A interseção entre a Inteligência Artificial e a Privacidade de Dados: conformidade com a LGPD e segurança da informação

Camila Melo Franco Gonçalves Motta[1]

Resumo: Este artigo investiga a interseção entre a inteligência artificial (IA) e a privacidade de dados, concentrando-se na conformidade com a Lei Geral de Proteção de Dados (LGPD) e na garantia da segurança da informação. Explora-se o potencial da IA para melhorar processos em diversos setores, ao mesmo tempo em que se consideram os riscos associados à violação da privacidade e discriminação. São discutidos temas como transparência no uso de algoritmos, consentimento informado, minimização de dados e justiça algorítmica. Além disso, são examinadas medidas de segurança da informação, como políticas robustas, criptografia e gerenciamento de riscos, necessárias para proteger dados pessoais contra violações e ataques cibernéticos. Por fim, aborda-se a importância da representação do conhecimento na concepção de sistemas de IA compatíveis com a LGPD e práticas para auditoria e monitoramento da conformidade regulatória. Este artigo visa oferecer insights sobre como conciliar avanços em IA com a proteção da privacidade de dados e a segurança da informação.

Palavras-chave: Inteligência Artificial, Privacidade de Dados, LGPD, Segurança da Informação, Conformidade.

The intersection between Artificial Intelligence and Data Privacy: LGPD compliance and information security

Abstract: This article investigates the intersection between artificial intelligence (AI) and data privacy, focusing on compliance with the General Data Protection Act (GDPR- LGPD) and ensuring information security. The potential of AI to improve processes in various sectors is explored, while at the same time the risks associated with breaches of privacy and discrimination are considered. Topics such as transparency in the use of algorithms, informed consent, data minimization and algorithmic justice are discussed. In addition, information security measures are examined, such as robust policies, encryption and risk management, which are necessary to protect personal data from breaches and cyber-attacks. Finally, the importance of knowledge representation in the design of GDPR-compliant AI systems and practices for auditing and monitoring regulatory compliance are addressed. This article

[1] Advogada graduada pela Faculdade de Direito Milton Campos, pós-Graduada em Direito Público, com MBA em Negócios Internacionais pela FGV, especialista em Proteção de dados, Investigação e ESG pela LEC. Presidente da Comissão de Compliance da OAB/MG 2022/2024. Head do Núcleo de Compliance do escritório Geraldo Néry Lopes Advogados. Membra do Conselho de Combate à Corrupção de MG, coordenadora da Câmara de Integridade Professora de pós-graduação da ESA/CEDIN.camilamelo-franco@gmail.com.

aims to offer insights into how to reconcile advances in AI with data privacy protection and information security.

Keywords: Artificial Intelligence, Data Privacy, LGPD, Information Security, Compliance.

1 INTRODUÇÃO

Nas últimas décadas, o avanço da tecnologia da informação e, em especial, da inteligência artificial (IA), tem promovido significativas transformações econômicas e sociais. A aplicação de IA nos mais diversos setores promete revolucionar processos e otimizar o uso de recursos. Entretanto, este avanço ocorre em um ambiente desafiador, onde a proteção da privacidade dos dados torna-se crucial, especialmente sob a égide da Lei Geral de Proteção de Dados (LGPD).

"O mundo nos é oferecido sem concessões" (MAGRANI; EDUARDO, 2019, p. 11). Essa frase nos lembra que o mundo está lá, à nossa disposição, sem restrições ou limitações impostas por outros. É como se a própria existência nos convidasse a explorar, a descobrir e a viver plenamente. A inteligência artificial, embora seja uma área de grande potencial e inovação, não é um mundo sem restrições ou limitações. Contudo, um dos grandes desafios contemporâneos é a perseguição vagarosa do Direito na busca da solução prudente ao franco e lépido desenvolvimento tecnológico.

O combo internet das coisas, big data e inteligência artificial, certamente têm transformado e ainda transformará muito a sociedade. A consequência de tudo isso ainda não alcançamos. Pensar e discutir sobre o tema é urgente, mas não finito.

Nesse cenário, este artigo tem como objetivo analisar essa interseção, destacando tanto as oportunidades quanto os riscos envolvidos, além de abordar medidas imprescindíveis para a conformidade e segurança da informação.

2 INTELIGÊNCIA ARTIFICIAL E SEUS IMPACTOS

Hoje a inteligência artificial é uma realidade tão presente que muitas vezes sequer nos damos conta de que interagimos com ela a todo tempo. Quando usamos a TV, quando acessamos nossas redes sociais, em uma compra com cartão de crédito, quando entramos em um prédio, em nossos cadastros na internet etc.

Lidar com a Inteligência Artificial parece-nos, hoje, um caminho sem volta, mas não a qualquer custo.

Em um compilado de estáticas de pesquisas pelo mundo, obtidas pela *Grand View Research*, PWC, *McKinsey Global Institute*, IBM, entre outros, a Hostinger publicou em seu site[2] alguns dados importantes e que merecem destaque:

> "1. Estima-se que o tamanho do mercado global de IA cresça 37% anualmente de 2023 a 2030.
>
> A tecnologia de IA não é apenas modismo: ela veio para ficar, pelo menos como uma ferramenta útil. Usar a IA para automatizar tarefas repetitivas permite que você se concentre em tarefas mais complexas e criativas.
>
> Para líderes de negócios, a adoção da automação impulsionada por IA leva a ganhos imediatos na produtividade. Entender como trabalhar com as ferramentas de IA pode também te tornar um funcionário indispensável na empresa que você trabalha.
>
> (...)
>
> 3. A IA Poderá Contribuir com Mais de US$ 15 Trilhões para a Economia Mundial até 2030.
>
> Essas estatísticas de crescimento da IA provam que o investimento em aprendizado de máquina é bastante lucrativo. Por isso, empresas devem investir em iniciativas voltadas à IA se quiserem se manter à frente da concorrência.
>
> Já para pessoas físicas, isso significa que praticamente todos os setores vão implementar a IA em um dado momento. Ficar por dentro do uso da IA no seu setor — seja agricultura, setor financeiro ou manufatura — pode proporcionar insights valiosos para fazer escolhas de carreira e tomar decisões de investimento mais inteligentes.
>
> (...)
>
> 6. Na China e na Índia, a Adoção da IA já é superior a 40%
>
> (...)

