

VERITAS (PORTO ALEGRE)

Revista de Filosofia da PUCRS

Veritas, Porto Alegre, v. 69, n. 1, p. 1-13, jan.-dez. 2024 e-ISSN: 1984-6746 | ISSN-L: 0042-3955

http://dx.doi.org/10.15448/1984-6746.2024.1.45911

SEÇÃO: ÉTICA E FILOSOFIA POLÍTICA

Repensando a segurança da inteligência artificial com base na confiança: Proteção contra a discriminação algorítmica

Rethinking trust-based artificial intelligence security: Protection against algorithmic discrimination

Replantearse la seguridad de la inteligencia artificial basada en la confianza: Protección contra la discriminación algorítmica

Marcelo Pasetti¹

orcid.org/0000-0003-1993-1422 marcelo.pas@hotmail.com

Nythamar de Oliveira¹

orcid.org/0000-0001-9241-1031 nythamar@yahoo.com

Recebido: 15 mar. 2024. **Aprovado:** 19 abr. 2024. **Publicado:** 19 ago.2024.

Resumo: A rápida ascensão da inteligência artificial (IA) levanta desafios éticos, especialmente relacionados à confiança depositada nessa tecnologia e suas implicações para diversos grupos demográficos. Este texto adota uma abordagem filosófica fenomenológica e hermenêutica, fundamentada em Husserl e Heidegger, para explorar a segurança existencial da IA e sua conexão com a confiança. A confiança na IA é examinada não apenas como uma questão técnica, mas como um fenômeno ligado a dinâmicas sociais complexas, desafiando a reflexão sobre influências discriminatórias nos sistemas inteligentes. O referencial teórico incorpora contribuições recentes sobre confiança na IA para intensificar a produção de literatura sobre segurança nesse campo de estudo com base na confiança, e interage com o Código de Conduta Internacional do Processo de Hiroshima para sistemas avançados de IA.

Palavras-chave: inteligência artificial; segurança; confiança; discriminação algorítmica; lógica interseccional.

Abstract: The rapid rise of artificial intelligence (AI) raises ethical challenges, primarily related to the trust in this technology and its implications for various demographic groups. This text takes a phenomenological and hermeneutic philosophical approach, grounded in Husserl and Heidegger, to explore the existential safety of AI and its connection to trust. Trust in AI is examined not only as a technical issue but as a phenomenon linked to complex social dynamics, challenging reflection on discriminatory influences in intelligent systems. The theoretical framework incorporates recent contributions on trust in AI to intensify the production of literature on trust-based AI safety. It interacts with the Hiroshima Process International Code of Conduct for Advanced AI Systems.

Keywords: artificial intelligence, safety, trustworthy, algorithmic discrimination, intersectional logic

Resumen: El rápido auge de la inteligencia artificial (IA) plantea retos éticos, especialmente relacionados con la confianza depositada en esta tecnología y sus implicaciones para diversos grupos demográficos. Este texto adopta un enfoque filosófico fenomenológico y hermenéutico, basado en Husserl y Heidegger, para explorar la seguridad existencial de la IA y su conexión con la confianza. La confianza en la IA se examina no sólo como una cuestión técnica, sino como un fenómeno vinculado a dinámicas sociales complejas, que desafía la reflexión sobre las influencias discriminatorias en los sistemas inteligentes. El marco teórico incorpora contribuciones recientes sobre la confianza en la IA para intensificar la producción de literatura sobre la seguridad de la IA basada en la confianza, e interactúa con el Código Internacional de Conducta para Sistemas Avanzados de IA del Proceso de Hiroshima.

Palabras clave: inteligencia artificial; seguridad; confianza; discriminación algorítmica; lógica interseccional.



Artigo está licenciado sob forma de uma licença Creative Commons Atribuição 4.0 Internacional.

¹ Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Porto Alegre, RS, Brasil.

1 INTRODUÇÃO

A rápida ascensão da inteligência artificial (IA) trouxe consigo desafios éticos significativos, especialmente no que diz respeito à confiança depositada nessa tecnologia e suas implicações para diferentes grupos demográficos.

À medida que a IA avança e seus sistemas desempenham papéis sociais cada vez mais relevantes, torna-se crucial explorar a questão da segurança existencial que promova a confiança e proteção contra as formas de discriminação que se manifestam, de maneira interconectada, nas diversas realidades. Nessa perspectiva, utiliza-se uma abordagem filosófica fenomenológica e hermenêutica fundamentada nas obras de Edmund Husserl e Martin Heidegger. O objetivo, neste estudo, é compreender como a fenomenologia possibilita uma análise mais precisa das experiências humanas, fomentando uma reflexão sobre a confiança na IA à luz dessas experiências e das implicações éticas da tecnologia.

A fenomenologia, como metodologia, permite uma suspensão temporária de preconceitos, na medida em que questiona pressupostos e busca instigar uma exploração imparcial das experiências humanas em relação à IA. Sob essa ótica, a confiança na IA deixa de ser apenas uma questão técnica e se revela como um fenômeno intrinsecamente ligado às percepções individuais, experiências passadas e contextos socioculturais. Atrai a atenção para as inquietações relacionadas a quem deposita confiança ou mesmo a sua desconfiança na IA.

Além disso, o campo em ascensão da segurança existencial da IA tem atraído a atenção pública e significativos investimentos para respaldar sua promessa subjacente, isto é, a habilidade de implementar IA avançada e, ao mesmo tempo, mitigar seus riscos mais severos, como ameaças existenciais à humanidade. Antes desse avanço, é imperativo que a IA seja introduzida na sociedade de maneira segura. Daí a importância em aprofundar os requisitos para que o seu desenvolvimento seja considerado um modelo de confiança e antecipar-se ao impacto de suas decisões. Outrossim, ver que há um sentido fun-

damental de mudança de atitude ao passarmos de um uso meramente instrumental da técnica para uma reflexão fenomenológico-hermenêutica que busca a sua essência, sem incorrer em essencialismo ou misticismo.

