade e proteção de dados diante da inteligência artificial

A questão da privacidade e da proteção dos dados emerge como um tema central e controverso diante do avanço da inteligência artificial e suas técnicas. As lacunas na proteção legal do privado se aprofundam à medida que a capacidade de troca e difusão de informação se amplia. No entanto, é importante examinar os tipos de privacidade que a lei busca salvaguardar: (1) Informações sobre atos em geral que o indivíduo inevitavelmente pratica em público; (2) Informações sobre a vida pessoal que se deseja manter privativas. Enquanto a lei demonstra ser mais eficaz na

proteção do segundo tipo, o controle sobre o primeiro caso é menos eficiente, uma vez que as informações tornam-se públicas ao serem retiradas do âmbito privado, perdendo-se gradualmente o controle sobre elas.

Com o advento da Internet e, mais recentemente, da inteligência artificial em rede, as facilidades para obtenção de informação privada aumentam significativamente. Diversas são as formas de obter informações sobre os usuários, seja por meio de registros explícitos ou das pegadas deixadas durante o uso da rede. Embora as informações sejam geralmente fornecidas voluntariamente pelos usuários, é notório que muitos não estão preocupados em ocultar dados sobre suas vidas, entregando-os prazerosamente em troca de alguma vantagem social. Muitos justificam esse compartilhamento como forma de facilitar a navegação e receber sugestões personalizadas, orientadas por seus interesses.

No entanto, esse cenário suscita um paradoxo entre privacidade e liberdade de expressão. Enquanto é desejável evitar qualquer forma de censura na Internet, é essencial questionar quem determina o que é verdade ou relevante para o usuário. A liberdade de escolha entre diversas opções parece ser um direito fundamental, porém, há interesses políticos e econômicos em restringir essa liberdade, o que pode levar a um cenário reminiscente de um possível Big Brother.

Diante desses desafios, torna-se crucial promover mais liberdade e transparência para proteger os dados pessoais e a privacidade dos cidadãos, sem comprometer a resposta adequada aos desafios impostos pela intersecção entre tecnologia, privacidade e liberdade de expressão.

4. Inteligência Artificial apoiada por técnicas como aprendizado de máquina, Big Data e Large Language Models

A Inteligência Artificial é uma disciplina que recentemente alcançou a maturidade. Existem várias definições, sendo o paradigma da inteligência humana sua referência principal. Conforme Minsky (1985) afirmou, podemos defini-la como a ciência da construção de máquinas capazes de realizar tarefas que demandam inteligência, tal como seriam realizadas por seres humanos. Por outro lado, é também o campo de estudo que busca simular processos inteligentes ou de aprendizagem em máquinas, ou ainda tornar os computadores capazes de executar tarefas nas quais os seres humanos atualmente se destacam. Isso abrange habilidades como agir como especialistas, compreender e comunicar em linguagem natural, e reconhecer padrões como a escrita. Assim, há uma ampla gama de áreas de aplicação, ou melhor, desafios enfrentados por essa tecnologia: processamento de linguagem natural, reconhecimento de padrões (incluindo assinaturas, vozes e impressões digitais), robótica, execução de tarefas, resolução de problemas gerais ou especializados, bases de dados inteligentes, bancos de conhecimento, jogos, entre outros.

O ato de conhecer envolve três componentes: uma representação simbólica do objeto conhecido, uma inferência sobre ele e a capacidade de aprendizagem. Em termos de pesquisa, essa divisão é confirmada pelo foco em três grandes áreas dentro da inteligência artificial: representação do conhecimento, raciocínio e aprendizado (Rover, 2001, p. 108).

Os sistemas de inteligência artificial se valem da heurística, uma técnica utilizada para otimizar os processos de busca, ainda que em detrimento da perfeição ideal. Isso reflete o modo como os seres humanos interagem com o mundo. Essa abordagem serve como base para a implementação dos métodos dedutivo, indutivo e abdutivo. É um processo de compreensão do mundo que utiliza um conjunto definido de regras sobre um conhecimento específico. Assim, raciocinar implica em manipular informações (julgamentos, reconhecimentos), definir uma busca em um espaço de estados e inferir conclusões (Rover, 2001, p. 108).

Quanto ao aprendizado, em termos gerais, é a capacidade de um agente ou sistema melhorar seu desempenho (D) em uma classe de tarefas (T) como resultado da experiência (P). Existem diversas técnicas para implementar o aprendizado nos sistemas. Elas visam melhorar o desempenho, aumentar a robustez e eficiência dos sistemas, aprendendo novas regras e gerando novas soluções (Rover, 2001, p. 63).