[2] Disponível em: https://www.hostinger.com.br/tutoriais/estatisticas-inteligencia-artificial?utm_campaign=Generic-Tutorials-DSA|NT:Se|LO:BR-t3&utm_medium=ppc&gad_source=1&gclid=Cj0KCQjw9vqyBhCKARIsAIIcLMEUd9LWy894O2Wezno-jgj5pFwINd7h0G-r3oGS0ckArdaio3y-hCgMaAsLmEALw_wcB Acesso em 04 de junho de 2024.

7. 25% das Empresas Adotaram a IA para Suprir a Escassez de Mão de Obra

(...)

9. O Financiamento Global da IA Atingiu US$ 45 Bilhões em 2022

Está claro que a confiança do mercado na IA está aumentando.

Para empresários, esse número indica que o momento para inovação em tecnologia de IA é agora, com amplo financiamento disponível. Já para profissionais que trabalham no mercado de IA, altos níveis de investimento frequentemente se traduzem em segurança no emprego e oportunidades para crescimento na carreira.

(...)

12. A Demanda por Habilidades em IA está Superando a Oferta de Talentos em IA

Há uma nítida lacuna entre a demanda por habilidades de IA e a disponibilidade atual de talentos.

Para as empresas, isso sugere que será cada vez mais concorrido atrair e reter trabalhadores qualificados em IA. Para as pessoas, a escassez de pessoas especializadas em IA sinaliza uma oportunidade lucrativa – adquirir habilidades em IA significa estabilidade no emprego e avanço na carreira.

(...)

14. 30% das Horas Trabalhadas em Todo o Mundo Poderão ser automatizadas com a IA até 2030

(...)

15. Mais de 95% dos Executivos Concordam que a IA Gerativa vai Revolucionar Onde e Como a IA será usada

(...)

16. Mais de 60% dos Estadunidenses estão preocupados com o Viés da IA e a Possível Discriminação durante o Processo de Contratação

(...)

25. Estima-se que o Setor de Inteligência Artificial Valerá US$ 190 Bilhões até 2030

O valor de mercado previsto para o setor de IA sugere que inteligência artificial se espalhará por diversos outros setores.

Isso significa que as empresas, independentemente do seu tamanho ou setor, precisam pensar em integrar a IA em seus planos ope-

> racionais e estratégicos. Para as pessoas, isso significa que entender a IA está se tornando uma necessidade na vida cotidiana e no trabalho.
>
> (...)"

Fato é que essa evolução é iminente e inafastável para todos nós, seja no trabalho ou na vida pessoal, e como disse Jeff Bezos, perigoso é não evoluir. Construir racionais sobre limites e controles, além do desenvolvimento de uma cultura de ética na condução e desenvolvimento de IA é essencial.

Não à toa que a *Fundación del Español* Urgente (FundéuRAE), promovida pela Real Academia Española e pela Agência EFE, escolheu a "palavra do ano" para 2022: inteligência artificial[3].

Para melhor entendimento é necessário a contextualização e conceituação do tema.

2.1. Conceito

A tentativa de entender a inteligência artificial envolve o esforço de defini-la. Entretanto, essa é uma tarefa desafiadora, já que não existe uma definição universalmente aceita e a própria conceituação da inteligência pode ter diversos significados.

O termo Inteligência Artificial foi gravado por John McCarthy, como título de uma Conferência de Dartmouth, realizada em 1956. Porém, um pouco antes, em 1950 Allan Turing escreveu um artigo a partir da necessidade de resposta para: *as máquinas podem pensar? "can machines think?"*[4] iniciando uma discussão bem fundamentada sobre o tema.

[3] TN. La Real Academia Española eligió a la "palabra del año": cuál es y por qué fue la ganhadora.29 dez. 2022. Disponível em: https://tn.com.ar/sociedad/2022/12/29/la-real-academia-espanola-eligio-a-la-palabra-del-ano-cual-es-y-por-que-fue-la-ganadora/. Acesso em: 04 de junho de 2024.

[4] TURING, Alan. Computing Machinery and Intelligence. Mind 49, 433-460, 1950

Para tanto, ele desenvolveu o "Teste de Turing" que coloca ênfase na capacidade da máquina de se comunicar de forma convincente e natural, simulando uma inteligência humana[5], em um Jogo da Imitação.

Ou seja, a IA se estruturou como um braço da computação, quando seu foco era de desenvolver programas computacionais capazes de automatizar ações inteligentes.

McCarthy (2007, p. 2) orginalmente diz que:

> "It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.[6]"

Em um artigo escrito para a Revista Cacto – Ciência, Arte, Comunicação em Transdisciplinaridade Online, do Instituto Federal Sertão Pernambuco[7], eles citam:

> "A inteligência artificial pode ser então considerada algo artificial capaz de pensar ou agir, ou ambos, de forma racional, como o ser

5 Basicamente o funcionamento do Teste de Turing é: Três Participantes: o teste envolve três participantes: um ser humano (o interrogador), uma máquina e outro ser humano. O interrogador é encarregado de manter uma conversa escrita com ambos, mas não sabe qual é qual.

Comunicação por Escrito: a comunicação entre o interrogador e as entidades (a máquina e o ser humano) é feita por escrito, geralmente por meio de um computador.

Objetivo: o objetivo do teste é determinar se a máquina pode manter uma conversa de tal maneira que o interrogador não consiga distinguir qual entidade (a máquina ou o ser humano) está respondendo.

Perguntas e Respostas: o interrogador faz uma série de perguntas às duas entidades, que respondem às perguntas também por escrito. As respostas das entidades são baseadas em texto, e o interrogador deve avaliar a qualidade das respostas para determinar qual entidade está gerando as respostas.

Aprovação: se o interrogador não conseguir determinar corretamente qual entidade é a máquina e qual é o ser humano com base em suas respostas, a máquina é considerada aprovada no Teste de Turing. Isso sugere que a máquina foi capaz de simular um comportamento inteligente indistinguível daquele de um ser humano na conversa escrita.

https://blog.pareto.io/teste-de-turing/#:~:text=O%20teste%20foi%20projetado%20para,natural%2C%20simulando%20uma%20intelig%C3%AAncia%20humana. Acesso feito em 04 de junho de 2024.