A confiança na IA surge da interação entre o raciocínio observável e o comportamento, sendo esses elementos fundamentais para o estabelecimento dessa confiança. Dessa forma, a conexão com teorias que exploram as dinâmicas sociais concentra-se em examinar as interações intricadas entre diversas formas de opressão e marginalização. Como garantir que os sistemas inteligentes não discriminem? Em se tratando de uma abordagem fenomenológico-hermenêutica, observa-se que somente assim pode-se desmascarar a alienação, a coisificação e a reificação que subjazem a processos discriminatórios.

Nesse contexto, almeja-se oferecer concepções que promovam um enfoque mais produtivo ao contemplar a segurança das aplicações de IA direcionadas para questões atuais. A análise dessas considerações visa aprimorar a confiança depositada nesse campo, explorando, simultaneamente, implicações mais amplas relacionadas aos princípios éticos da IA (responsabilidade, justiça e transparência). A reflexão sobre como esses elementos reverberam em dinâmicas sociais é fundamental para uma compreensão holística e progressiva que possa gerar uma cultura epistêmica para segurança da IA, para além de uma mera comunidade, mas como método de produção científica.

O referencial teórico que embasa as considerações traçadas neste artigo apoia-se em Knowles et al. (2023) para intensificar a produção de literatura sobre confiança na IA, com a ampliação dos princípios éticos da IA. Propõe-se, ainda, uma interação com o Código de Conduta Internacional do Processo de Hiroshima para Sistemas Avançados de AI (COMISSÃO EUROPEIA, 2023). O propósito é repensar a segurança da IA com base na confiança e, assim, promover a proteção contra discriminação em sistemas automatizados.

2 ESSÊNCIA DA TECNOLOGIA

Nas reflexões de Edmund Husserl (1965), aborda-se a aspiração filosófica como sendo uma ciência rigorosa que atenda às necessidades teóricas fundamentais e oriente uma vida ético-religiosa baseada em normas racionais. No entanto, ao longo da evolução teórica, apesar das persistentes pretensões, a disciplina enfrentou desafios à liberdade de investigação, mesmo na filosofia moderna, que buscou a constituição de uma ciência da origem e da natureza do conhecimento por meio de reflexões críticas e investigações metodológicas mais aprofundadas. O objetivo é alcançar uma filosofia em sintonia com os avanços científicos, atenta aos valores culturais fundamentais e assentada em princípios teóricos sólidos.

A introdução da *epoché* por Husserl (2012) busca a suspensão temporária de todos os juízos, opiniões e pressupostos sobre o mundo externo, permitindo que o pesquisador se concentre nas experiências "puras" e conscientes em si mesmas, evitando distorções e pressupostos. A proposta para a "regra de epoché" na abordagem sugerida envolve a suspensão de quaisquer suposições ou preconceitos e, aqui, relaciona-se à resistência e justiça social, em busca de uma análise mais objetiva e cuidadosa dessas questões. Na perspectiva de Martin Heidegger (2015), destaca-se a importância das decisões fundamentais na relação com o ser, sendo possível traçar um paralelo em decorrência da complexidade invisível dessas escolhas na atualidade por meio de sistemas inteligentes. Embora a técnica (die Technik) possa ser definida como um fazer humano enquanto um meio para fins, Heidegger (2007, p. 376) argumenta que devemos pensar para além de tal "determinação instrumental e antropológica da técnica" para resgatá-la como "um modo de desabrigar" (ent-bergen). Nessa conferência proferida em 1953, Heidegger (2007) observa que a "técnica se essencializa no âmbito onde acontece o desabrigar e o desocultamento, onde acontece a aletheia" - segundo a controversa concepção heideggeriana de "verdade" enquanto desvelamento (p. 381).

Com o advento da tecnologia moderna e da tecnociência - termo que não é empregado por Heidegger, dada a sua origem francesa a partir de Bachelard (1934) sobre o papel imprescindível da tecnologia para a emergência de pesquisas em física quântica –, a questão da techne enquanto arte (concepção primordial a ser resgatada, segundo Heidegger) se contrapõe a concepções modernas da técnica, cristalizadas como tecnociência e tecnologia, em sua mera instrumentalidade, disponibilidade e suposta neutralidade. Em se tratando de um resgate fenomenológico da técnica e da tecnologia (observando, en passant, que Technik pode nos remeter a ambos termos em português), é essencial reconhecer a diferença entre uma concepção meramente instrumental e uma reflexão que busca a essência da techne como arte primordial, conforme proposto por Heidegger.

Heidegger nos oferece também uma leitura hermenêutica da cartografia husserliana da matematização da natureza a partir da modernidade. Foi sobretudo a partir de Dreyfus (1992) que a fenomenologia e a hermenêutica começaram a ser evocadas em estudos sobre IA e novas tecnologias, destacando a irredutibilidade da experiência humana enquanto Dasein (ser-ai), ser incorporado e corporificado em suas vivências (Erlebnisse) que experienciam o que é significativo para cada um de nós de forma singular e na primeira pessoa (ou seja, em nossa complexa autocompreensão do eu, self, Selbst, mesmo na experiência coletiva de "nós", na primeira pessoa do plural). Todavia, Dreyfus (2007) se manteve cético quanto à possibilidade de alcançarmos, através de sofisticados algoritmos, programas e sistemas de IA, "um modelo de corpo muito parecido com o nosso, com nossas necessidades, desejos, prazeres, dores, formas de locomoção, formação cultural, etc." de forma a "desenvolver um sistema embutido e incorporado" (p. 265).

A análise existencial da tecnologia proporciona uma cultura epistêmica útil, capacitando a comunidade a compreender a segurança da inteligência artificial como uma fonte fundamental para a construção desse campo, dado que

a tecnologia não é um meio neutro, muito pelo contrário, ela molda a compreensão do mundo. Isso levanta a questão inevitável de como a tecnologia influencia nossa compreensão da verdade. Destaca-se, assim, a necessidade de coerência entre as diferentes ideias apresentadas. Isso inclui a relação entre a construção do saber, a especificidade das ciências, o rigor científico e a essência da tecnologia.

Shazeda Ahmed et al. (2023) argumentam que a finalidade da segurança da IA é reunir especialistas técnicos e pesquisadores dedicados à prevenção de eventos catastróficos provenientes de sistemas que utilizam agentes algorítmicos, considerados como elementos cruciais de uma cultura epistêmica. Nesse contexto, é fundamental compreender como se forma a confiabilidade que orienta a tomada de decisões e molda as agendas de pesquisa dentro dessas comunidades. Elas não apenas desempenham um papel técnico, mas também possuem uma função social ao facilitar a troca, consumo e avaliação das previsões entre os membros, evidenciando a interconexão entre a confiabilidade técnica e a dinâmica social no campo da segurança da IA.