Por fim, a representação do conhecimento é crucial. O conhecimento precisa ser representado dentro da máquina para que possa ser processado e apresentar as conclusões desejadas. Isso envolve escolhas de modelagem ontológicas (fonte, alcance, orientação, nível, resolução), de comportamento (precisão, incerteza) e principalmente de representação (equações, associações, procedimentos). Existem várias técnicas de representação, como sistemas de produção, redes semânticas, quadros (frames) e lógica (Rover, 2001, p. 63).

Há muitas técnicas para implementar sistemas inteligentes, e geralmente são introduzidas inovações às técnicas tradicionais ou sistemas híbridos que combinam várias delas. Entre as mais discutidas estão os Sistemas Baseados em Regras, os Sistemas Baseados em Casos e as Re-

des Neurais. Cada técnica tem sua aplicação específica, e é importante evitar a tentativa de substituição arbitrária entre elas, pois suas características são distintas.

A técnica de aprendizado de máquina, tão discutida e testada nos últimos anos, não é uma novidade em si, mas sim uma evolução de algoritmos antigos em sistemas relacionados, como redes neurais ou algoritmos genéticos. O que é novo é a capacidade de acessar e interpretar dados massivos, estruturados e não estruturados, e utilizá-los para fazer predições automáticas (análise preditiva) sem necessidade de nova programação (Assunção, 2018, p. 23). O aprendizado de máquina geralmente é supervisionado por humanos, que preparam e rotulam os dados antes de treinar o algoritmo. Esse processo envolve ajustes com base nos resultados, identificando gradualmente o melhor caminho para alcançar um objetivo específico. A evolução dos algoritmos e o acesso facilitado a grandes bases de dados estão permitindo a automação de decisões que antes eram exclusivamente humanas. É fundamental garantir a correção dos resultados dessas aplicações, utilizando dados imparciais e corrigindo os algoritmos conforme necessário.

As máquinas de aprendizado, embora conhecidas há muito tempo, só recentemente puderam ser implementadas e utilizadas com eficiência devido à disponibilidade de grandes bases de dados para uso geral. Neste contexto, o termo Big Data refere-se à gestão de dados em larga escala, com múltiplos conteúdos e produção em alta velocidade (Ribeiro, 2014, p. 101). A análise desses dados visa à predição de fenômenos com base em correlações diretas, sem necessidade de amostragens menores. No contexto do governo eletrônico, embora o termo Big Data não seja comum, a ideia de "governo aberto" se aproxima, pois os dados governamentais são frequentemente considerados Big Data, e as características mencionadas anteriormente também se aplicam. No entanto, ao contrário do modelo tradicional de dados abertos do governo, nos quais a ênfase está na abertura pelos próprios órgãos governamentais, a abertura possibilitada pela tecnologia de Big Data é mais automatizada, permitindo acesso a um conhecimento que antes era inacessível devido à sua complexidade.

Além das máquinas de aprendizado, uma vertente tecnológica que vem ganhando destaque são os LLMs (Large Language Models), modelos de linguagem de grande escala que utilizam técnicas avançadas de processamento de linguagem natural para entender e gerar texto de forma cada vez mais próxima à humana. Esses modelos, como o GPT (Generative Pre-trained Transformer), têm sido aplicados em uma variedade de campos, desde assistentes virtuais até tradução automática e geração de texto criativo. Com suas capacidades de processamento e compreensão de grandes volumes de dados textuais, os LLMs representam uma ferramenta poderosa para análise e geração de insights em meio ao Big Data.

Mais precisamente, os LLM (Large Language Models), são modelos de aprendizado de máquina treinados em vastos conjuntos de dados. Eles são utilizados para gerar linguagem para interações com humanos e para desenvolver contexto, possibilitando respostas rápidas em plataformas de IA generativa. Tecnologias como ChatGPT, Gemini, Copilot, DALL-E e Midjourney dependem desses LLMs para operar. Essas redes neurais adquirem conhecimento ao longo do tempo e produzem respostas em texto, imagem, vídeo e até mesmo em código de programação. Por outro lado, o ChatGPT é um sistema de IA gratuito que permite conversas envolventes, oferece insights e automatiza tarefas. Ele se baseia em um LLM com 175 bilhões de parâmetros, treinado em uma extensa base de dados, e é capaz de gerar textos sofisticados e aparentemente inteligentes.