6 Tradução livre pelos autores: É a ciência e a engenharia que consiste em criar máquinas inteligentes, especialmente programas de computador inteligentes. Está relacionada com a tarefa semelhante de utilizar computadores para compreender a inteligência humana, mas a IA não tem de se limitar a métodos que são biologicamente observáveis.

7 BARBOSA, Pablo; CAMACHO, Rafael; SILVA, Cindy. Dilemas Éticos envolvidos no desenvolvimento da Inteligência Artificial. Revista Cacto-Ciência, Arte, Comunicação em Transdisciplinaridade Online, v. 4, n. 1, p. e24010-e24010, 2024. Acesso em 31 mai. 2024.

> humano ou como John McCarthy até disse na conferência de Dartmouth em 1956, "fazer a máquina comportar-se de tal forma que seja chamada inteligente caso fosse este o comportamento do ser humano".

O propósito era dotar as máquinas, por meio de programação, de inteligência suficiente para resolver problemas que não tinham sido submetidos antes.

A ideia é a conceituação da IA com base na inteligência humana na resolução de problemas, mas não limitada a ela.

O Parlamento Europeu define IA[8] em três etapas:

> "(1)IA é a capacidade de uma máquina exibir capacidades semelhantes às humanas, como raciocínio, aprendizagem, planejamento e criatividade.
>
> (2)A IA permite que os sistemas técnicos percebam o seu ambiente, lidem com o que percebem, resolvam problemas e atuem para atingir um objetivo específico. O computador recebe dados – já preparados ou recolhidos através dos seus próprios sensores, como uma câmara –, processa-os e responde.
>
> (3)Os sistemas de IA são capazes de adaptar o seu comportamento até certo ponto, analisando os efeitos de ações anteriores e trabalhando de forma autônoma."

Patrick Henry Winston[9], caracteriza como o campo da computação que permite a um sistema realizar percepções, raciocínios e ações.

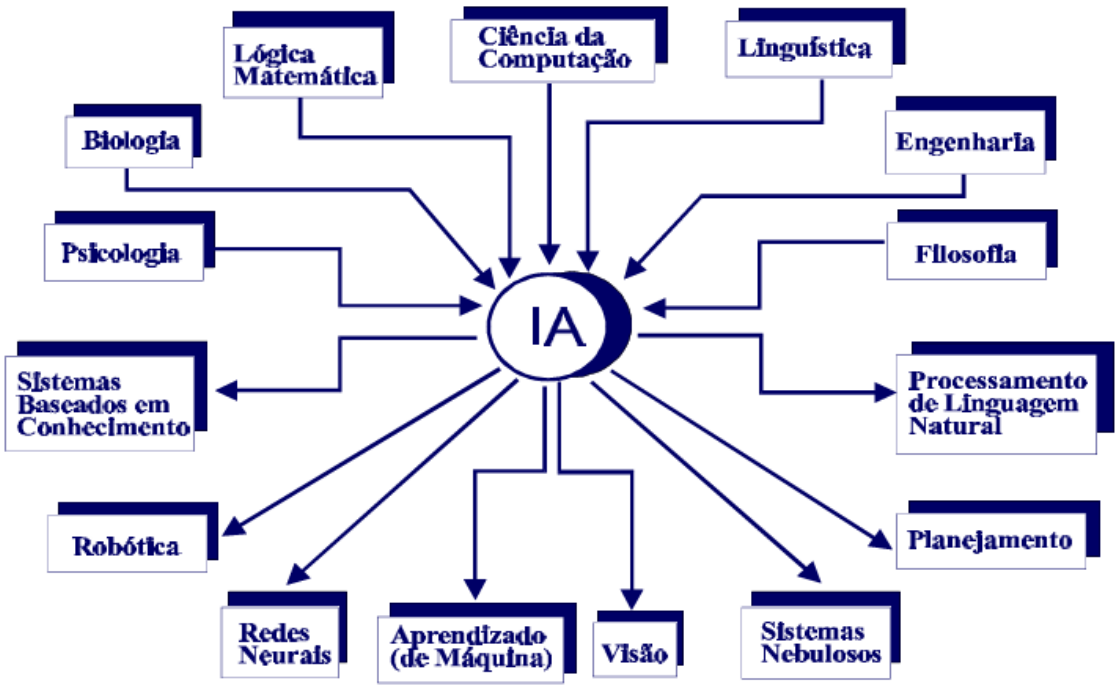
Segundo José Augusto Baranauskas[10] (2000) a IA é um ramo da ciência da Computação que busca fazer os computadores pensarem ou se comportarem de forma inteligente, relacionando-se com psicologia, biologia, lógica matemática, linguística, engenharia, filosofia, entre outras áreas científicas, conforme abaixo:

8 European Parliament News. What is artificial intelligence and how is it used? Parlamento Europeu, 4 de setembro de 2020. Disponível em: https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

9 WINSTON, Patrick Henry. Artificial Intelligence. 3rd edition, Massachussets: Addison-Wesley Publishing Company, 1993, p. 5.

10 MONARD, Maria Carolina e BARANAUSKAS, José Augusto. Aplicações de inteligência artificial: uma visão geral. 2000, Anais. São Paulo: Faculdade SENAC de Ciências Exatas e Tecnologia, 2000. Acesso em 11 de junho de 2024.

Figura 1 – Áreas relacionadas com a Inteligência Artificial



Fonte: MONARD; BARANAUKAS, 2000, p. 2

Os principais pontos conceituais da Inteligência Artificial são, sem dúvida, a experimentação e o aprendizado, por meio de uma base de dados. E esse tema nos exige falar de um outro conceito: aprendizado de máquina ou machine learning.