No entanto, é imperativo centralizar nos impactos reais da IA no mundo atual, a busca em mitigar e gerenciar os riscos associados aos danos, inclusive, aqueles que afetam de forma específica indivíduos com características distintas, conforme destacado no item 2, "a", Parte 1 da Introdução da Online Safety Act 2023 do Reino Unido (2023): "... imposes duties which, in broad terms, require providers of services regulated by this Act to identify, mitigate and manage the risks of harm (including risks which particularly affect individuals with a certain characteristic) from".

Daí a necessidade de fomentar uma cultura epistêmica que estimule a redefinição da confiança na AI é evidente, pois permite a identificação de alinhamentos de valores necessários para estabelecer paradigmas apropriados em sua implementação. Essa análise leva em consideração tanto as dimensões filosóficas relacionadas à moralidade quanto as questões científicas sociais sobre o comportamento humano. Aqueles

elementos, se negligenciados, podem potencialmente resultar em danos imediatos (AHMED *et al.*, 2023).

Nas próximas subsecções, será explorada a interseção entre ética, tecnologia e questões sociais, considerando a confiança não apenas como uma crença na precisão técnica da IA, mas como uma construção social contextual, atitudinal e (inter)subjetiva.

2.1 Ética da IA: confiança

Conforme destacado por Jacovi et al. (2021), o objetivo da confiança é primariamente tornar a vida social previsível, antecipando o impacto do comportamento e facilitando a colaboração entre as pessoas. Dentro do contexto da confiança Humano-IA, as ideias de antecipação e vulnerabilidade desempenham um papel importante. Isso ocorre porque a confiança busca reduzir a incerteza e o risco relacionados à colaboração, esforçando-se para antecipar as possíveis consequências do comportamento em situações de risco.

Segundo David Manheim (2023), de maneira abrangente, os ganhos decorrentes da maximização da tecnologia podem conduzir ao surgimento gradual, e não súbito, de catástrofes existenciais. Nesse contexto, a abordagem fenomenológica hermenêutica de Heidegger (2015) oferece uma análise da compreensão do mundo e dos desafios associados à mitigação de riscos potenciais que podem emergir no futuro, especialmente no que diz respeito aos sistemas de IA.

A ética da IA, conforme discutida por Corrêa et al. (2023), está passando por um rápido desenvolvimento, interligando-se com questões sociais como justiça, igualdade e discriminação. Nesse caso, a aplicação da "epoché" emerge como uma abordagem essencial para analisar se a confiança está alinhada com a resistência e a justiça social, desempenhando um papel crucial na construção de um futuro sociotécnico mais equitativo.

A fenomenologia hermenêutica exerce uma função básica ao interpretar o significado das experiências humanas no âmbito da resistência e justiça social. Em outras palavras, ela envolve a análise de reações contrárias a ações de terceiros e a garantia do acesso aos direitos, conforme estabelecidos por lei, para corrigir desigualdades, ilegalidades ou desrespeitos (KNOWLES *et al.*, 2023), permitindo a exploração da interconexão desses conceitos com a percepção, a ação e a compreensão da realidade.

Além disso, é importante destacar que os princípios éticos da IA cumprem uma missão basilar na integração de valores semelhantes e ressonantes, ao mesmo tempo em que preservam diferenças significativas na repetição das palavras (CORRÊA et al., 2023). A construção da confiança na inteligência artificial surge, portanto, como um aspecto vital de nossa orientação existencial, transcendendo a mera precisão técnica para abraçar uma confiança fundamental na própria natureza da realidade moldada por ela (KNOWLES et al., 2023).

Como assevera Côrrea et al. (2023), uma das questões centrais em torno da ética da IA é determinar quais premissas devem orientar os princípios éticos, como são descritos, quais suas características intrínsecas e se existe uma compreensão consistente deles. Embora a confiança seja um dos princípios mais comuns da ética da IA, ela não é homogênea. A subjetividade da confiança na IA se manifesta especialmente em contextos sociais, onde decisões importantes sobre alocação de recursos levantam preocupações sobre equidade (KNOWLES et al., 2023).

Com efeito, a abordagem das inquietações populares sobre a confiança na inteligência artificial destaca a importância de identificar quem deposita confiança ou desconfiança. A partir desse ponto, surge a necessidade de desenvolver técnicas e práticas para alcançar dois objetivos principais propostas por Knowles *et al.* (2023): a) promover a "confiabilidade" da IA, alinhada a diversos princípios; e b) avaliar essa confiabilidade de maneira eficaz.

A falta de análises abrangentes sobre a confiança na literatura dedicada à IA sugere que a questão pode ser mais complexa do que aparenta. Não se trata simplesmente de uma crença isolada na confiabilidade da IA. Estabelecer con-

fiança cognitiva requer, entre outros fatores, que os padrões diferenciadores entre casos corretos e incorretos do modelo estejam disponíveis para o usuário. Tornar essa informação acessível e interpretável para ele tem se revelado um desafio significativo no contexto da IA (KNOWLES et al., 2023).

O cerne da questão está na possibilidade de considerar a confiabilidade como uma característica objetiva de um sistema de IA, determinada pela precisão da cognição e do controle. A incerteza que se apresenta é se a desconfiança de uma pessoa em relação à IA é tão justificada quanto a confiança de outra (KNOWLES *et al.*, 2023), sugerindo que a confiabilidade pode ser, ao menos em parte, subjetiva?

De acordo com Jacovi et al. (2021), a compreensão da desconfiança é essencial, pois representa o mecanismo pelo qual o usuário busca evitar resultados desfavoráveis. Assim, o usuário pode não aceitar a vulnerabilidade como justificativa, uma vez que a desconfiança é percebida como confiança no cenário negativo. Esse dilema ganha mais clareza ao restringir a análise da IA aplicada em contextos sociais específicos, como em sistemas que influenciam decisões sobre a alocação de recursos ou oportunidades em uma população (KNOWLES et al., 2023).