Dessa forma, o ChatGPT é capaz de conduzir conversas cada vez mais naturais e sofisticadas com os usuários, adaptando-se ao contexto e respondendo a uma ampla gama de perguntas e solicitações. Sua capacidade de compreender a linguagem humana e gerar respostas relevantes o torna uma ferramenta valiosa não apenas para entretenimento, mas também para suporte ao cliente, educação e até mesmo assistência em tarefas complexas. Assim, o ChatGPT exemplifica como os LLMs estão transformando a maneira como interagimos com a tecnologia e exploramos o vasto universo de dados disponíveis.

No entanto, junto com os avanços e benefícios trazidos pelas máquinas de aprendizado e os LLMs, também surgem preocupações e riscos significativos. Um dos principais receios está relacionado à privacidade e segurança dos dados, especialmente em um contexto de Big Data, onde enormes quantidades de informações pessoais podem ser coletadas, armazenadas e analisadas sem o consentimento adequado dos usuários. Além disso, há preocupações éticas sobre o uso dessas tecnologias para manipulação de opiniões, disseminação de desinformação e até mesmo criação de conteúdo prejudicial, como deepfakes. Outro risco é a amplificação de preconceitos e discriminação, uma vez que os modelos de aprendizado de máquina podem reproduzir e até mesmo agravar viés presentes nos dados de treinamento. Portanto, é crucial que os desenvolvedores e usuários estejam atentos a

essas questões e implementem medidas adequadas para mitigar esses riscos enquanto aproveitam os benefícios oferecidos pela tecnologia.

Enfim, as soluções inteligentes que avançam e a enorme quantidade de dados disponíveis devem ser utilizadas por óbvio, não apenas como uma oportunidade, mas como uma necessidade. No entanto, é crucial avançar nessa direção de forma técnica e ética, a fim de evitar abusos e garantir a defesa dos direitos individuais. Por isso, já temos algumas iniciativas de regulamentação para garantir sua utilização responsável e a preservação dos direitos individuais (SARLET, 2022, p. 25). Por exemplo, no Brasil, várias medidas estão em curso nesse sentido. A Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, estabelece princípios para o tratamento de dados pessoais, cuja aplicação se estende também ao uso de dados na IA, apesar de não ser seu foco principal. A Autoridade Nacional de Proteção de Dados (ANPD) é a entidade encarregada de implementar a LGPD e promover uma cultura de proteção de dados no país, acompanhando de perto o debate sobre a regulamentação da IA. O Projeto de Lei nº 21/2020, já aprovado na Câmara dos Deputados e aguardando avaliação no Senado Federal, estabelece um marco legal para o desenvolvimento e uso da IA no Brasil, delineando princípios, direitos e deveres, enquanto o Projeto de Lei 2338/2023, em tramitação, busca estabelecer normas específicas para a IA, com foco em princípios como respeito à dignidade humana e proteção da privacidade. A Política Nacional de Inteligência Artificial (PNIA), lançada pelo governo brasileiro em 2023, define diretrizes para o desenvolvimento e uso da IA no país, reconhecendo a importância da proteção de dados e da ética. Na área da saúde, a regulação da IA demanda transparência na coleta de dados, gestão de riscos, validação externa de dados e proteção da privacidade.

No cenário global, diversas iniciativas também merecem destaque. O Regulamento Geral de Proteção de Dados (RGPD), em vigor na União Europeia desde 2018, é um marco abrangente na proteção de dados, incluindo disposições específicas para o tratamento de dados na IA. A Lei de Proteção de Dados Pessoais e Privacidade da Califórnia (CCPA), em vigor desde 2020, concede direitos aos consumidores californianos em relação aos seus dados pessoais, com disposições específicas para o uso de dados na IA. Além disso, diversas outras nações e organizações internacionais estão empenhadas em desenvolver iniciativas para regular a IA e proteger os dados, como as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e os princípios da UNESCO sobre IA. Em suma, várias nações estão adotando estratégias para promover o desenvolvimento da IA, envolvendo governos, indústrias e universidades.

5. Metodologia da bibliometria utilizada

A bibliometria é uma técnica essencial para medir índices que indicam a produção e disseminação do conhecimento científico (Fonseca, 1986, p. 73). Estes índices permitem a análise detalhada de um campo científico específico, revelando características como o crescimento temporal da produção científica, a produtividade de autores e instituições, a colaboração entre pesquisadores e instituições, o impacto das publicações, bem como a análise e avaliação das fontes de disseminação de trabalhos e a distribuição da produção científica em diversas fontes e temáticas. Esta análise pode revelar a evolução e tendências nesse campo (Bufrem & Prates, 2005, p. 12).

Para explorar esse tema, realizamos uma análise através do levantamento de artigos indexados no Google Acadêmico, uma base reconhecida pela sua amplitude e pela variedade de revistas que indexa. As buscas foram restritas aos títulos das publicações, utilizando os operadores OR e AND, Essas escolhas restringem os resultados, porém dão maior precisão aos mesmos.

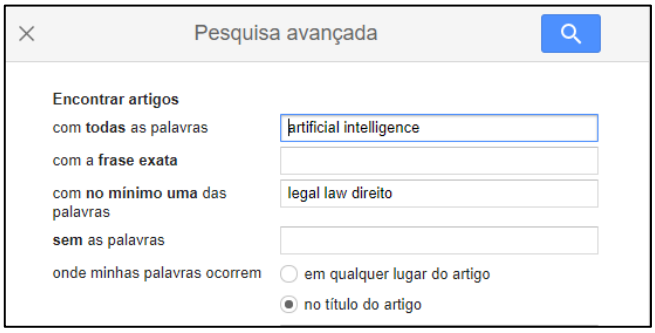

Figura 1. Janela da pesquisa avançada do Google Acadêmico

Dada a diversidade de palavras-chave, estas foram utilizadas de forma estratégica para organizar os resultados. As buscas foram conduzidas com dois polos: um principal, formado por termos equivalentes ligados pelo operador OR, e um secundário, composto por termos não equivalentes, exigindo uma busca distinta para cada um. A inclusão de termos no plural ampliou o espectro de estudos pertinentes ao tema.

Durante a análise dos resultados, não impusemos restrições temporais aos artigos. Quando os resultados eram escassos, repetições foram desconsideradas para evitar distorções.

As palavras-chave selecionadas abordam tanto os temas relativos à inteligência artificial quanto os relativos à proteção de dados pessoais.

6. Discussão dos resultados

A busca realizada (B1) teve como objetivo fornecer um panorama amplo da interação entre o Direito e os temas de inteligência artificial, Large language models e chatgpt. Para isso, as palavras-chave foram categorizadas em dois grupos: os termos principais que abrangem o Direito de forma geral (legal e law) e os termos secundários relacionados à inteligência artificial. As buscas foram conduzidas para cada termo secundário, combinando-os com os termos principais usando o operador AND. Foram utilizados exclusivamente termos em inglés.

legal OR law	
AND	*Total de artigos*
artificial intelligence	2300
Large language models	81
chatgpt	88

Figura 2. Busca B1

Os resultados quantitativos revelam que houve um grande número de retornos com o termo artificial intelligence, com os seis primeiros artigos apresentando mais de 100 citações cada, e os demais mantendo uma quantidade próxima. Esse achado indica um alto interesse na interseção dessas duas áreas. No entanto, é importante notar que esses resultados são relevantes apenas em termos de contexto, uma vez que os artigos mais citados apresentam uma visão bastante geral da relação entre as duas temáticas. Seria preciso uma análise dos demais artigos para identificar se especificam mais as temáticas.

Por outro lado, a análise do termo Large language models em relação ao Direito resultou em uma diminuição significativa nos retornos, mesmo assim um número alto de artigos. Além disso, o número de citações desses artigos é até razoável, entre 10 e 30. Isso sugere que a temática é mais específica e, portanto, há um interesse relativo nesse campo de estudo, embora não seja negligenciável. A maioria dos artigos exploram o papel e o potencial dos grandes modelos de linguagem na esfera jurídica, abordando diversos aspectos que vão desde a compreensão do conhecimento jurídico até a aplicação prática desses modelos. O primeiro texto discute o impacto do tamanho e do método de treinamento dos modelos de linguagem na sua performance, buscando identificar os aspectos mais influentes nesse desempenho. Em seguida, um outro estudo apresenta o ChatLaw, um modelo de linguagem jurídica desenvolvido especialmente para o contexto legal chinês, destacando a importância da qualidade dos dados para sua eficácia. Outro trabalho propõe o Legalbench, um benchmark colaborativo para medir o raciocínio jurídico em grandes modelos de linguagem, ressaltando como avanços nessa área estão levando profissionais do direito a reconsiderar suas práticas. Além disso, há uma análise sobre a integração dos grandes modelos de linguagem no campo jurídico, destacando seus resultados promissores em tarefas como análise de documentos legais e revisão de contratos. Um estudo mais específico examina as "ficções legais", ou seja, distorções na interpretação de fatos legais por parte desses modelos, enquanto outro destaca a emergência de capacidades de compreensão jurídica em evolução nos modelos de linguagem. Também são abordadas propostas para ensinar esses modelos a prever julgamentos legais, bem como desafios enfrentados por eles e métodos de avaliação. Finalmente, um estudo chinês apresenta um benchmark de modelos de linguagem jurídica, mostrando diferentes focos e aplicações dentro desse contexto. Esses trabalhos refletem um interesse crescente e multidisciplinar na interseção entre inteligência artificial e direito, explorando tanto os desafios quanto as oportunidades que essas tecnologias representam para a prática jurídica contemporânea.

Já a análise do termo chatgpt resultou também uma diminuição nos retornos, na mesma faixa do termo anterior. Além disso, o número de citações desses artigos é parecido com o caso anterior, ocorrendo entre 10 e 40 vezes. Da mesma forma acima, os artigos abordaram várias facetas da integração do ChatGPT no campo jurídico, revelando tanto as oportunidades quanto os desafios associados a essa tecnologia. Primeiramente, destaca-se a capacidade do ChatGPT de auxiliar professores de direito em tarefas comuns, demonstrando um desempenho positivo em prompts relacionados ao serviço, o que sugere que a ferramenta pode oferecer suporte próximo aos professores de direito. Em contrapartida, há uma discussão sobre os desafios legais e éticos decorrentes do uso de modelos de linguagem grandes, como o ChatGPT, incluindo preocupações com parrots estocásticos e alucinações, que podem impactar questões legais e sociais de maneira significativa. Outro artigo explora como o ChatGPT pode ser aplicado na educação jurídica e na prática, oferecendo exemplos de prompts e conselhos sobre seu uso. Também são discutidas implicações éticas e legais específicas do uso do ChatGPT na urologia, destacando a necessidade de considerar cuidadosamente os impactos éticos e legais ao integrar essa tecnologia em áreas

sensíveis. A pesquisa também aborda o papel do ChatGPT no campo jurídico, destacando suas possíveis utilidades para paralegais e assistentes jurídicos em diversas tarefas legais. Além disso, são examinadas as implicações do ChatGPT para a educação e prática jurídica, considerando como essa tecnologia pode influenciar o ensino e o exercício do direito. A discussão sobre inteligência artificial no contexto jurídico também levanta questões sobre a tomada de decisões legais e a autenticidade do ChatGPT em investigações forenses, evidenciando a necessidade de uma avaliação cuidadosa de sua aplicação. Por fim, são exploradas as implicações do ChatGPT para os serviços legais e a sociedade, destacando seu potencial como ferramenta valiosa, mas também ressaltando a importância de considerar questões éticas e legais ao implementá-lo.

Inteligência artificial	
AND	*Total de artigos*
proteção de dados	10
privacidade	41

Figura 3. Busca B2

Em seguida fizemos buscas mais focadas. A busca B2 relacionou o termo principal inteligência artificial com os secundários proteção de dados e privacidade, todos os termos em português.

O termo, proteção de dados, resultou 10 artigos, mostrando ser pequena a amostragem e com poucas citacoes. Quanto a análise dos titulos dos artigos, ficou evidente a interconexão entre os conceitos de Direitos Humanos, inteligência artificial e privacidade em diversos contextos. Os artigos abordam temas que vão desde os riscos e implicações da inteligência artificial e dos algoritmos para a privacidade, até questões específicas como a utilização da inteligência artificial no âmbito da saúde e seus limites em relação à privacidade dos pacientes. Além disso, há discussões sobre a relativização da privacidade em situações como a violência doméstica, onde se questiona a ponderação entre a garantia à integridade física e a preservação da privacidade dos envolvidos. A aplicação da inteligência artificial nas redes sociais também é explorada em relação à proteção da privacidade e dos dados pessoais dos usuários, destacando a importância de políticas de privacidade transparentes. Outros temas incluem os desafios enfrentados pela legislação de proteção de dados na era da inteligência artificial, especialmente em relação às violações de privacidade decorrentes do uso de robôs e das chamadas telefônicas automatizadas. A discussão sobre ética, transparência e responsabilidade no uso da inteligência artificial também é abordada em relação ao equilíbrio entre eficiência e privacidade na luta contra as fake news.

Já o termo privacidade, resultou 41 amostras, com 3 deles tendo algumas citacoes. Alguns estudos destacam o papel das leis gerais de proteção de dados como possíveis vetores para a regulamentação da inteligência artificial, investigando se o princípio da precaução, aliado à accountability e aos relatórios de impacto à proteção de dados, poderia ser o portal de entrada para essa regulamentação. Outros artigos focam na aplicação da Lei Geral de Proteção de Dados Pessoais como ponto de partida para a regulação da inteligência artificial em setores específicos, como a saúde, apontando para a necessidade de desenvolvimento de tecnologias e legislações que garantam a salvaguarda dos direitos individuais. Além disso, há estudos que exploram a relação entre a inteligência artificial, a proteção de dados pessoais e a responsabilidade na era digital, destacando a importância de conciliar o impacto da inteligência artificial sobre as pessoas com o respeito aos direitos fundamentais estabelecidos pela Constituição Federal. Ainda, há reflexões sobre os desafios suscitados pelo uso da inteligência artificial e do big data no contexto da COVID-19, especialmente no que diz respeito à proteção adequada dos dados pessoais e à alocação de responsabilidade por eventuais danos. Esses estudos também abordam a mudança de paradigma na proteção de dados e o uso da inteligência artificial a partir de um modelo constitucional, visando garantir a proteção dos direitos fundamentais envolvidos. Ademais, é discutido o papel da accountability e do direito fundamental à proteção de dados pessoais como limites ao uso da inteligência artificial na relação de emprego, enfatizando a necessidade de mecanismos que garantam a transparência e a prestação de contas no tratamento automatizado de dados.

Artificial intelligence	
AND	*Total de artigos*
data protection	144
privacy	354

Figura 4. Busca B3

Na busca B3, foram utilizados exclusivamente termos em inglês, sendo o termo principal "artificial intelligence" e os secundários "data protection" e "privacy".

O termo "data protection" resultou em 144 artigos, sendo os primeiros 10 muito citados (de 20

a 50 citações). Estes 10 artigos destacam várias questões, como a crescente importância da regulação da inteligência artificial (IA), especialmente no contexto da proteção de dados pessoais. Um dos debates examina a relação entre o Regulamento Geral de Proteção de Dados (GDPR) e a IA, evidenciando preocupações sobre a capacidade do GDPR em lidar eficazmente com os avanços rápidos e significativos na IA. Outra discussão sobre a ética na governança de TI e a aplicação de modelos de governança legal, como o GDPR, revela a necessidade de uma abordagem abrangente que leve em consideração as especificidades da IA e da proteção de dados. Além disso, há uma análise sobre como a IA e o big data apresentam novos desafios para a proteção de dados, uma vez que permitem previsões sobre terceiros com base em dados anônimos. Esses artigos destacam a urgência de uma abordagem multidisciplinar e colaborativa para lidar com as interseções entre IA, proteção de dados e cibersegurança, a fim de garantir um quadro legal eficaz e ético.

Já o termo "privacy" resultou em 354 amostras, sendo os 10 primeiros muito citados (de 100 a 300 citações). É notável que este termo desperta grande interesse na interseção entre privacidade e inteligência artificial (IA). Os artigos abordam diversos contextos, incluindo saúde, destacando técnicas e aplicações para preservar a privacidade dos dados. Há também discussões sobre privacidade e IA, enfatizando a importância de garantir a segurança dos dados em um cenário de crescente uso de algoritmos de IA. Uma abordagem específica sobre privacidade na área da saúde ressalta os desafios adicionais enfrentados ao lidar com informações sensíveis dos pacientes. Ao explorar os riscos associados à IA para a privacidade, os textos apontam como a prática da IA pode afetar diretamente a segurança dos dados pessoais, levantando preocupações sobre potenciais violações e uso inadequado das informações. Além disso, discute-se os riscos para a privacidade e a democracia, destacando as implicações mais amplas do uso da IA na manipulação de informações e influência em processos democráticos. Por fim, ao mencionar a aplicação de técnicas como a privacidade diferencial em IA, os textos sugerem abordagens para mitigar os riscos à privacidade, evidenciando a necessidade contínua de inovação e pesquisa nesse campo para equilibrar os avanços tecnológicos e a proteção dos direitos individuais.

A busca B4 explorou a interconexão entre o termo central "machine learning" e os conceitos secundários de "data protection" e "privacy", ambos discutidos anteriormente. Surpreendentemente, apesar da natureza altamente específica dessas áreas, os resultados foram extensos. Isso ressalta a distinção marcante entre "machine learning" e "inteligência artificial", onde o primeiro é notavelmente mais preciso, uma distinção que tem implicações significativas.

machine learning	
AND	*Total de artigos*
data protection	68
privacy	1130

Figura 5. Busca B4

Começando com "data protection", a busca resultou em 68 artigos. Os principais temas abordados nesses artigos variam desde a implementação do Regulamento Geral de Proteção de Dados (GDPR) de 2016 até questões cruciais sobre conformidade legal sem prejudicar a precisão das análises, especialmente em setores sensíveis como a pesquisa médica. Outros temas incluem a Privacidade por Design como uma abordagem essencial para equilibrar insights úteis e proteção de dados, além do potencial do aprendizado de máquina federado para compartilhamento de dados entre instituições, respeitando os requisitos de privacidade. No entanto, destaca-se a lacuna entre a regulamentação de proteção de dados e a prática dos algoritmos de aprendizado de máquina, apontando para a necessidade de uma definição mais precisa de dados e informações para uma regulamentação mais eficaz. Também é levantada a questão da soberania cognitiva e a crescente preocupação com o rastreamento e perfilamento de indivíduos.

Quanto ao termo "privacy", os resultados foram ainda mais impressionantes, com 1130 amostras identificadas. A alta quantidade de citações desses artigos destaca a forte ligação entre o aprendizado de máquina e a privacidade, evidenciando a relevância dessa discussão. Os temas abordados incluem a integração de técnicas de privacidade no aprendizado de máquina, uma revisão da literatura existente sobre privacidade nesse domínio, ataques à privacidade em modelos de aprendizado de máquina, propostas de serviços que preservam a privacidade dos dados dos usuários, segurança e privacidade no contexto do aprendizado de máquina, e ameaças potenciais à privacidade, soluções propostas e desafios futuros nesse campo em constante evolução.

É notável que os aspectos puramente jurídicos e regulatórios não sejam predominantes nesses resultados, sugerindo que a ênfase está na

adoção de práticas estabelecidas e reconhecidas. No entanto, a confirmação dessa hipótese requer uma análise completa dos artigos em estudos futuros.

large language model OR chatgpt	
AND	Total de artigos
data protection	7
privacy	81

Figura 6. Busca B5

A análise B5 examinou a relação entre os termos "large language models" ou ChatGPT, considerados sinônimos nesta discussão, e os termos "data protection" e "privacy", abordados separadamente. Dada a distinção jurídica entre os termos, as amostras obtidas foram notavelmente distintas.

Em relação a "data protection", apenas sete artigos foram encontrados, com poucas citações, exceto pelo primeiro, que obteve 20 citações. Estes artigos exploram várias perspectivas, começando com a proteção de dados em chatbots baseados em inteligência artificial, especialmente o ChatGPT da OpenAI. Outras preocupações incluem o impacto dos grandes modelos de linguagem, como o ChatGPT, na segurança dos dados dos usuários, desafios e oportunidades para legisladores alemães na balança entre proteção de dados e uso do ChatGPT, e o impacto do ChatGPT nas leis de privacidade e proteção de dados, destacando questões específicas para garantir conformidade e melhorias na privacidade. Além disso, avalia-se se o ChatGPT está influenciando efetivamente as preocupações com segurança cibernética e proteção de dados em diferentes regiões, como a União Europeia, os EUA e a China. Também são explorados os princípios de proteção de dados, especialmente em relação ao GDPR, com os quais o ChatGPT está em conformidade. Por fim, discute-se técnicas de marca d'água em dados de texto em grandes modelos de linguagem para proteger direitos autorais dos conjuntos de dados e garantir a privacidade dos usuários.

Quanto ao termo "privacy", os resultados foram mais substanciais, com 81 amostras identificadas. Os cinco primeiros artigos foram citados entre 40 e 160 vezes, enquanto os demais tiveram até 10 citações. Os primeiros artigos abordam diversas questões relacionadas ao uso do ChatGPT, com menção limitada às LLMs. O primeiro tópico discute sustentabilidade, avaliando o impacto ambiental e a viabilidade a longo prazo dessas tecnologias. Em seguida, a privacidade é destacada, com foco nas ameaças à privacidade decorrentes do uso desses sistemas, especialmente em relação à coleta e uso de dados pessoais. A divisão digital é mencionada como um fator que pode agravar disparidades sociais e econômicas. Por fim, questões éticas são levantadas, ressaltando a importância de considerações morais ao desenvolver e implantar sistemas de IA, especialmente aqueles que afetam diretamente a interação humana. Esses temas destacam a necessidade urgente de avaliação contínua e aprimoramento em todas as áreas mencionadas para garantir que o progresso tecnológico seja equitativo, sustentável, respeite a privacidade e seja ético.

É relevante observar que os aspectos puramente jurídicos e regulatórios são abordados de maneira genérica, com foco nos aspectos técnicos.

7. Considerações finais

A presente pesquisa teve como objetivo realizar um mapeamento quantitativo das publicações científicas sobre inteligência artificial, machine learning e large language model (LLM) em relação à privacidade e proteção de dados. Utilizou-se uma abordagem bibliométrica, priorizando buscas nos títulos das publicações e cruzando termos de maneiras diversas para avaliar a frequência dessas relações e seu significado qualitativo. Alguns resultados foram qualitativamente apresentados.

Os achados revelaram um avanço significativo na discussão científica desses temas técnicos em conexão com questões regulatórias e normativas. As publicações em língua inglesa foram o foco principal, com uma busca limitada em termos em português, resultando em um retorno ainda restrito.

Na relação entre a inteligência artificial e o direito os resultados demonstram que são temas já consolidados, destacando-se a análise dos desafios enfrentados pela legislação, especialmente diante do rápido avanço tecnológico, a relevância da Privacidade por Design e a importância de abordagens multidisciplinares para lidar com questões de cibersegurança e proteção de dados.

Já nos artigos relacionados ao aprendizado de máquina e sua relação com a proteção de dados e privacidade, embora mais restritos, também obtiveram bons resultados. Um pouco menos a relaçãco com os "Large Language Models" e o "ChatGPT", indicando um espaço importante de discussão ainda em aberto. Emergem aqui preocupações como alucinações e a necessidade de assegurar transparência e responsabilidade no

emprego dessas tecnologias. Preocupações éticas e legais são ainda bem gerais e não são predominantes, sugerindo que a ênfase está na discussão de temas mais práticos e técnicos.

Como é obvio, nossa conclusão não é geral e diz respeito apenas aos artigos mais citados. Em estudos futuros seria possível avançar para uma análise mais completa de todos artigos recuperados. Espera-se que os resultados deste estudo contribuam para a disseminação e mapeamento desses temas, apontando para um amplo campo de novas e futuras pesquisas nessa área interdisciplinar.

Referencias

Assunção, Luís. Machine learning, big data e inteligência artificial. I// Lex Machinae. https://www.lexmachinae.com/2017/12/08/machine-learning-big-data-e-inteligencia-artificial-qual-o-be.

Beck, Ulrich; Zolo, Danilo (2022). A sociedade global do risco. // Prim@ Facie. 1: 1, 18-29.

Bufrem, L.; Prates, Y. (2005). O saber científico registrado e as práticas de mensuração da informação. // Ciência da Informação. 34:2, 9-25, 2005.

Castells, Manuel (1999). A sociedade em rede. São Paulo: Paz e Terra.

Fonseca, E. N. (1986). Bibliometria: teoria e prática. São Paulo: Cultrix, Ed. da USP.

Gehlen, Arnold (1980). Man in the Age of Technology. New York: Columbia Univ. Press.

Medeiros, Nelma (2003). O Homem Pós-Orgânico: Quarta Ferida Narcísica? // Novamente Revista. 4/5, 247-252.

Minsky, M. (1985). The Society of Mind. New York, USA: Touchstone.

Ribeiro, Claudio José Silva (2014). Big Data: os novos desafios para o profissional da informação. // Informação & Tecnologia (ITEC). 1:1, 96-105.

Rover, Aires J. (2001). Informática no direito: inteligência artificial: introdução aos sistemas especialistas legais. Juruá Editor.

Rover, Aires José; Melo, Marco A M Ferreira de (1995). Perspectivas do uso da Internet no curso de direito. In: Revista seqüência.30, 65-79.

Sarlet, Ingo Wolfgang (2022). Inteligência Artificial, Proteção de Dados Pessoais e Responsabilidade na Era Digital. Série Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação. eBook Kindle, 2022.

Enviado: 2024-05-06. Segunda versión: 2024-05-23.
Aceptado: 2024-05-23.