> "O *maching learning* é operado através de um algoritmo, que é comumente descrito como um conjunto de instruções, organizadas de forma sequencial, que determina como algo deve ser feito. Todo algoritmo tem uma entrada (input), e uma saída (output): os dados entram no computador, o algoritmo faz o que precisa com eles, e um resultado é produzido. Na técnica de machine learning, por outro lado, os dados entram no computador, e o algoritmo cria outros algoritmos; assim, através dessa técnica, os computadores escrevem seu próprio programa. Não existem regras definidas que serão codificadas no software, mas o sistema aprende suas decisões utilizando algum tipo de modelo estatístico, geralmente, a partir de exemplos, com base em um conjunto de dados que são apresentados para a máquina. Quanto maior a quantidade e qualidade dos dados disponibilizados ao algoritmo, maior a chance de o resultado estar próximo do real. Por isso a importância do Big Data e da coleta massiva de dados para o desenvolvimento da IA. Através da técnica de machine learning, portanto, os processos decisórios com base em IA são dotados de autonomia. Essa característica se distingue da automação, em que um processo é repetido pela máquina, e se refere à habilidade de autoaprendizagem com base nas experiên-

> cias que adquiriu. Antes dessa tecnologia, a programação de computadores resumia-se ao processo de descrever, detalhadamente, todas as etapas necessárias para que um computador realizasse determinada tarefa e alcançasse um determinado objetivo. Por outro lado, pela técnica de machine learning, os programas de computador têm a capacidade de serem criativos e desenvolverem, eles próprios, a habilidade de desempenhar ações e chegar a resultados que os seus criadores não eram capazes de alcançar ou de prever, com a ferramenta de IA podendo atuar de forma diferente em uma mesma situação, a depender da sua performance anterior, o que é muito parecido com a experiência humana. Desse modo, a solução encontrada pela IA pode não ter sido prevista nem mesmo pelo humano que a projetou."[11]

Então, machine Learning, ou aprendizado de máquina, é um subcampo da inteligência artificial que se concentra no desenvolvimento de algoritmos e técnicas que permitem aos computadores aprender a partir de dados e tomar decisões ou fazer previsões com base nesses dados. Em vez de serem programados explicitamente para realizar uma tarefa, os sistemas de machine learning são treinados usando grandes conjuntos de dados e algoritmos que os ajudam a identificar padrões e a melhorar seu desempenho ao longo do tempo. Existem diferentes tipos de aprendizado de máquina, incluindo aprendizado supervisionado, não supervisionado e por reforço, cada um com suas próprias abordagens e aplicações.

2.2. Potencial da IA em Diversos Setores

A IA tem sido instrumento de melhorias significativas em setores como saúde, finanças e comércio. Na área da saúde, por exemplo, sistemas baseados em IA podem diagnosticar doenças com maior precisão e rapidez. No setor financeiro, modelos preditivos ajudam a identificar fraudes e a otimizar investimentos. No comércio, a personalização de ofertas e a análise de comportamento do consumidor são impulsionadas por algoritmos complexos.

Em uma pesquisa global realizada pela McKinsey & Company em dezembro de 2022, os números que demonstram o estado da IA em 2022 chamam nossa atenção, inclusive quanto à exponencial expansão.

---

[11] MELO, Gustavo Da Silva. Inteligência artificial e responsabilidade civil: uma análise do anteprojeto do marco legal da inteligência artificial e do projeto de lei 2338/2023 Revista IBERCv. 7, n.1, p. 49-65, jan./abr. 2024www.responsabilidadecivil.org/revista-iberc DOI: https://doi.org/10.37963/iberc.v7i1.271

O uso da IA desde 2017 em pelo menos uma área de operação aumentou 150%, atingindo o pico em 2019, quando 58% dos participantes afirmaram ter adotado IA em pelo menos uma área de suas operações.[12]

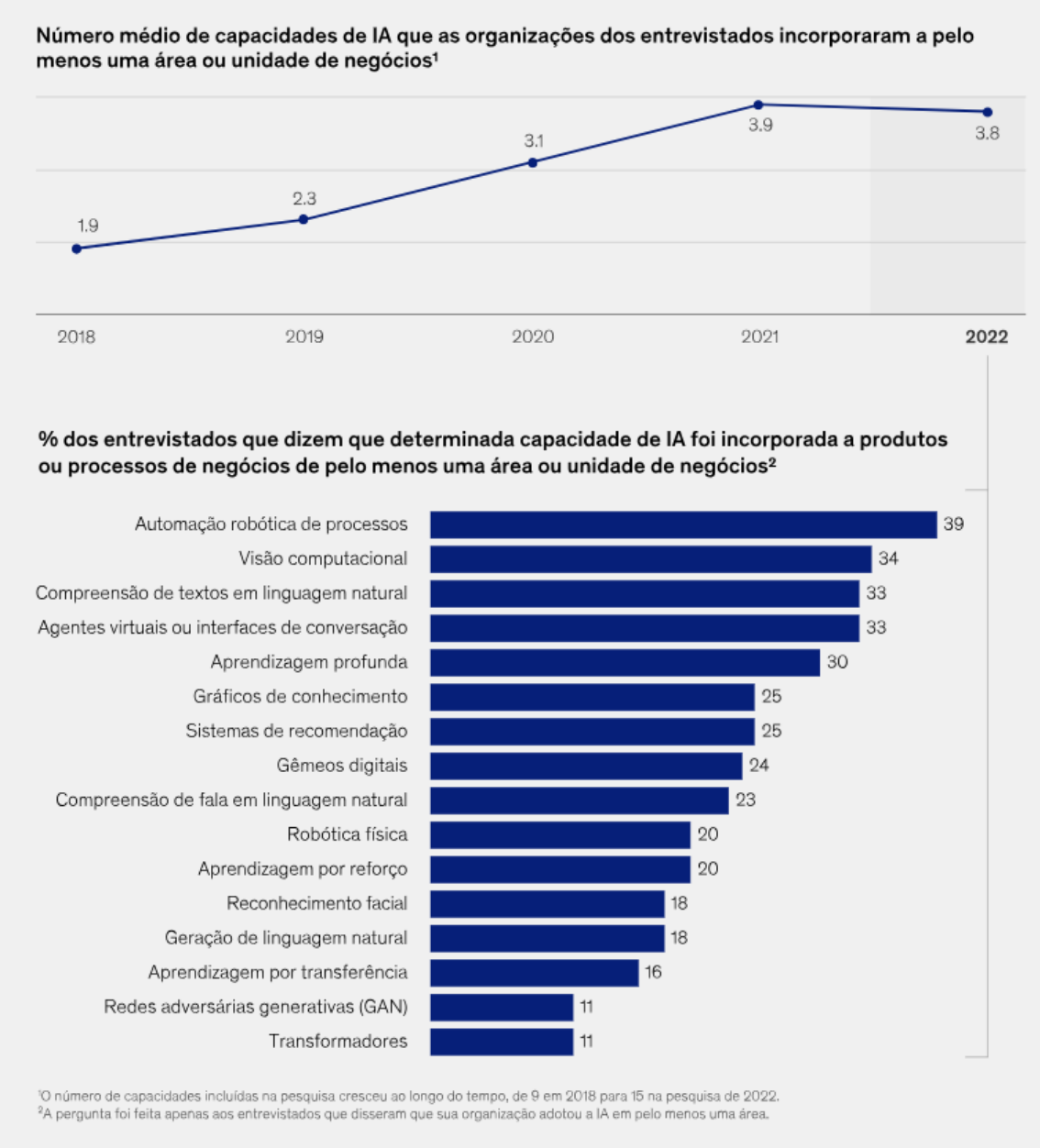
Figura 2 – Proporção de entrevistados que dizem que sua organização adotou a IA em pelo menos uma área, %.