Como ilustração, menciona-se a ordem executiva emitida pelo Presidente dos Estados Unidos, Joe Biden, sobre o desenvolvimento e uso seguro e confiável de IA para corrigir distorções, teve como objetivo promover a equidade e os direitos civis. Essa medida visa prevenir o uso de algoritmos de IA que possa agravar a discriminação em programas de benefícios e contratos federais (WHITE HOUSE, 2023).

Na mesma linha, o Código de Conduta Internacional do Processo de Hiroshima para Sistemas Avançados de IA visa promover segurança e confiabilidade em todo o mundo. Ele oferece orientações voluntárias às organizações que desenvolvem sistemas inteligentes mais avançados com foco na abordagem de riscos. Trata-se de um documento vivo estribado nos princípios de IA existentes da OCDE (COMISSÃO EUROPEIA, 2023).

Por isso, a definição de confiança levanta a questão de haver ou não vantagens para determinados indivíduos ao se permitirem ser vulneráveis à IA. A vulnerabilidade, resultante do potencial de traição da confiança, pode revelar-se injustificada. A confiança, embora arriscada, oferece potenciais recompensas. Optar por confiar (ser vulnerável à possível traição da confiança) permite usufruir dos benefícios da confiança e avaliar se a confiança foi bem depositada, possibilitando ajustes futuros (KNOWLES et al., 2023).

O componente conativo da confiança, que abrange juízos, decisões e intenções conducentes à disposição para confiar, aplica-se especialmente à desconfiança na IA em sentido abstrato, expressa em afirmações generalizadas pela falta de confiança na IA. A conação é contextual dependente, sujeita a mudanças com alterações no contexto. Por isso, ao ser usada pela IA poderá criar uma subclasse digital rotulada como "indiferente", torna moralmente aceitável a violência estrutural. A desconfiança, vista como resposta legítima a uma ameaça percebida, pode ser explorada como uma ação para abordar preocupações legítimas de quem corre maior risco de danos algorítmicos (KNOWLES et al., 2023).

2.2 Concepção da confiança na IA

No campo da ética da IA, a abordagem conhecida como confiança da IA destaca a interseção entre ética, tecnologia e questões sociais. A confiança na IA não é apenas considerada como uma crença na sua precisão técnica, mas é compreendida como uma construção social que envolve quem confia, quem desconfia e por quê. A complexidade da questão da confiabilidade da IA é evidenciada na literatura sobre IA confiável. revelando uma lacuna na compreensão desse tópico. A confiança não é uma crença universal, mas sim contextual e subjetiva. Mesmo que a confiabilidade seja frequentemente vista como uma qualidade objetiva, ela pode ser influenciada por diferentes perspectivas, uma vez que levanta dúvidas sobre a subjetividade associada à desconfiança (KNOWLES et al., 2023).

Essa abordagem se mostra relevante em

contextos sociais nos quais a IA desempenha um papel na tomada de decisões que impactam a distribuição de recursos e oportunidades. Dessa forma, a confiança na IA não se limita apenas ao aspecto técnico, mas carrega implicações éticas e sociais significativas (KNOWLES *et al.*, 2023).

De acordo com Pérez Y Madrid e Wright (2023), a confiança abrange diferentes interpretações, incluindo aspectos afetivos, normativos e racionais. Na perspectiva afetiva da confiança, o instituidor é aquele que confia na benevolência do administrador - que pode ser uma pessoa, grupo de pessoas, organização ou sistema - e espera que este seja motivado por tal afeto. Contudo, é crucial destacar que a IA não pode ser impulsionada por intenções benevolentes ou pela expectativa de confiança. Já na interpretação normativa da confiança, as expectativas do instituidor não se restringem apenas ao que o administrador fará, mas também ao que ele deverá fazer. Isso implica que o administrador, seja ele quem for, sinta uma motivação para ser moralmente responsável por suas ações, assumindo um compromisso normativo.

No entanto, a IA também não é capaz de assumir responsabilidade moral por suas ações. Já na interpretação racional da confiança, o instituidor realiza cálculos racionais para determinar se deve confiar no administrador. Essa abordagem se baseia em previsões unilaterais e não resulta de uma relação bidirecional entre o instituidor e o administrador (PÉREZ Y MADRID; WRIGHT, 2023).

De acordo com Jacovi et al. (2021), é possível aprimorar a confiança intrínseca de maneira disciplinada, formalizando os antecedentes por trás do comportamento confiável ou não suspeito e incorporando-o de modo que defenda esses princípios. Tornar algo confiável, nesse contexto, implica uma explicação detalhada. A confiança extrínseca, por sua vez, baseia-se essencialmente no esquema de avaliação. É possível alcançá-la por meio da explicação da metodologia ou dos dados de avaliação. A confiança, nesse caso, é derivada da observação dos sintomas de um modelo confiável, em vez de depender do entendimento interno do seu funcionamento.

Após explorar essas visões sobre a confiança na IA, analisam-se as distintas dinâmicas de discriminação e desafios para repensar a segurança da IA com base na confiança.

3 DINÂMICAS DE DISCRIMINAÇÃO ALGORÍTMICA

A discriminação é uma realidade que persiste em diversas sociedades, manifesta-se de maneiras variadas e em contextos distintos. Esse fenômeno intricado vai além de simples tratamentos desiguais, infiltrando-se nas interações sociais de forma sutil e, por vezes, inadvertida. Em sua obra de 2021, Wachter et al. exploram dois tipos essenciais de discriminação que merecem análise: a discriminação direta, caracterizada por tratamentos menos favoráveis baseados em características específicas, e a discriminação indireta, que se manifesta por meio de políticas ou práticas aparentemente neutras, mas que, de maneira desproporcional, impactam grupos protegidos.

A discriminação direta se materializa quando um indivíduo é alvo de tratamento desfavorável com base em características protegidas, tais como sexo, raça, religião, idade, deficiência e orientação sexual. Esse tipo de discriminação se apresenta de maneira explícita e evidente, muitas vezes refletindo preconceitos arraigados na sociedade. Por outro lado, a discriminação indireta adquire uma forma mais sutil e ocorre quando políticas, práticas ou critérios aparentemente neutros afetam de maneira desproporcional um grupo protegido, colocando-o em desvantagem em relação a outros grupos. Essas práticas, embora inicialmente possam parecer imparciais, revelam-se injustas ao se analisar seus impactos prejudiciais sobre comunidades vulneráveis (WACHTER et al., 2021).

