

INTELIGÊNCIA ARTIFICIAL E GOVERNANÇA - UMA NECESSIDADE GLOBAL

ARTIFICIAL INTELLIGENCE AND GOVERNANCE - A GLOBAL NECESSITY

Flavio Cesar Vasconcellos Ferreira¹

Resumo: Através deste resumo expandido, buscou-se demonstrar que a evolução das aplicações da Inteligência Artificial tomou proporções irreversíveis no cotidiano dos indivíduos em todo o mundo e, conseqüentemente, a coleta, tratamento, uso e o compartilhamento de dados também alcançaram uma escala global. Empresas e desenvolvedores de Inteligência Artificial armazenam e comercializam dados de indivíduos como um ativo importante para os negócios, abrindo a possibilidade de utilizações não consentidas e manipulações em massa. Questões éticas passaram a integrar as discussões acerca dos limites e dos riscos que cercam a utilização dos sistemas de Inteligência Artificial, a proteção dos dados e as responsabilizações judiciais em casos de vazamento, mau uso ou roubo de dados. Ao examinar algumas propostas para regulamentações, este trabalho procurou contribuir para a discussão, trazendo a visão da governança como uma forma de auxiliar na supervisão, responsabilização e imposição de limites para as aplicações da Inteligência Artificial, de modo que os riscos de má utilização desses sistemas inteligentes sejam mitigados por meio do controle, da supervisão e da responsabilização de humanos.

Palavras-Chave: Inteligência Artificial; Governança; Regulamentação; Privacidade; Ética.

Abstract: Through this extended summary, it sought to demonstrate that the evolution of Artificial Intelligence applications has taken on irreversible proportions in the daily lives of individuals worldwide. Consequently, the collection, processing, use, and sharing of data have also reached a global scale. Companies and developers of Artificial Intelligence store and trade individual data as an important asset for business, opening up the possibility of non-consensual uses and mass manipulations. Ethical issues have become part of the discussions regarding the limits and risks surrounding the use of Artificial Intelligence systems, data protection, and legal liabilities in cases of data breaches, misuse, or theft. By examining some proposals for regulations, this paper aimed to contribute to the discussion by bringing the perspective of governance as a way to assist in supervision, accountability, and the imposition of limits on the applications of Artificial Intelligence, so that the risks of misuse of these intelligent systems are mitigated through control, supervision, and accountability of humans.

Keywords: Artificial Intelligence; Governance; Regulation; Privacy; Ethics.

¹ Administrador, Especialista em Compliance e Mestrando em Governança Corporativa pela FMU/Unifesp.

INTRODUÇÃO

Matéria do jornal norte-americano The New York Times, publicada em 16 de setembro de 2024, reportava que um grupo internacional de pesquisadores da Inteligência Artificial (IA) se reuniu para expressar suas preocupações com os avanços da tecnologia que auxiliaram a construir e que, segundo os cientistas, os avanços sinalizam que poderiam causar danos severos à sociedade.

Reunindo pesquisadores nos Estados Unidos, China, Grã-Bretanha, Cingapura, Canadá, entre outros países, o comunicado conjunto afirmou que a IA ultrapassaria a capacidade de seus criadores e, a consequente perda de controle humano, levaria a resultados severos para a humanidade. Os pesquisadores sugerem que os países deveriam articular a criação de um sistema global de supervisão que verificasse os riscos potencialmente graves apresentados pela tecnologia em rápida evolução.

De acordo com a reportagem, no início do mês de setembro de 2024, em Veneza, na Itália, pesquisadores de todo o mundo realizaram a terceira reunião do Diálogo Internacional sobre Segurança em I.A., que resultou em um alerta para que os governos saibam o que está em curso nos laboratórios de pesquisa e nas empresas que trabalham com sistemas de I.A. A proposta dos pesquisadores é pelo estabelecimento de autoridades de segurança em I.A. para acompanhar o desenvolvimento de sistemas dentro de suas fronteiras. Estas autoridades trabalhariam de forma articulada para o estabelecimento de sinais de que um sistema de I.A. poderia copiar-se ou ludibriar intencionalmente seus criadores ou controladores, coordenados por um corpo internacional.