Fonte: Mckinsey & Company (2022)

Ainda, houve um considerável aumento em relação ao número médio de capacidades de Inteligência Artificial usados nas organizações, incorporada à produtos ou processos de negócios.

[12] https://www.mckinsey.com/featured-insights/destaques/o-estado-da-ia-em-2022-e-meia-de-cada-passada-em-revista/pt. Acesso em 04 de junho de 2024.

Figura 3 – Número médio da capacidade de IA que as organizações dos entrevistados incorporaram a pelo menos uma área ou unidade de negócios.



Fonte: Mckinsey & Company (2022)

Outro importante dado obtido e que corrobora o uso da IA em diversas áreas de negócio foram:

Figura 4 – Casos de uso de IA mais adotados em cada área de negócio

Fonte: Mckinsey & Company (2022)

Há inúmeros textos, artigos, publicações em jornais na internet que discorrem sobre a atuação, impacto e uso da IA nas mais diversas áreas: na saúde (radiologia, oncologia, saúde suplementar etc.), no setor público (inclusive nos concursos públicos), setor financeiro, no direito, nos negócios, na indústria e outros mais.

A influência revolucionária das tecnologias de Inteligência Artificial (IA) é inquestionável. Tanto no âmbito da inovação, quanto na automação de tarefas, no incremento da eficiência ou na diminuição de despesas, os benefícios proporcionados pela implementação da IA são variados e abrangem muitos setores diferentes.

2.3. Riscos Associados à Violação da Privacidade de dados pessoais

O uso extensivo de IA não está isento de riscos. Os sistemas de IA podem exacerbar problemas de privacidade, pois manipulam grandes quantidades de dados pessoais. Além disso, há o risco de que algoritmos perpetuem discriminações, prejudicando grupos minoritários.

O Reino Unido tem sido protagonista em Inteligência Artificial criando um Comitê de Inteligência Artificial na Câmara dos Lordes, no ano de 2017 e que publicou suas descobertas em um relatório intitulado "IA no Reino Unido: pronto, disposto e capaz?" ("AI in the UK: ready, willing and able?"[13]). O relatório trouxe argumentos forte de que o Reunido já possui condições para se tornar um líder mundial em Inteligência Artificial, trazendo, ao mesmo tempo, várias recomendações para proteger a sociedade contra possíveis ameaças e riscos futuros.

Entre as recomendações questões sobre responsabilidade legal em casos em que uma decisão tomada por um algoritmo que tenha um impacto negativo na vida de alguém, o potencial uso criminoso da inteligência artificial e dos dados, e o uso de IA em sistemas de armas autônomas, foram ventiladas.

Acrescentamos aos riscos as questões relativas à Privacidade de dados pessoais e Discriminação.

O direito de privacidade de dados refere-se à proteção e ao controle que indivíduos têm sobre suas informações pessoais. Este direito envolve várias diretrizes legais e regulatórias destinadas a garantir que os dados pessoais sejam coletados, processados, armazenados e compartilhados de maneira justa e segura, respeitando a privacidade dos indivíduos.

Como modelo regulatório mundial, o Regulamento da União Europeia sobre Proteção de dados (GDPR - *General Data Protection Regulation*[14]) dispôs várias regras

[13] Authority of the House of Lords, AI in the UK: ready, willing and able? Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf . Acesso em 11 de junho de 2024.

[14] Disponível em: https://gdprinfo.eu/pt-pt

para a coleta, o armazenamento e o uso de informação pessoal, inclusive o direito à explicação ao titular de dados sobre o tratamento realizado com seus dados pessoais, garantindo um processamento justo e transparente desses dados.

No Brasil, seguindo o comando do GDPR o congresso editou em 2018 a LGPD – Lei Geral de Proteção de Dados, que entrou em vigor em 2020, contribuindo no mesmo sentido do GDPR, para um aumento na transparência no uso de dados pessoais.

Nessa toada, os principais riscos relacionados à privacidade advêm do uso em massa de dados pessoais pela Inteligência Artificial para seu processo de reconhecimento de padrões (machine learning). Como descrevem Song et al., (2020)[15], estes sistemas requerem um grande volume de dados para treinar as máquinas, e por este aspecto é um desafio projetar estes recursos sem olhar para dados privados.

Ainda, nesse mesmo caminho a transparência na tomada de decisões da máquina pode ser prejudicada por vários motivos: (i) muitos modelos de IA, especialmente aqueles baseados em aprendizado profundo (deep learning[16]), são altamente complexos. Eles possuem milhões ou bilhões de parâmetros que interagem de maneiras que são difíceis de compreender e de rastrear, inclusive, como uma decisão específica foi tomada. (ii) modelos de aprendizado profundo (deep learning), como redes neurais, são frequentemente descritos como "caixas pretas" porque, apesar de sabermos as entradas e as saídas de informação e dados, a maneira como a IA chegou a uma determinada conclusão é opaca. O processo interno de como as camadas da rede processam a informação nem sempre é interpretável. (iii) a ciência da IA ainda está desenvolvendo padrões e práticas para tornar os modelos mais explicáveis. Embora haja progressos com técnicas como redes neurais explicáveis, ainda está longe de se ter uma abordagem totalmente transparente aplicável a todos os cenários. (iv) empresas que desenvolvem modelos de IA podem não querer divulgar totalmente

[15] SONG, Chengyun et al. User abnormal behavior recommendation via multilayer network. PLoS One, China, v. 14, n. 12, p. 1-17, 2019. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0224684#references. Acesso em 11 de junho de 2024.