Além disso, a discriminação indireta, embora não se apresente de forma explícita, pode perpetuar desigualdades profundas e persistentes. A ausência de uma intenção discriminatória direta não elimina o impacto prejudicial sobre os grupos protegidos. Nesse sentido, a análise crítica desses fenômenos é essencial para a construção de sociedades mais justas e inclusivas. Ao se entender as nuances da discriminação direta e indireta, está-se mais apto a confrontar as estruturas que perpetuam a injustiça, promovendo diálogos e ações que visam à eliminação dessas formas de marginalização (WACHTER et al., 2021).

Outra questão conexa que surge ao considerar a composição de grupos desfavorecidos é o desafio da discriminação multidimensional. Isso ocorre quando as pessoas enfrentam discriminação com base em mais de uma característica protegida. Pode-se fazer uma distinção entre discriminação aditiva e interseccional. A discriminação aditiva refere-se à disparidade baseada em duas ou mais características protegidas consideradas individualmente, como ser tratada separadamente como "negra" e "mulher". Já a discriminação interseccional diz respeito a uma desvantagem baseada em duas ou mais características consideradas em conjunto, por exemplo, ser uma "mulher negra" (WACHTER et al., 2021).

Lógicas interseccionais referem-se a uma abordagem teórica e analítica que destaca a interconexão e interseção de diferentes formas de opressão e identidades sociais. Essa abordagem, central para entender as complexidades das experiências individuais e coletivas, ganha ainda mais relevância quando se considera o problema da discriminação multidimensional. No momento em que se analisa a composição de grupos desfavorecidos, surge o desafio de compreender como diversas características protegidas interagem para criar diferentes camadas de desvantagem. Desse modo, a perspectiva interseccional, originada nos estudos críticos da raça e do feminismo, amplia a compreensão das dinâmicas sociais e contribui para abordagens mais inclusivas e holísticas na análise das experiências humanas (KNOWLES et al., 2023).

De acordo com Gohar e Cheng (2023), a teoria da interseccionalidade reconhece que as pessoas podem vivenciar diversas formas de opressão simultaneamente, e essas opressões estão interligadas em diferentes níveis de discriminação que impactam vários subgrupos potenciais. Segundo Knowles *et al.* (2023), isso implica que

as categorias de identidade, como raça, gênero, classe social, orientação sexual, habilidade física, entre outras, não operam de maneira isolada, mas interagem de maneiras complexas e, muitas vezes, interdependentes e interseccionais. Gohar e Cheng (2023) argumentam que, ao classificar indivíduos apenas em categorias claramente definidas e em grupos sobrepostos, a justiça de grupo independente negligencia a discriminação enfrentada pelas pessoas na interseção desses grupos.

Assim, as lógicas interseccionais buscam analisar as interações complexas e dinâmicas entre diferentes sistemas de poder, examinando como as identidades sociais se entrelaçam e afetam as experiências de discriminação e privilégio. Essa abordagem é importante para uma compreensão mais completa e inclusiva das desigualdades sociais e para informar práticas e políticas que buscam a justiça social (KNOWLES et al., 2023).

As lógicas interseccionais de desconfiança revelam porque grupos marginalizados podem desconfiar da IA mostrando como a tecnologia pode perpetuar desigualdades sociais, exemplificadas pela criação de uma subclasse digital "indesejável" que justifica a violência estrutural (KNOWLES et al., 2023). A desconfiança na IA, sob essas lógicas, não é apenas uma reação emocional, mas uma resposta legítima a ameaças percebidas, especialmente para os mais vulneráveis aos danos algorítmicos. Reconhecer que a confiança é um privilégio dos grupos majoritários destaca a importância de considerar quem se beneficia da confiança na IA (KNOWLES et al., 2023).

Portanto, faz-se necessário que os sistemas de IA incorporem a não discriminação como valor central, visando promover a equidade de tratamento, independentemente de características como raça, gênero e religião, contribuindo para a construção de sistemas éticos e normativos em busca de uma sociedade mais justa e equitativa. Segundo Amartya Sen (2011), a procura por uma fórmula que promova a igualdade ou um princípio de não discriminação em teorias normativas reflete a preocupação central com a

justiça, imparcialidade e equidade. A incorporação desse princípio tem como objetivo assegurar que as decisões políticas ou sistemas derivados da teoria sejam implementados de forma justa e sem qualquer viés injustificado.

Entretanto, a distribuição desigual pode ser mais justa em certos casos (GOHAR; CHENG, 2023). Para Knowles et al. (2023), as narrativas populares de não desejabilidade são replicadas e amplificadas pela IA. Assim como ocorre com as disparidades analógicas, esse processo possibilita que os merecedores logrem dos frutos da subjugação de uma classe inferior e aliviem a necessidade de abordar as desigualdades reforçadas pelos algoritmos e pelas lógicas que os orientam. De fato, por meio do poder narrativo da falta de merecimento, as desigualdades podem ser reinterpretadas como merecidas. Em resumo, a ideia de não merecimento é habilmente utilizada para obscurecer a violência estrutural da IA, apresentando-a como justificada.

A linguagem da marginalização destaca processos estruturais que sistematicamente prejudicam grupos específicos, resultando em desigualdades e danos relacionados à etnia, raça, gênero, idade, orientação sexual e outros marcadores de violência estrutural. A marginalização é contextual, não sendo uma característica inerente dos indivíduos, mas sim uma exclusão sistemática. Sistemas injustos podem causar danos mesmo sem intenção, e aqueles que se beneficiam desses sistemas correm o risco de serem cúmplices da violência estrutural, a menos que ativamente trabalhem para compreender e desmantelar a opressão (KNOWLES *et al.*, 2023).

Nesse diapasão, a aplicação da *epoché* se mostra oportuna para entender conceitos como resistência (uma reação contrária à ação de outrem) e justiça social (assegurar o acesso aos direitos legalmente previstos, corrigindo desigualdades, ilegalidades ou desrespeitos), proporcionando uma compreensão mais aprofundada dessas questões na experiência humana. Ao suspender preconceitos e pressupostos, torna-se possível explorar a maneira como esses conceitos se entrelaçam com a percepção, a ação e a com-

preensão da realidade (KNOWLES et al., 2023).

Em síntese, a discriminação frequentemente se manifesta de maneira sutil, abstrata e desafiadora de ser identificada, pois as vítimas podem não perceber que estão sendo alvo desse comportamento. A discriminação automatizada ocorre quando algoritmos de IA, em vez de agentes humanos, tomam decisões que resultam em tratamento injusto ou prejudicial com base em características protegidas (WACHTER et al., 2021).

A seguir, apresentam-se propostas de abordagens alternativas para reconsiderar a segurança da IA, fundamentadas em confiança, tendo como pilares a responsabilidade, a transparência e a justiça, visando, dessa maneira, fomentar a salvaguarda contra a discriminação em sistemas automatizados.

3.1 Desafios para repensar a segurança da IA com base na confiança

Pode-se definir a segurança da IA como uma iniciativa abrangente para garantir que a sua implementação não resulte em danos à humanidade (SINGH et al., 2021). A busca por essa redefinição pode ser conduzida por meio de conceitos, conforme estudos de Knowles et al. (2023). Esses estudos concentram-se em experiências que visam redefinir a confiança na IA, sobressaindo os princípios éticos da responsabilidade, transparência e justiça. Essa abordagem busca identificar lacunas nas práticas convencionais para fortalecer a confiança pública na IA, especialmente em relação a vários métodos de discriminação.

A redefinição da responsabilidade na IA pode ocorrer por meio de uma abordagem ética centrada em valores morais, que descentraliza o desenvolvimento da IA e integra práticas de monitoramento e cuidado. A transparência, vital para a conformidade, deve ser reformulada de maneira a envolver eficazmente o público, incluindo diversas partes interessadas, e revisar os regulamentos a fim de evitar "injustiça epistêmica" (KNOWLES et al., 2023).

Ao reconhecer e acolher a vulnerabilidade, fomenta-se o estabelecimento de relações de produção de conhecimento mais solidárias. Na busca pela justiça na IA, é crucial reavaliar o viés estatístico, reconhecendo as limitações dos julgamentos fundamentados em méritos passados. A IA pode servir como uma ferramenta para direcionar recursos de maneira mais equitativa, fortalecendo não apenas sua confiabilidade, mas também contribuindo para a confiança nas instituições que a empregam (KNOWLES *et al.*, 2023).

3.1.1 Redimensionando a "responsabilidade"

No contexto da IA confiável, a responsabilidade é um processo de avaliar a conformidade com um conjunto de princípios e objetivos acordados. É crucial notar que isso frequentemente envolve uma classe de especialistas se comunicando com outra sobre essa conformidade. Os objetivos da responsabilidade podem incluir a rastreabilidade e talvez a verificabilidade, que oferecem salvaguardas importantes, mas muitas vezes são definidos por uma elite de indivíduos (KNOWLES et al., 2023).

A responsabilização exige a existência de mecanismos que garantam a prestação de contas, a responsabilidade e a responsabilização pelos sistemas de IA e pelos seus resultados, tanto antes como depois do seu desenvolvimento, implantação e utilização (PÉREZ Y MADRID; WRIGHT, 2023).

Desenvolver, implementar e comunicar políticas de governança, bem como a gestão de riscos da IA, são essenciais para promover a segurança, a proteção e a confiabilidade dos sistemas avançados. É fundamental que haja colaboração entre organizações ao longo do ciclo de vida da IA e o compartilhamento de informações com o público e autoridades. Mecanismos organizacionais devem ser estabelecidos para identificar, avaliar, prevenir e abordar riscos, respeitando a propriedade intelectual (COMISSÃO EUROPEIA, 2023).

Daí a importância do compartilhamento de informações entre organizações, incluindo indústria, governos, sociedade civil e academia para o desenvolvimento de sistemas avançados de IA. Recomenda-se, igualmente, estabelecer padrões e melhores práticas compartilhadas para

garantir a segurança e a confiabilidade assim como a divulgação de políticas de privacidade, dados pessoais e resultados de sistemas de IA, especialmente daquelas (políticas) baseadas em risco, além da atualização regular das mesmas (COMISSÃO EUROPEIA, 2023).

As organizações devem comunicar suas políticas de governança da IA e implementar mecanismos organizacionais para avaliar e mitigar riscos ao longo do ciclo de vida da IA. Além disso, é essencial estabelecer políticas, procedimentos e treinamento para garantir que os colaboradores estejam familiarizados com as práticas de gestão de riscos (COMISSÃO EUROPEIA, 2023).

3.1.2 Redimensionado a "transparência"

Uma ação de grande relevância para garantir a confiabilidade é ser transparente sobre o progresso na compreensão dos danos causados pela IA e sobre como essa compreensão foi adquirida. Isso implica, primeiramente, refletir sobre essas questões e, em seguida, expô-las à crítica pública, permitindo que aqueles que desenvolvem a IA compartilhem sua visão do mundo (KNOWLES et al., 2023).

É forçoso relatar publicamente as capacidades, limitações e contextos apropriados e inapropriados dos sistemas avançados de IA para garantir a transparência, pois esta se encontra intimamente associada ao princípio da explicabilidade e abrange a clareza dos elementos essenciais para um sistema de IA incluindo os dados, o sistema e os modelos de negócios (PÉREZ Y MADRID; WRIGHT, 2023).

A divulgação de relatórios de transparência, acompanhados de instruções de uso e documentação técnica, deve ser contínuo. Também será preciso abordar aspectos como os impactos na segurança e na sociedade, incluindo preconceitos, discriminação, ameaças à privacidade e efeitos na justiça. Esses relatórios devem ser claros e compreensíveis, permitindo que implementadores e usuários interpretem os resultados e usem os sistemas adequadamente (COMISSÃO EUROPEIA, 2023).

Além disso, é relevante que a transparência

seja respaldada por processos de documentação robustos, como documentos técnicos e instruções de uso, para oferecer uma compreensão abrangente do funcionamento e da aplicação dos sistemas avançados de IA. Essas práticas visam promover uma utilização ética e responsável dessas tecnologias (COMISSÃO EUROPEIA, 2023).

3.1.3 Redimensionando a "justiça"

As principais preocupações no discurso sobre justiça em relação à IA são a segurança e a mitigação de preconceitos. Uma IA é considerada injusta quando os resultados ou previsões que gera afetam diferentes grupos de forma desigual, com base em características socialmente construídas, como raça ou gênero. Isso se reflete em taxas diferentes de falsos positivos, falsos negativos e decisões favoráveis/desfavoráveis. Além disso, pode ser considerada injusta quando indivíduos semelhantes recebem resultados diferentes (KNOWLES et al., 2023).

É indispensável observar a importância da justiça em duas dimensões. Primeiramente, a dimensão substantiva, que requer a garantia de uma distribuição equitativa e justa dos benefícios e custos, assegurando tratamento justo aos indivíduos. Da mesma forma, é imperativo observar a dimensão processual da justiça, que envolve a capacidade de contestar e buscar uma reparação efetiva em relação às decisões tomadas por sistemas de IA e pelos seres humanos que os operam (PÉREZ Y MADRID; WRIGHT, 2023).

Segundo Singh et al. (2021), no âmbito do aprendizado de máquina, um algoritmo específico é caracterizado como justo ou imparcial quando seus resultados não sofrem influência das variáveis fornecidas, especialmente aquelas consideradas sensíveis, como as características individuais que não devem ter correlação com o resultado, tais como gênero, etnia, orientação sexual, deficiência, entre outras. Um sistema de IA receberia a designação de justo ou imparcial ao atender a esse critério.

Por outro lado, Pérez Y Madrid e Wright (2023) argumentam que a justiça distributiva implica que um algoritmo é considerado justo se

produzir resultados equitativos, ainda que suas recomendações impactem, de maneira desigual, diferentes grupos sociais. Uma abordagem para resolver esse problema seria estabelecer limites distintos para cada grupo, sacrificando assim a justiça processual em prol da justiça distributiva.

Enquanto exploram as oportunidades de inovação, é desejável e em certo sentido obrigatório que as organizações adiram ao Estado de direito, aos direitos humanos, ao devido processo legal, à diversidade, à justiça, à não discriminação, à democracia e à centralização no ser humano durante o desenvolvimento, concepção e implementação de sistemas avançados de IA. Mesmo que reconheça-se a dificuldade ou até a impossibilidade de fundamentar-se uma ideia de normatividade jurídico-legal a partir de uma ideia ético-normativa ou de uma fenomenologia moral (DRUMMOND & TIMMONS, 2023), pode-se postular a necessidade de obter diretrizes normativas universalizáveis ou capazes de serem subscritas por todos os membros de uma sociedade democrática. É crucial que tais sistemas não sejam concebidos ou implementados de modo a comprometer os valores democráticos ou representar riscos significativos para indivíduos ou comunidades, facilitar atividades terroristas ou, ainda, promover o uso criminoso indevido ou apresentar ameaças substanciais à segurança e aos direitos humanos (COMISSÃO EUROPEIA, 2023).

4 CONSIDERAÇÕES FINAIS

Neste texto, objetivou-se colocar em pauta a fenomenologia hermenêutica voltada para compreender a confiança na IA e as diversas formas de discriminações algorítmicas. Ao suspender preconceitos e explorar as experiências humanas subjacentes, somos capazes de compreender as complexidades da confiança depositada na tecnologia. Não se trata apenas de uma questão técnica, mas uma questão existencial que poderá influenciar a nossa compreensão do mundo e de nós mesmos.

A discriminação algorítmica, seja direta ou indireta, apresenta-se como um obstáculo sig-

nificativo, requerendo um constante redimensionamento dos princípios que regem o desenvolvimento e a aplicação da IA. Por sua vez, a teoria interseccional emerge como uma ferramenta crucial para analisar as múltiplas dimensões da discriminação, reconhecendo as interconexões entre diferentes formas de opressão e identidades sociais. A desconfiança na IA, especialmente entre grupos marginalizados, é fundamentada em ameaças percebidas e lógicas interseccionais, e na ênfase da importância de considerar quem se beneficia dessa confiança.

A proposta de repensar a segurança da IA com base na confiança foi delineada por meio dos pilares éticos da responsabilidade, transparência e justiça. Redefinir a responsabilidade envolve descentralizar o desenvolvimento da IA, incorporar práticas de monitoramento e cuidado, e estabelecer mecanismos de responsabilização. A transparência, essencial para a conformidade, exige relatórios contínuos, documentação técnica abrangente e divulgação de impactos. A justiça, tanto substantiva quanto processual, destaca a necessidade de distribuição equitativa de benefícios e custos, e a capacidade de contestar decisões injustas.

Diante desses desafios, é imperativo que os sistemas de IA incorporem não apenas a não discriminação como um valor central, mas também promovam a equidade de tratamento, contribuindo para a construção de uma sociedade mais justa e inclusiva. Como visto, é impossível garantir que os sistemas inteligentes não discriminem. Todavia, a colaboração entre comunidades de segurança da IA, o compartilhamento de informações e o compromisso com valores democráticos e direitos humanos são fundamentais para mitigar os riscos e assegurar que a IA seja uma força positiva na evolução da sociedade. Em última análise, a busca por IA segura deve ser guiada por princípios éticos sólidos e uma compreensão aprofundada das complexidades envolvidas.

Isso posto, é mister considerar a relevância de uma abordagem humana para a tecnologia por uma questão de pragmatismo, a saber, o que está em jogo é, afinal, a autopreservação da espécie humana. A confiança na IA simplesmente não pode ser desvinculada das experiências e valores humanos. Ao adotar essa perspectiva, não apenas enriquece-se nossa compreensão da confiança na IA, mas também promove-se um diálogo crítico sobre o papel da tecnologia na construção de um mundo compartilhado.

REFERÊNCIAS

Ahmed, Shazeda; Jaźwińska, Klaudia; Ahlawat, Archana; Winecoff, Amy; Wang, Mona. **Building the Epistemic Community of Al Safety.** Social Science Research Network (SSRN), New York, Nov. 22, 2023. Disponível em: http://dx.doi.org/10.2139/ssrn.4641526>. Acesso em: 02 dez. 2023.

BACHELARD, Gaston. Le nouvel esprit scientifique. Paris: Presses Universitaires de France, 1934.

COMISSÃO EUROPEIA. Código de Conduta Internacional do Processo de Hiroshima para Sistemas Avançados de Inteligência Artificial. Bruxelas, 30 out. 2023. Disponível em: https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems>. Acesso em: 10 nov. 2023.

Corrêa, Nicholas. K.; Galvão, Camila; Santos, James W., Del Pino, Carolina.; Pinto, Edson P.; Barbosa, Camila; Massmann, Diogo; Mambrini, Rodrigo; Galvão, Luíza; Terem, Edmund; Oliveira, Nythamar (2023). Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. **Patterns**, v. 4, n. 10, p. 1-15, 2023. Disponível em: https://doi.org/10.1016/j.patter.2023.100857>. Acesso em: 30 de nov. 2023.

DREYFUS, Hubert L. **What Computers Still Can't Do: A critique of Artificial Reason**. Cambridge: MIT Press, 1992.

DREYFUS, Hubert L. "Why Heideggerian Artificial Intelligence failed and how fixing it would require making it more". **Heideggerian. Philosophical Psychology**, Abingdon, v. 20, n. 2, p. 247-268, 2007.

DRUMMOND, John; TIMMONS Mark. Moral Phenomenology, *The Stanford Encyclopedia of Philosophy* (Fall 2023 Edition). ZALTA, Edward N. & NODELMAN, Uri (Eds.). Disponível em: https://plato.stanford.edu/archives/fall2023/entries/moral-phenomenology/>. Acesso em 1º mar. de 2024.

Gohar, Usman; Cheng, Lu. A Survey on Intersectional Fairness in Machine Learning: Notions, Mitigation, and Challenges. *In:* Proceedings of the **Thirty-Second International Joint Conference on Artificial Intelligence**, (JCAI-23). International Joint Coferences on Artificial Intelligence Organization, 2023. Disponível em: https://doi.org/10.24963/ijcai.2023/742>. Acesso em: 20 nov. 2023.

HEIDEGGER, Martin. A questão da técnica. Scientiæ Studia v. 5, n. 3, p. 375-398, 2007.

HEIDEGGER, Martin. **Contribuições à Filosofia** (Do Acontecimento Apropriador). Rio de Janeiro: Via Verita, 2015.

HUSSERL, Edmund. **A filosofia como ciência de rigor.** Coimbra: Atlântida, 1965.

HUSSERL, Edmund. A crise das ciências europeias e a fenomenologia transcendental: um a introdução à filosofia fenomenológica. BIEMEL, Walter (Ed.). Rio de Janeiro: Forense Universitária, 2012.

JACOVI, Alon; MARASOIC, Ana; MILLER, Miller; and GOLDBERG, Yoav. Formalizing Trust in Artificial Intelligence: Prerequisites, Causes and Goals of Human Trust in Al. *In:* **ACM Conference on Fairness, Accountability, and Transparency (FAccT),** 2021, New York. [Proceedings of the...]. Fremont: Association for Computing Machinery (ACM), 2021. Disponível em: https://doi.org/10.1145/3442188.3445923>. Acesso em: 30 nov. 2023.

KNOWLES, Bran; FLEDDERJOHANN, Jasmine; RI-CHARDS, John. T., & VARSHNEY, Kush. R. (2023). Trustworthy AI and the Logics of Intersectional Resistance. *In:* **ACM Conference on Fairness, Accountability, and Transparency (FAccT),** 2023, New York. [Proceedings of the ...] Fremont: Association for Computing Machinery. Disponível em https://doi.org/10.1145/3593013.3593986>. Acesso em: 09 out. 2023.

Manheim, David. **Building a Culture of Safety for AI:** Perspectives and Challenges Social Science Research Network (SSRN), New York, Jun. 26, 2023. Disponível em: https://ssrn.com/abstract=4491421. Acesso em: 20 out. 2023.

PÉREZ Y MADRID, Aniceto; WRIGHT, Connor. **Trustworthy AI Alone Is Not Enough.** Madri: Editorial Dykinson, 2023. Disponível em: https://hdl.handle.net/10016/3. Acesso em: 30 nov. 2023.

REINO UNIDO. **Online Safety Act 2023.** CHAPTER 50, UK Public General Acts. Norwich - England, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50/enacted>. Acesso em: 15 nov. 2023.

SEN, Amartya. **A ideia de justiça.** São Paulo: Companhia das Letras, 2011.

SINGH, Richa; VATSA, Mayank; and RATHA, Nalini. Trustworthy Al. *In:* **3rd ACM India Joint International Conference on Data Science & Management of Data** (8th ACM IKDD CODS & 26th COMAD), 2021, New York. [Proceedings of the...]. Fremont: Association for Computing Machinery. Disponível em: https://doi.org/10.1145/3430984.3431966>. Acesso em: 30 nov. 2023.

Wachter, Sandra; Mittelstadt, Brent; Russell, Chris. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. **Computer Law & Security Review,** v. 41, 2021. Disponível em: http://dx.doi.org/10.2139/ssrn.3547922>. Acesso em: 10 ago. 2023.

WHITE HOUSE. **Fact Sheet:** President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. Washington, 30 out. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>. Acesso em: 15 nov. 2023.

Marcelo Pasetti

Doutorando em Filosofia pela PUCRS. Mestre em Fundamentos Constitucionais do Direito Público e do Direito Privado pela PUCRS.

Nythamar de Oliveira

Ph.D. in Philosophy pela State University of New York. Professor Titular da PUCRS.

Endereço para correspondência

MARCELO PASETTI

Av. Carlos Gomes, 1610, sala 607 Três Figueiras, 90480-002 Porto Alegre, RS, Brasil

NYTHAMAR DE OLIVEIRA

Pontifícia Universidade Católica do Rio Grande do Sul Av. Ipiranga 6681, prédio 8 Partenon, 90.619-900 Porto Alegre, RS, Brasil

Agradecimentos

Esta pesquisa está integrada ao Projeto RAIES (Rede de Inteligência Artificial Ética e Segura) com apoio da FAPERGS (Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul).

Os textos deste artigo forma revisados pela Mais H Consultoria Linguística Internacional e submetidos para validação dos autores antes da publicação.