Ainda segundo a matéria jornalística, movimentos governamentais neste sentido já ocorrem em países como os Estados Unidos, China e na Grã-Bretanha. O governo americano expediu uma ordem executiva exigindo que as empresas relatassem ao governo federal dos riscos que seus sistemas de I.A. poderiam representar, como a criação de armas de destruição em massa ou o potencial para uso em ações de terrorismo. A China possui um marco de segurança para as aplicações de I.A. e a Grã-Bretanha tem uma iniciativa mais ampla, reunindo oficiais de 28 países que concordaram em cooperar na avaliação dos riscos da I.A., mas ainda não houve a definição de políticas específicas para esta coordenação.

Como o avanço da tecnologia da I.A. ocorre rapidamente, é mais difícil que empresas e governos consigam abordá-la de forma isolada, por isso, a cooperação internacional é crucial para a segurança global, conclui a reportagem do The New York Times.

Justifica-se este estudo pela evidenciação de que a evolução segura da I.A. passa pela conjugação da proteção dos direitos fundamentais, como a privacidade e a não discriminação, com o fomento à inovação para pesquisas, máquinas, tecnologias e avanços que viabilizem soluções para problemas complexos. E a problemática proposta questiona “Como os mecanismos de governança poderiam se inserir na evolução segura das aplicações de I.A.?”.

Para atender ao proposto, a pesquisa documental foi utilizada como método de trabalho.

DISCUSSÕES E RESULTADOS

Houve um avanço legislativo na União Europeia que posiciona o bloco na vanguarda regulatória da I.A. Aprovado pelo Parlamento Europeu em 21 de maio de 2024, a Lei de Inteligência Artificial da União Europeia (IA Act) propõe uma abordagem baseada em riscos para a segurança, transparência e respeito aos direitos fundamentais no desenvolvimento e aplicação dos sistemas de I.A.

Os sistemas classificados como de risco inaceitável são as aplicações de I.A. consideradas como forma de ameaça ou de controle do indivíduo e, por estas características, serão proibidas. Aqui estão as aplicações para **manipulação cognitiva de comportamentos e para classificação social**, como os sistemas que utilizam **dados biométricos** para classificar o indivíduo por raça, religião ou orientação sexual, não permitidas na União Europeia.

Os sistemas de I.A. que apresentem um **risco considerado elevado são aqueles que afetam negativamente a segurança ou os direitos fundamentais e estarão sujeitos a um conjunto de requisitos e obrigações para que sejam autorizados a acessar o mercado da União Europeia. Os sistemas considerados de risco limitado deverão atender a algumas obrigações para transparência. E entre as aplicações consideradas como de risco mínimo estão os jogos com I.A. e os filtros de spam.**

Prevê ainda a legislação da União Europeia que os sistemas de I.A. serão avaliados antes de serem disponibilizados ao público e durante todo o seu ciclo de vida, bem como

poderão os indivíduos apresentarem queixas junto às autoridades nacionais competentes contra os sistemas que violem os termos da legislação.

Segundo o Parlamento Europeu, a IA Act visa a promoção, o desenvolvimento e a utilização de sistemas de I.A. **seguros** e confiáveis, que resguardecam o respeito aos **direitos fundamentais** dos cidadãos e estimulem o investimento e a inovação na União Europeia. A IA Act é restrita aos países do bloco e prevê algumas isenções, como para os sistemas exclusivamente militares e de defesa e os sistemas de investigação criminal.

Há também a previsão de uma estrutura de governança para apoiar a efetividade da IA Act na União Europeia, como a criação de uma comissão para fiscalizar o cumprimento regulatório na região, um painel científico independente para apoiar a execução, um comitê de aconselhamento à comissão e aos Estados-Membros e um fórum consultivo para oferecer conhecimentos técnicos.

As primeiras críticas à proposta regulatória da I.A. na União Europeia partem da abordagem da gestão de riscos que, usualmente, atua na medição, mitigação e aceitação dos riscos em favor de algum benefício. Ocorre que os avanços da I.A., além de rápidos, contemplam inúmeras áreas possíveis de aplicação e replicação. Isso dificulta a classificação dos riscos conforme proposta, uma vez que as aplicações, desdobramentos e consequências da I.A. são ilimitados. A utilização da gestão de riscos pode desconsiderar em sua análise os eventuais danos oriundos de direitos fundamentais, como os danos à dignidade humana, à liberdade e à igualdade e os danos de mais complexa mensuração prévia, como as questões de cunho emocional e social.

ÉTICA E AS APLICAÇÕES DE INTELIGÊNCIA ARTIFICIAL

Nas preocupações éticas derivadas das aplicações de I.A. encontram-se, por exemplo, os impactos sobre a privacidade e a coleta ostensiva, armazenamento e utilização de dados captados por dispositivos integrados à vida cotidiana, como aplicativos de segundo plano em smartphones, smartwatches e assistentes virtuais, que permanentemente coletam informações e podem gerar vulnerabilidades pelos potenciais violações de privacidade resultantes deste tipo de vigilância virtual.

A complexidade ética das aplicações de I.A. passa pela pelo fato de que os dados e as informações pessoais converteram-se em um ativo importante das empresas de tecnologia, do

desenvolvimento tecnológico e da economia. As legislações dos vários países sobre a proteção de dados renovaram a importância da atenção à privacidade e da necessidade do controle sobre a utilização de dados pessoais.

No ambiente regulatório brasileiro, a Lei nº 13.709/18, Lei Geral de Proteção de Dados, LGPD, estabeleceu em seu artigo vigésimo o direito do titular dos dados solicitar a revisão de decisões tomadas por tratamento automatizado de dados pessoais que afetem seus interesses, como decisões de consumo, de crédito ou de aspectos de sua personalidade. Tal previsão legal se mostra ainda mais relevante diante dos avanços verificados e previstos da I.A. que, conforme visto, caminha na direção da tomada de decisões autônomas com frequência cada vez maior. No entanto, verifica-se que não há clareza de que a revisão deva ser promovida obrigatoriamente por pessoa natural, o que permite interpretações divergentes do exercício do direito à revisão das decisões automatizadas.

É certo que as decisões humanas são influenciadas por variáveis diversas e que contém vieses, inclusive inconscientes, mas é igualmente seguro ponderar que decisões automatizadas não contenham critérios outros que não os originalmente concebidos, abrindo espaço para a criação de uma aprendizagem de máquina que pode comprometer ou ignorar direitos humanos fundamentais por não reconhecerem limites éticos.

RISCOS

Outro aspecto a ser considerado é o de ocorrência de quebras na segurança dos dados que permitam acessos não autorizados de forma acidental ou mesmo através de ações ilícitas deliberadas e que resultem na obtenção, manipulação ou divulgação dos dados armazenados. E como grande parte das atividades cotidianas ocorrem através de meios digitais, há maior e constante coleta de dados do indivíduo em poder das organizações e das tecnologias de I.A. Em caso de quebras na segurança dos dados, quanto maior a exposição dos dados pessoais, maiores poderão se tornar os riscos de manipulações ou de limitações do exercício dos direitos fundamentais, podendo mesmo alcançar o cerceamento de certos direitos.

De Sá e De Lima (2020) trazem questionamentos acerca da responsabilização em caso de danos ou de violações de direitos decorrentes do desenvolvimento e do emprego da I.A.

Primeiramente, sobre quem recai a responsabilidade jurídica? Sobre o cientista, que é o 'pai' da tecnologia? Sobre o proprietário da máquina inteligente? Sobre a pessoa que está utilizando e monitorando o sistema de IA? Sobre a pessoa que determina a qual propósito a máquina deverá servir? Ou seria possível conferir personalidade jurídica

aos robôs, autônomos e sistemas de IA, de modo a imputar-lhes o dever de ressarcir danos? (De Sá; De Lima, 2020, p. 240).

E continuam as autoras, trazendo questionamentos de outros tópicos relevantes acerca da responsabilização jurídica:

Como se faria a compensação do dano ou da violação de direito? Qual a natureza dessa responsabilidade? Deve ser promulgada lei prevendo novos tipos penais? E, caso se estenda a todos os participantes da cadeia, que se inicia com a concepção da máquina e finda com sua utilização, a responsabilização patrimonial deve ser solidária ou fracionária? (De Sá; De Lima, 2020, p. 240).

Observamos o desenvolvimento tecnológico e econômico global, fomentando a inovação, a livre iniciativa, a livre concorrência. Ao mesmo tempo, observamos o crescimento das preocupações com o respeito a privacidade, a informação, a liberdade de expressão e de opinião, a inviolabilidade da intimidade, da honra e da imagem.

O avanço e a disseminação da I.A. tangenciam os direitos humanos e a ética na responsabilização e proteção dos dados coletados, armazenados e utilizados para os mais diversos fins, em especial nas tomadas de decisões automatizadas e os riscos decorrentes. Os sistemas de I.A. impactam cada vez mais aspectos da sociedade, desde a privacidade pessoal até a segurança pública, colocando as implicações éticas e de direitos humanos como preocupações críticas que demandam ações imediatas.

A ESTRUTURA DE GOVERNANÇA APLICADA À INTELIGÊNCIA ARTIFICIAL

Hammad Raza, é Engenheiro da Computação e pesquisador na National College of Business Administration & Economics, no Paquistão e publicou em outubro de 2024 um artigo acadêmico ponderando a adoção de uma estrutura de governança eficaz para abordar tais desafios e estabelecer estruturas que protejam os direitos individuais, promovam a transparência e garantam a responsabilização em sistemas de I.A. Para Raza (2024), as considerações de direitos humanos para uma governança de I.A. envolvem a proteção da privacidade, a prevenção da discriminação e a garantia da justiça em processos automatizados de tomada de decisão, constituindo estes fatores que determinarão a confiabilidade em sistemas de I.A.

Raza defende que a estrutura de governança para sistemas de I.A. envolva a criação de mecanismos para auditoria de algoritmos, a divulgação de fontes de dados e de metodologias nas decisões automatizadas como forma de construir a confiança pública e permitir a supervisão

humana das decisões dos sistemas de I.A. Além destes atributos, a estrutura de governança devem incluir claros mecanismos de responsabilização, permitindo que as partes interessadas apresentem queixas e que eventuais danos causados pelas aplicações de I.A. sejam rapidamente detidos e reparados.

A estruturação desta governança inclui o estabelecimento de responsabilidades para desenvolvedores e operadores de I.A., priorizando a proteção da privacidade, transparência, justiça e responsabilização. As estruturas de governança devem assegurar que os sistemas de I.A. sejam implantados e atuem na defesa dos direitos fundamentais, ou seja, impondo limitações e supervisão para as decisões automatizadas de I.A. através da adoção de mecanismos claros e rigorosos protocolos de segurança contra violações, uso indevido e proteção de dados.

Uma das bases para a governança da I.A. começa pelos mecanismos de consentimento para a coleta, uso e compartilhamento de dados. O indivíduo deve ser claramente informado sobre os dados que serão coletados, como serão utilizados, quem terá acesso a eles e, se consentir a utilização, o consentimento deve ser facilmente revogado a qualquer instante, conferindo ao indivíduo a possibilidade de controle sobre seus próprios dados.

Princípios de minimização de dados e limitação de finalidade devem ser observados. Os sistemas de I.A. devem coletar somente os dados essenciais para seus objetivos específicos e não devem manter os dados além do período necessário a sua finalidade. Os sistemas de I.A. devem ser desenvolvidos tendo a privacidade por padrão e incorporados desde o desenvolvimento, assegurando que a privacidade esteja integrada aos processos desde sua concepção.

CONCLUSÃO

Em conclusão, a proposta de Raza é que uma estrutura de governança em I.A. é urgente para assegurar a transparência nas operações automatizadas e que a educação das partes interessadas através de uma estrutura de regramento apoiaria o estabelecimento de limites éticos e legais e a previsão de responsabilizações. A governança eficaz da I.A. requer uma abordagem abrangente para estabelecer o respeito aos direitos humanos, promover justiça e manter padrões éticos.

Braga et al (2024) relatam um modelo de governança em três níveis, sendo o primeiro no plano da infraestrutura técnica para acessos seguros, funcionais e robustos em termos de estabilidade e alcance. A segunda camada de governança recai sobre as aplicações e serviços disponibilizados de forma virtual, onde se situam as estruturas para a privacidade de dados, cibersegurança e livre concorrência, sendo necessárias permanente avaliação e revisões. A terceira camada se relaciona com os usuários, empresas, governos e a sociedade em geral para assegurar mecanismos de proteção e responsabilização por danos relacionados ao emprego da I.A. Concluem os autores que a governança para a regulamentação de protocolos, algoritmos, softwares e infraestrutura é algo complexo e em evolução, que envolve aspectos técnicos, políticos, econômicos, jurídicos, sociais, culturais e exigirá a participação de organismos globais, governos, empresas e sociedade civil. Não será uma solução centralizadora ou hierarquizada, mas distribuída, colaborativa e articulada conforme os riscos forem evoluindo.

Os sistemas de valores da governança regulam o relacionamento entre as partes, os propósitos estratégicos, a estrutura de poder e as práticas para a gestão. A aplicação dos princípios de equidade entre as partes, transparência, prestação de informações e a questão da conformidade com os regramentos aparecem aplicadas de forma customizada para contribuir com a necessidade da evolução segura da I.A. A inserção da governança nesta nova era do desenvolvimento da humanidade oferece a possibilidade de segurança para a disciplina e para a adequada aplicação da I.A., bem como a previsão de responsabilização e de sanções para os que optarem por desvios do caminho que a coletividade global entender como seguro e ético.

REFERÊNCIAS

BORGES, Davi Wesley, et al. As Leis de Proteção de Dados e Sua Aplicação ao Treinamento de IA. **Revista Foco**, 2024, 17.10: e6614-e6614.

BRAGA, Julião, et al. Como a Governança de Múltiplas Partes Interessadas Pode Moldar a IA Responsável. **OSF Preprint**, Março de 2024. Disponível em: <https://osf.io/preprints/osf/zeg9m>. Acesso em: 28 outubro 2024.

CONSELHO DA UNIÃO EUROPEIA. Regulamento Inteligência Artificial (IA): Conselho dá luz verde final às primeiras regras do mundo em matéria de IA. **Comunicado de Imprensa**. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/>. Acesso em: 30 outubro 2024.

DE SÁ, Maria de Fátima Freire; DE LIMA, Taisa Maria Macena. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil**, 2020, 26.04: 227-227.

LEI DE INTELIGÊNCIA ARTIFICIAL DA UNIÃO EUROPEIA (IA Act). **Website dedicado**. Disponível em: <https://artificialintelligenceact.eu/>. Acesso em: 29 outubro 2024.

RAZA, Hammad. Data Ethics and Human Rights: Designing Robust Governance Structures for AI Systems. **Researchgate.net**. 2024. 10.13140/RG.2.2.11535.80805.

TOBIN, Meaghan. A.I. Pioneers Call for Protections Against ‘Catastrophic Risks’. **The New York Times**. Nova Iorque, EUA. No 60.309, edição de 16 de outubro de 2024. Disponível em <https://www.nytimes.com/2024/09/16/business/china-ai-safety.html?searchResultPosition=4>. Acesso em: 25 outubro 2024.