[16] O *deep learning* é tido como o método mais evoluído da IA. Ele se baseia em uma tecnologia chamada redes neurais, que simula o comportamento do cérebro humano em um nível extremamente avançado, e é entendido como um subgrupo do Machine Learning.

como suas tecnologias funcionam, devido a preocupações com a propriedade intelectual e vantagem competitiva. Isso pode limitar a transparência sobre os algoritmos e modelos subjacentes. (v) a qualidade e a natureza dos dados de treinamento podem influenciar fortemente as decisões de uma IA. Se os dados de treinamento não forem completamente transparentes ou compreensíveis, se houver vieses fortes, a aplicabilidade das decisões tomadas pela IA também será comprometida. (vi) algumas técnicas para aumentar a transparência, como métodos de explicação pós-hoc (que tentam explicar decisões após serem tomadas), ainda são limitadas e podem não capturar completamente as nuances do processo de tomada de decisão. (vii) ferramentas robustas para explicar modelos de IA ainda estão em desenvolvimento, e pode faltar capacitação entre os cientistas de dados e engenheiros para usar essas ferramentas de maneira eficaz.

Neste sentido, torna-se um desafio definir medidas suficientes para manutenção da melhor prática no uso ético, transparente e responsável da IA, mas também, impossível de não ser enfrentado.

Santos (2018)[17] ressalta que a IA merece "discussões cada vez mais abrangentes em termos de sociedade e que envolvam, sobretudo, as redes sociais virtuais, dadas as fragilidades legislativas nesse campo que abrem margem à violação dos aspectos não apenas éticos e legais, bem como humanos".

3. BOAS PRÁTICAS NO USO DE DADOS

3.1. Transparência no uso dos dados

A transparência no uso dos dados é fundamental para assegurar a confiança dos usuários. É importante que as organizações expliquem claramente como e por que seus dados são usados, e que estas explicações sejam acessíveis e compreensíveis.

[17] DE MELLO, Mariana Rodrigues Gomes; DA SILVA CAMILLO, Everton; DOS SANTOS, Beatriz Rosa Pinheiro. Big data e inteligência artificial: aspectos éticos e legais mediante a teoria crítica. Complexas Revista de Filosofia Temática, Belém, v. 3, n. 1, p. 50-60, 2018. Acesso em: 11 de junho de 2024.

Nesse caminho, dada importância do tema, surge a expressão *data ethics* que se refere aos princípios e valores orientadores que governam a coleta, uso, gestão e compartilhamento de dados, especialmente dados pessoais. O objetivo principal da ética de dados é assegurar que o manejo dos dados respeite a privacidade, a segurança, a justiça e a dignidade dos indivíduos, além de promover o bem-estar social.

Algumas estratégias e práticas são recomendadas para assegurar essa confiança como (i) consentimento informado; (ii) auditoria regulares; (iii) transparência na divulgação clara e acessível as práticas da coleta, uso, processamento e compartilhamento de dados; (iv) oferta aos titulares da capacidade de acessar, corrigir e, quando aplicável, eliminar seus próprios dados; (v) uso de algoritmos de Código Aberto, sempre que possível, para permitir revisões e contribuições da comunidade; (vi) divulgação de critérios e pesos utilizados pelos algoritmos para tomar decisões, sempre que isso não comprometer a segurança ou a propriedade intelectual; (vii) garantir que os dados e os algoritmos que utilizam esses dados não reforcem ou criem vieses injustos ou discriminatórios, além de permitir que todos os indivíduos, independentemente de sua origem, raça, gênero ou status socioeconômico, tenham o mesmo acesso às oportunidades e benefícios proporcionados pelos dados e pela análise de dados; (viii) implementar mecanismos para assegurar que indivíduos e organizações sejam responsabilizados pelo uso indevido ou negligente dos dados, além de estabelecer políticas e estruturas de governança que regulem como os dados são geridos e protegidos; (ix) adotar medidas técnicas e administrativas para proteger os dados contra acesso não autorizado, roubo, perda ou danos; (x) avaliar e mitigar os riscos associados ao uso de dados, especialmente no que diz respeito a dados sensíveis; (xi) utilizar os dados de maneira que promova o bem-estar social e contribua positivamente para a sociedade; (xii) evitar ações que possam causar danos ou impactos negativos aos indivíduos ou grupos.

3.2. Práticas de Minimização de Dados

A minimização de dados é uma estratégia importante para proteger o uso indevido ou exagerado de informações.

A proposta é coletar, processar e armazenar apenas os dados necessários para uma finalidade específica, limitando assim a quantidade de informações pessoais em posse das empresas.

No contexto da inteligência artificial, a minimização de dados é crucial para garantir que apenas as informações relevantes sejam utilizadas nos algoritmos de aprendizado de máquina. Ao reduzir a quantidade de dados coletados e analisados, diminui-se o risco de vazamento de informações pessoais e de uso indevido deles.

A minimização de dados requer que apenas os dados estritamente necessários sejam coletados e processados. Esta prática não apenas reduz riscos de privacidade, mas também facilita a conformidade com a LGPD.

Técnicas como a anonimização e a pseudonimização são eficazes para esta finalidade. Essas técnicas visam proteger a privacidade dos usuários, reduzindo o risco de identificação pessoal, ao mesmo tempo em que permitem o uso dos dados de forma eficaz para treinamento de modelos de IA.

A anonimização envolve a remoção ou alteração de informações identificáveis de um conjunto de dados, tornando-os anônimos e impossíveis de serem vinculados a um indivíduo específico. Isso permite que os dados sejam utilizados de forma mais segura, sem comprometer a privacidade dos indivíduos. Por outro lado, a pseudoanonimização envolve a substituição de identificadores diretos por códigos ou identificadores indiretos, mantendo a possibilidade de reidentificação apenas por pessoas autorizadas que possuam as chaves de descriptografia.

Ao aplicar essas técnicas, os desenvolvedores de Inteligência Artificial podem garantir que os dados sensíveis, por exemplo, sejam protegidos adequadamente, mitigando o risco de exposição indevida ou uso inadequado. Isso é essencial para cumprir regulamentações de privacidade, como a GDPR e a LGPD, além de fortalecer a confiança com os usuários finais.

Dessa forma, a combinação de minimização de dados com técnicas de anonimização e pseudoanonimização é uma prática recomendada para promover a segurança e a privacidade em projetos de inteligência artificial.

3.3. Justiça Algorítmica

Acredita-se que atualmente muitas pessoas ainda possuem preconceitos que podem levar à discriminação, baseados em ideias ultrapassadas de superioridade de certas características sobre outras. Portanto, é necessário considerar que avaliações feitas por humanos ou conjuntos de dados empregados no treinamento de algoritmos podem conter injustiças. Assim, os sistemas algorítmicos devem ser projetados para refletir decisões humanas, porém, com a consciência dos possíveis vieses e erros presentes nas informações coletadas.

A justiça algorítmica é um conceito que aborda a necessidade de garantir a equidade, transparência e responsabilidade no uso de algoritmos e inteligência artificial em processos judiciais e sistemas de tomada de decisões. É essencial considerar a aplicação da justiça algorítmica para assegurar que os algoritmos utilizados no contexto jurídico não perpetuem preconceitos ou discriminações existentes na sociedade.

Anna Wierzbicka[18] conceitua fairness como "suposições culturais" com relação à "regulamentação da vida [humana] levada a efeito por regras geralmente aplicáveis e razoáveis de interação declaradas e não declaradas".

A inteligência artificial pode ser aplicada em diversas áreas do direito, como análise de casos, previsão de decisões judiciais e avaliação de riscos, trazendo eficiência e agilidade para o sistema jurídico. No entanto, é crucial garantir que essas ferramentas não reproduzam viés e injustiças presentes nos dados de treinamento. A justiça algorítmica busca promover a imparcialidade e a equidade ao verificar e corrigir possíveis tendências discriminatórias nos algoritmos.

Em 2014 a Amazon na implementação de IA para recrutamento de candidatos[19], percebeu que seu novo sistema não classificava os candidatos para emprego de desenvolvimento de software e outros cargos técnicos de uma forma neutra em termos de gênero. A razão disso foi o treinamento dos modelos computacionais da Amazon observando padrões nos currículos enviados à empresa durante um período de 10

[18] Anna Wierzbicka, English: Meaning and Culture. Oxford: Oxford University, 2006, pp. 152-54

[19] Dastin, Jeffrey. Insight - Amazon descarta ferramenta secreta de recrutamento de IA que mostrava preconceito contra mulheres. Reuters (2018).

anos. A maioria veio de homens, um reflexo do domínio masculino na indústria tecnológica.

Os exemplos não se encerram e há várias maneiras pelas quais um modelo de aprendizado de máquina pode se enviesar, quando, por exemplo, faltam dados que são representativas da população-alvo, ou quando os algoritmos buscam minimizar os erros de predição de toda a base, assim, por realizarem essa análise agregada, tais objetivos podem levar ao favorecimento da maioria em relação à minoria, ou também quando atributos que podem ser utilizados para identificação indireta de uma característica sensível, como gênero ou raça são usados.

Para aplicar a justiça algorítmica na inteligência artificial, é importante adotar práticas como a transparência na utilização dos algoritmos, a realização de auditorias regulares para identificar e corrigir possíveis preconceitos e a garantia de que os sistemas sejam desenvolvidos de forma ética e responsável. Além disso, é essencial envolver especialistas em ética, direitos humanos e diversidade no desenvolvimento e implementação de soluções baseadas em IA no contexto jurídico.

Dessa forma, a justiça algorítmica se torna um instrumento importante para garantir que a tecnologia seja usada de maneira a promover a igualdade, a justiça e o respeito aos direitos fundamentais de todos os envolvidos no sistema jurídico.

3.4. Medidas de Segurança da Informação

3.4.1. Políticas de Segurança

Políticas de segurança robustas são essenciais para a proteção dos dados pessoais, especialmente quando há uma intersecção com a inteligência artificial (IA). Nesse sentido, é importante considerar alguns aspectos fundamentais como: (i) Conformidade Legal, em que se assegure de que as políticas estejam em conformidade com regulamentos como o GDPR na Europa, LGPD no Brasil, a depender da robustez da empresa;(ii) implementar práticas que incorporam a proteção de dados desde o início do desenvolvimento de sistemas de IA; (iii) definir na Política claramente quem é responsável pela coleta, armazenamento, uso e exclusão de dados; (iv) integrar à Política descrição detalhada sobre aquisição, armazenamento, processamento, compartilhamento e descarte de dados; (v) definir medidas rigorosas para limitar o

acesso aos dados a indivíduos autorizados; (vi) informar claramente aos usuários sobre quais dados são coletados, como são usados e armazenados; (vii) definir procedimentos transparentes para auditorias regulares e monitoramento contínuo da segurança dos dados, inclusive quanto a identificação e mitigação de riscos associados ao tratamento de dados pessoais; (viii) desenvolver planos para responder rapidamente às violações de dados.

Obviamente, após criada as Políticas, é necessário elaborar programas regulares de formação e conscientização para funcionários sobre práticas de proteção de dados e segurança da informação, criando o senso de responsabilidade da equipe, incentivando a cultura de proteção de dados em toda a organização.

3.4.2. Criptografia e Gerenciamento de Riscos

A criptografia de dados é uma técnica fundamental em segurança da informação que visa proteger a confidencialidade, integridade e autenticidade dos dados. Ela desempenha um papel crucial na era digital, especialmente em aplicações que envolvem inteligência artificial, onde grandes volumes de dados, inclusive sensíveis, são frequentemente processados e transmitidos.

Na prática é o processo de converter dados legíveis em uma forma codificada, que só pode ser revertida ao seu estado original por meio de uma chave criptográfica específica. O objetivo principal da criptografia é garantir que os dados permanecem inacessíveis e incompreensíveis para qualquer entidade não autorizada, mesmo que sejam interceptados.

No contexto da inteligência artificial, a criptografia de dados tem um papel vital em garantindo que os dados pessoais utilizados para treinar modelos de IA sejam protegidos contra acessos não autorizados, assegure que os dados transmitidos entre diferentes componentes de um sistema de IA não sejam interceptados ou modificados por atacantes e permitam a realização de operações sobre dados criptografados, preservando a privacidade dos dados.

Falando sobre gerenciamento de riscos no contexto da privacidade de dados, e neste, no uso da IA, é necessária uma abordagem multifacetada na identificação, avaliação, mitigação e monitoramento contínuo de riscos.

A noção do risco segundo dicionário da língua portuguesa é a "Probabilidade da ocorrência de danos, geralmente em função da exposição a um perigo"[20]. De acordo com a norma NP ISO 31000:2018[21], o risco é o efeito da incerteza nos objetivos, sendo, segundo a mesma norma, a gestão de risco como atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos (ISO, 2013).

A conformidade com as regulamentações de proteção de dados, a implementação de tecnologias de segurança robustas e a manutenção de políticas transparentes são fundamentais para garantir que as aplicações de IA sejam seguras e respeitem a privacidade dos indivíduos.

Na identificação de riscos em IA, na busca pelo respeito à Privacidade, pontos como identificação de quais dados são coletados, sua origem, e se incluem informações pessoais sensíveis é o primeiro passo. Em seguida, auditoria ou processos que percebam dados incorretos ou enviesados, que podem levar a resultados imprecisos e decisões prejudiciais. Ainda, a abordagem em relação a riscos de acesso não autorizado, violações de dados e ataques cibernéticos que podem comprometer a integridade e a confidencialidade dos dados. Também, riscos relacionados às decisões automatizadas que podem afetar significativamente os indivíduos se mal direcionadas.

Villani (2018) defende, com ênfase, a premência de incorporar a ética à formação e ao treinamento de desenvolvedores propiciando contemplar, no processo de elaboração dos modelos, os impactos éticos e socioeconômicos, no que se convencionou denominar "ética *by design*". No mesmo caminho temos o *privacy by design* como uma estrutura que busca incorporar práticas para proteção à privacidade dados pessoais em cada etapa de desenvolvimento de um projeto, produto ou serviço, nesse caso, no uso da IA.

4. CONSIDERAÇÕES FINAIS

A interseção entre inteligência artificial e privacidade de dados apresenta tanto oportunidades quanto desafios. O potencial da IA para transformar setores diversos

[20] Dicionário Priberam da Língua Portuguesa [em linha], 2008-2024, https://dicionario.priberam.org/risco."

[21] ISO/IEC (2018) 31000:2018. Gestão de riscos — Diretrizes.

é inegável, mas deve ser equilibrado com medidas rigorosas de proteção de dados e segurança da informação.

A IA representa um reservatório crescente de inteligência capaz de multiplicar a capacidade, melhorando e agilizando suas ações de modo amplo. Contudo, é essencial manter, ao menos em parte, a supervisão e as decisões humanas para assegurar o acompanhamento do desempenho dos sistemas, prevenir e/ou corrigir danos, além de garantir que, em qualquer fase do processo, a responsabilidade seja atribuída a um ser humano por meio de um procedimento previamente definido.

As boas práticas no uso dos dados e o uso de medidas de segurança da informação são pilares fundamentais para este equilíbrio. A implementação de políticas robustas, a utilização de criptografia e o gerenciamento de riscos, juntamente com auditorias regulares e práticas de "*privacy by design*", são essenciais para garantir um uso responsável e ético da IA.

A implementação de medidas de conformidade e segurança não deve ser vista como um obstáculo, mas sim como um facilitador para a utilização segura e eficaz da inteligência artificial. Ao equilibrar a inovação tecnológica com a proteção de dados, conseguimos criar um ambiente digital mais seguro e confiável, que respeita os direitos de privacidade das pessoas e promove o desenvolvimento sustentável.

REFERÊNCIAS

MAGRANI, Eduardo; Entre dados e robôs: ética e privacidade na era da hiperconectividade — 2. ed. — Porto Alegre: Arquipélago Editorial, 2019. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=P7KeDwAAQBAJ&oi=fnd&pg=PT3&dq=intelig%C3%AAncia+artificial+e+privacidade+de+dados&ots=3spkXecUjc&sig=U8v6XrKSnCda73GeU06wG45LVfo#v=onepage&q&f=false. Acesso em 29 mai. 2024.

McCARTHY, John. Interview: What Is Artificial Intelligence - Computer Science Department. Stanford University, 2007. Disponível em: http://www-formal.stanford.edu/jmc/whatisai.pdf. Acesso em: 31 mai. 2024.

BARBOSA, Pablo; CAMACHO, Rafael; SILVA, Cindy. Dilemas Éticos envolvidos no desenvolvimento da Inteligência Artificial. Revista Cacto-Ciência, Arte, Comunicação em Transdisciplinaridade Online, v. 4, n. 1, p. e24010-e24010, 2024. Acesso em 31 mai. 2024.

WINSTON, Patrick Henry. Artificial Intelligence. 3rd edition, Massachussets: AddisonWesley Publishing Company, 1993.

MELO, Gustavo Da Silva. Inteligência artificial e responsabilidade civil: uma análise do anteprojeto do marco legal da inteligência artificial e do projeto de lei 2338/2023 Revista IBERCv. 7, n.1, p. 49-65, jan./abr. 2024www.responsabilidadecivil.org/revista-iberc DOI: https://doi.org/10.37963/iberc.v7i1.271

MONARD, Maria Carolina e BARANAUSKAS, José Augusto. Aplicações de inteligência artificial: uma visão geral. 2000, Anais. São Paulo: Faculdade SENAC de Ciências Exatas e Tecnologia, 2000. Acesso em 11 de junho de 2024.

AUTHORITY OF THE HOUSE OF LORDS, AI in the UK: ready, willing and able? Disponível em chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf . Acesso em 11 de junho de 2024.

SONG, Chengyun et al. User abnormal behavior recommendation via multilayer network. PLoS One, China, v. 14, n. 12, p. 1-17, 2019. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0224684#references. Acesso em 11 de junho de 2024.

Anna Wierzbicka, English: Meaning and Culture. Oxford: Oxford University Press, 2006, pp. 152-54

Dastin, Jeffrey. Insight - Amazon descarta ferramenta secreta de recrutamento de IA que mostrava preconceito contra mulheres. Reuters (2018). Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ Acesso em 14/06/2024.

ISO/IEC (2018) 31000:2018. Gestão de riscos — Diretrizes.

Legislação

UNIÃO EUROPÉIA. Regulation (UE) 2016/679. General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

BRASIL Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília, DF, 15.08.2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm