

Uma Proposta de Requisitos Não Funcionais para Aderência de Sistemas Computacionais ao Projeto de Lei de Regulamentação da Inteligência Artificial

Giovanni Bruno T. de Carvalho¹, Gabriel da S. Belarmino¹,
Luiz Fernando F. P. de Lima^{2,1}, Danielle Rousy D. Ricarte¹

¹Centro de Informática – Universidade Federal da Paraíba – João Pessoa, PB, Brasil

²CESAR – Recife, PE, Brasil

giovannibrunocarvalho@gmail.com, gabriel.belarmino@academico.ufpb.br,

lffplima@gmail.com, danielle@ci.ufpb.br

Abstract. *This paper proposes non-functional requirements (NFR) to promote the oversight of artificial intelligence (AI) to the Bill 2338/2023, which aims to regulate the development and ethical use of AI in the country, due the growing need for AI regulation, which presents ethical and technical challenges, especially in complex and high-risk systems. From the Bill articles we identified 32 non-functional requirements were identified, categorized into seven groups of legal product requirements. The methodology included an exploratory analysis of Bill and specialized literature for requirements identification, with the application of a unified NFR taxonomy. The main results include the requirements organization, its accordance with the specialized literature, and the analyses of its use on AI software development. This work contributes to legal compliance and the implementation of governance practices that ensure security, transparency, and ethics in AI systems, establishing a basis for future research that validates and expands the set of proposed requirements.*

Resumo. *Este trabalho propõe requisitos não funcionais (RNFs) para promover a aderência de sistemas de inteligência artificial (IA) ao PL 2338/2023, que visa regular o desenvolvimento e a utilização ética da IA no país, dada a crescente necessidade de regulamentação da IA, que apresenta desafios éticos e técnicos, especialmente em sistemas complexos e de alto risco. A metodologia adotada incluiu uma análise exploratória do PL e da literatura para a identificação dos requisitos, com a aplicação de uma taxonomia unificada de RNFs. A partir desta análise foram identificados 32 requisitos não funcionais, categorizados em sete grupos de requisitos legais de produto. Os principais resultados incluem a organização dos requisitos, sua conformidade com a literatura especializada e a análise das vantagens de seu uso no desenvolvimento de sistemas de IA. O trabalho contribui para a conformidade legal e para a implementação de práticas de governança que garantam a segurança, transparência e ética nos sistemas de IA, estabelecendo uma base para futuras pesquisas que validem e ampliem o conjunto de requisitos propostos.*

1. Introdução

Nas últimas décadas, a Inteligência Artificial (IA) tem evoluído rapidamente, passando de uma área de pesquisa teórica para uma tecnologia amplamente utilizada em diversas indústrias, incluindo saúde, finanças, educação, e transporte. Tecnologias como aprendizado de máquina, redes neurais e processamento de linguagem natural estão na vanguarda dessa revolução, permitindo que sistemas de IA realizem atividades cada vez mais sofisticadas e autônomas [RUSSEL and NORVIG 2021].

No entanto, à medida que a IA se integra mais profundamente na sociedade, surgem questões complexas relacionadas à sua regulamentação, pois o crescimento acelerado trouxe preocupações significativas em relação à privacidade, transparência e segurança [KEARNS and ROTH 2019, FLORIDI et al. 2018]. Devido à globalização e ao amplo potencial de aplicação de sistemas baseados em IA, uma falha em uma aplicação de larga escala pode prejudicar milhões de pessoas, como observado em casos como o COMPAS nos Estados Unidos da América [ANGWIN et al. 2016]. No cenário brasileiro também se pode observar casos de discriminação algorítmica, especialmente em sistemas de visão computacional para identificação de potenciais suspeitos. Tais aplicações tendem a reconhecer, erroneamente, pessoas pretas que podem ser detidas injustamente [FALCÃO 2021]. Portanto, à medida que as previsões baseadas em algoritmos se tornam mais comuns nas empresas em diferentes aplicações, a necessidade de IA confiável se torna cada vez mais premente [SILVA and ALVES 2023].

A regulamentação da IA é um possível caminho para garantir que o desenvolvimento e a aplicação dessas tecnologias sejam conduzidos de maneira ética e segura. A falta de legislação pode resultar em riscos significativos, como a ampliação de vieses existentes, a violação de privacidade e a criação de desigualdades sociais [LUDGERO 2024]. Além disso, há preocupações sobre a transparência e a responsabilidade dos sistemas de IA, especialmente em áreas críticas como a tomada de decisões automatizadas em processos judiciais, diagnósticos médicos e concessão de crédito.

Neste contexto, a regulamentação da IA não se trata apenas de mitigar riscos, mas também de criar um ambiente onde a inovação possa prosperar de forma segura e inclusiva. Leis e diretrizes adequadas podem incentivar a concepção responsável da IA, promover a confiança do público nas tecnologias emergentes e assegurar que os benefícios da IA sejam amplamente distribuídos.

A União Europeia tem sido pioneira no debate sobre a regulamentação da IA, tendo debatido esse assunto ao longo de vários anos e indicando um comprometimento de longo prazo com novas leis. Em abril de 2021, a Comissão Europeia propôs a versão inicial do texto de lei para regulamentação, chamado de Artificial Intelligence Act (AI Act), que propõe a classificação dos sistemas em diferentes categorias de riscos e define requisitos para aplicações de IA de alto risco, enfatizando a transparência, a responsabilidade e a supervisão humana. O EU AI Act é alinhado com as definições de princípios propostos pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), e serviu de inspiração para a maioria das legislações ao redor do globo.

Neste sentido, mostrando preocupação com a regulamentação de sistemas de IA, parlamentares brasileiros elaboraram o Projeto de Lei nº 2338 de 2023. O PL 2338/2023 visa estabelecer diretrizes e normas para o uso de tecnologias de Inteligência Artificial no

Brasil e está em tramitação no plenário.

Elaborado por um grupo composto por juristas, especialistas e representantes da sociedade civil, o texto do PL 2338/2023 estabelece diversas normas para o concepção e a implementação de sistemas de IA por empresas, assim como tenta assegurar que as pessoas tenham o direito de compreender como interagir com esses sistemas e entender as suas tomadas de decisão.

Apesar do avanço de legislações, muitas organizações podem enfrentar desafios durante a adaptação de seus sistemas de IA às exigências legais. A ausência de diretrizes claras sobre como traduzir essas leis em requisitos técnicos, especialmente requisitos não funcionais, cria uma distância entre o desenvolvimento de IA e sua conformidade legal.

Nota-se, assim, a necessidade de criação de mecanismos para auxiliar as organizações a atingir a conformidade com o PL 2338/2023, uma vez que as propostas e discussões são ainda incipientes. Pode-se pensar, por exemplo, em definir um conjunto de requisitos não funcionais (RNFs) para auxiliar empresas e desenvolvedores a atingir tal conformidade. RNFs são o conjunto de requisitos de um sistema que não estão diretamente relacionados às suas funcionalidades, mas sim à questões de confiabilidade, performance e restrições (de hardware ou legais), por exemplo [SOMMERVILLE 2007].

Portanto, no contexto da conformidade de sistemas de IA à regulamentações relacionadas, RNFs como segurança, auditabilidade e transparência, podem ser essenciais para garantir que seu desenvolvimento esteja aderente à tais legislações. Apesar disso, a definição destes requisitos podem não ser identificada ou priorizada no processo de desenvolvimento.

Deste modo, o objetivo geral deste trabalho é propor um conjunto de requisitos não funcionais que auxiliam a aderência de algoritmos de Inteligência Artificial às legislações, usando como base o PL 2338/2023. Com isso, esperamos contribuir para a produção de tecnologias mais seguras, transparentes e alinhadas aos princípios éticos e legais. Através dessa proposta, busca-se oferecer um referencial prático para empresas e desenvolvedores que desejam assegurar a conformidade de seus sistemas de IA com a legislação nacional.

Ao propor um conjunto de requisitos que possa guiar a elaboração de sistemas de IA de maneira consistente com as regulamentações, este trabalho busca facilitar o alinhamento entre tecnologia e leis, contribuindo para o desenvolvimento de sistemas mais seguros e transparentes. Isso não só beneficia as organizações que desenvolvem e utilizam algoritmos inteligentes, mas também promove uma maior confiança pública na adoção dessa tecnologia.

Em sua estrutura, o presente artigo apresenta nas Seções 2 e 3 um resumo sobre o Projeto de Lei 2338/2023 e sobre a taxonomia usada como base neste trabalho. A Seção 4 apresenta a metodologia empregada. Na Seção 5, são expostos os RNFs identificados e uma discussão sobre eles. A Seção 6 descreve as conclusões e trabalhos futuros.

2. Projeto de Lei 2338/2023

O PL 2338/2023 [PL-2338/2023 2023] estabelece diretrizes para o desenvolvimento, implementação e uso de sistemas de inteligência artificial no Brasil. Seu objetivo principal é assegurar que esses sistemas sejam utilizados de maneira ética, segura e responsável, promovendo o bem-estar social e evitando prejuízos a indivíduos ou coletividades. O Ar-

tigo 2º do projeto de lei apresenta fundamentos relevantes para o desenvolvimento, a implementação e o uso de sistemas de IA no país, como a centralidade da pessoa humana, o respeito aos direitos humanos, a não discriminação e a privacidade e proteção de dados.

Além dos princípios para o desenvolvimento e uso da IA, o PL também apresenta outros pontos importantes, como a categorização dos riscos, sanções e a promoção da pesquisa em IA. O Projeto de Lei ainda define alguns conceitos e agentes importantes envolvidos no desenvolvimento deste tipo de aplicação. Neste trabalho, seguimos as mesmas definições, sendo elas:

1. Sistema de inteligência artificial: sistema computacional desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento;
2. Fornecedor de sistema de inteligência artificial: pessoa natural ou jurídica, de natureza pública ou privada, que desenvolva um sistema de inteligência artificial com vistas à sua colocação no mercado ou à sua aplicação em serviço por ela fornecido;
3. Operador de sistema de inteligência artificial: pessoa natural ou jurídica, de natureza pública ou privada, que empregue ou utilize sistema de inteligência artificial, salvo se o referido sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional;
4. Agentes de inteligência artificial: fornecedores e operadores de sistemas de inteligência artificial;
5. Autoridade competente: órgão ou entidade da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional;
6. Discriminação: qualquer distinção, exclusão, restrição ou preferência, em qualquer área da vida pública ou privada, cujo propósito ou efeito seja anular ou restringir o reconhecimento, gozo ou exercício, em condições de igualdade, de um ou mais direitos ou liberdades previstos no ordenamento jurídico, em razão de características pessoais como origem geográfica, raça, cor ou etnia, gênero, orientação sexual, classe socioeconômica, idade, deficiência, religião ou opiniões políticas;
7. Discriminação indireta: discriminação que ocorre quando normativa, prática ou critério aparentemente neutro tem a capacidade de acarretar desvantagem para pessoas pertencentes a grupo específico, ou as coloquem em desvantagem, a menos que essa normativa, prática ou critério tenha algum objetivo ou justificativa razoável e legítima à luz do direito à igualdade e dos demais direitos fundamentais.

Em relação aos riscos dos sistemas baseados em IA, o PL 2338/2023 estabelece critérios de risco específicos para a classificação de sistemas de inteligência artificial, definindo dois níveis principais: risco excessivo e alto risco. Esta categorização visa diferenciar o grau de impacto que esses sistemas podem causar à segurança, aos direitos e às liberdades das pessoas e, assim, determinar o nível de controle regulatório necessário para garantir sua conformidade.

Sistemas de risco excessivo são considerados os mais prejudiciais, apresentando potenciais impactos significativos à integridade física, aos direitos fundamentais e à vida das pessoas, sendo proibidos pelo presente PL.

Já aplicações categorizadas de alto risco, embora não proibidas, são regulamentadas de forma rigorosa devido ao seu impacto potencial em setores críticos, como saúde, educação, segurança pública e justiça. De modo que o PL exige a implementação de controles específicos para garantir que esses sistemas sejam explicáveis, auditáveis e projetados para minimizar vieses discriminatórios.

Tais definições expostas no Projeto de Lei 2338/2023 mostram a importância de se construir mecanismos para que as empresas e desenvolvedores consigam melhor se adequar ao proposto na regulamentação quando esta for sancionada. Mas, mesmo antes da sanção, se tratando de aplicações com possíveis impactos e riscos na sociedade, é importante que passemos a considerar tais aspectos no desenvolvimento de nossas aplicações baseadas em IA.

3. Taxonomia unificada para RNF

[BENITTI and RHODEN 2015] apresentaram uma taxonomia unificada, a partir de diferentes taxonomias propostas na literatura para requisitos não funcionais. Em seu trabalho, abrangeram 90 aspectos relacionados aos RNFs, de modo a organizar os requisitos, facilitando a verificação, validação e reutilização.

A taxonomia unificada considera as taxonomias propostas por [SOMMERVILLE 2007] e pela norma [ISO/IEC-25010:2010 2010]. A primeira divide os RNFs em três classes: (1) produto - que especificam os atributos de qualidade que o sistema deve apresentar; (2) organizacionais - que são derivados de políticas e procedimentos da organização; e (3) externos - que abrangem todos os requisitos derivados de fatores externos ao sistema e o seu processo.

Já a taxonomia proposta pela [ISO/IEC-25010:2010 2010] baseia-se no segundo nível, dividindo os requisitos de produto de acordo com as sete características principais do software: confiabilidade, compatibilidade, usabilidade, eficiência, segurança, manutenibilidade e portabilidade.

Na proposta das autoras, os requisitos organizacionais e externos são divididos segundo a taxonomia definida por [SOMMERVILLE 2007], que divide os requisitos organizacionais entre comerciais e restrições de desenho/projeto, e divide os requisitos externos entre legais e éticos. Além disso, os requisitos de produto são destrinchados pelas categorias identificadas na norma [ISO/IEC-25010:2010 2010]. A Figura 1 apresenta a taxonomia unificada de RNFs proposta por [BENITTI and RHODEN 2015].

Neste trabalho foi adotada a taxonomia unificada apresentada na Figura 1 para identificar e classificar os requisitos não funcionais para sistemas de IA com base no PL 2338/2023. Esses resultados são explanados nas seções seguintes.

4. Metodologia

Neste trabalho tivemos como objetivo mapear RNFs para conformidade com a proposta de regulamentação de IA no Brasil. Para isso, foram necessárias etapas de imersão e revisão do texto do projeto de lei e literatura especializada sobre aspectos éticos no desenvolvimento de sistemas inteligentes.

Deste modo, aplicamos uma abordagem exploratória e descritiva. O caráter exploratório se justifica pela investigação da proposta de regulamentação de IA no Brasil, além

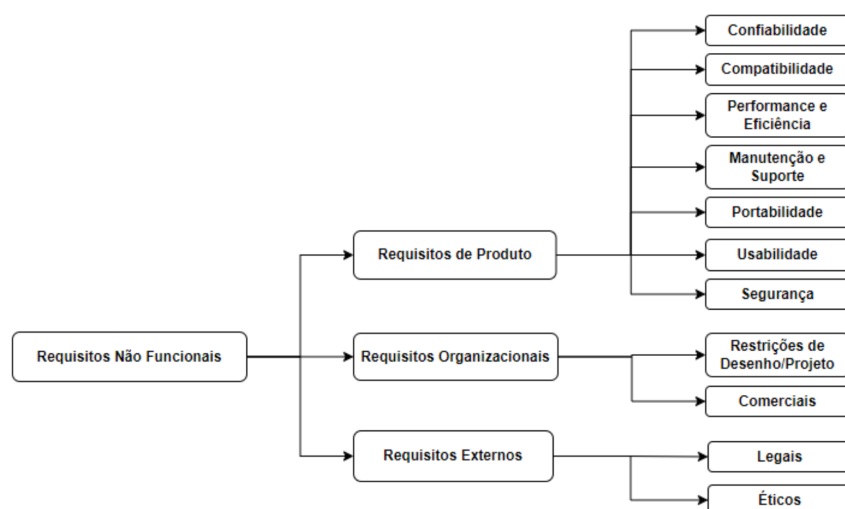


Figure 1. Taxonomia unificada dos RNF [BENITTI and RHODEN 2015]

da análise de artigos científicos e documentos legais. O objetivo foi identificar as principais diretrizes e requisitos que possam ser aplicados ao desenvolvimento de sistemas baseados IA, estabelecendo uma base sólida para a proposta de requisitos não funcionais.

Já o aspecto descritivo visa documentar de forma clara o processo de elaboração desses requisitos com base na legislação existente. Deste modo, buscamos responder a seguinte questão de pesquisa: É possível identificar um conjunto básico de requisitos não funcionais essenciais que todo sistema de IA deve se preocupar durante sua fase de desenvolvimento considerando o PL 2338/2023? Caso positivo, quais seriam eles?

Com a análise do PL buscou-se identificar os requisitos de conformidade legal, tanto em nível de proteção de dados e privacidade, quanto em transparência e acessibilidade dos sistemas. Essa etapa forneceu subsídios para mapear requisitos relevantes para os sistemas de IA, servindo como base para a formulação dos RNFs propostos.

A partir do mapeamento das exigências legais do PL 2338/2023, foram extraídos requisitos que se enquadram em categorias propostas pela taxonomia unificada apresentada na Seção 3 como segurança, usabilidade, confiabilidade, entre outros. Cada requisito proposto foi detalhado de forma a garantir que o desenvolvimento de sistemas baseados em IA esteja em conformidade com as obrigações legais e éticas delineadas pela regulamentação analisada.

Por fim, realizou-se uma avaliação com dois especialistas para validar e incorporar apontamentos externos. Tal validação se deu com a apresentação dos requisitos mapeados e classificados na taxonomia. Com esta seção com especialistas foi possível evoluir algumas das classificações dos RNFs, deixando-as mais adequadas ao contexto do PL. O resultado final do mapeamento dos RNFs com os apontamentos dos especialistas são apresentados na Seção 5. Entendemos que, apesar de valiosa, o número pequeno de especialistas consultados foi uma limitação deste trabalho.

5. Resultados e Discussões

Nesta Seção apresentamos e discutimos os principais RNFs mapeadas, em conformidade com o PL 2338/2023, que se aplicam ao desenvolvimento de sistemas de IA, incluindo

segurança, acessibilidade, transparência e explicabilidade. Além disso, discutimos como esses requisitos são cruciais para a aderência legal e os desafios que podem surgir durante a sua implementação em sistemas de IA. Nesta Seção destacaremos alguns dos RNFs mapeados por categoria e os demais podem ser consultados no repositório do projeto¹.

5.1. Mapeamento dos RNFs com base no PL 2338/2023

A partir da taxonomia unificada de tipos de RNFs proposta por [BENITTI and RHODEN 2015], realizamos uma modificação para adequá-la ao nosso problema. Como todos os RNFs aqui levantados são baseados em uma legislação, todos eles se enquadram na classificação de requisitos legais pela definição de [SOMMERVILLE 2007], portanto todos também são requisitos externos. Contudo eles também refletem em outros aspectos específicos associados com o produto sendo desenvolvido.

Assim, entendemos que os requisitos não funcionais extraídos da legislação são também requisitos de produto e fazem parte dos requisitos legais do projeto. Em nossa adequação da taxonomia, os requisitos éticos também fazem parte dos requisitos de produto. Além disso, identificamos uma categoria de requisitos para os sistemas de IA, que são os requisitos de transparência (não foram identificados requisitos de compatibilidade e portabilidade). A proposta de RNFs e suas classificações são apresentadas na Figura 2.

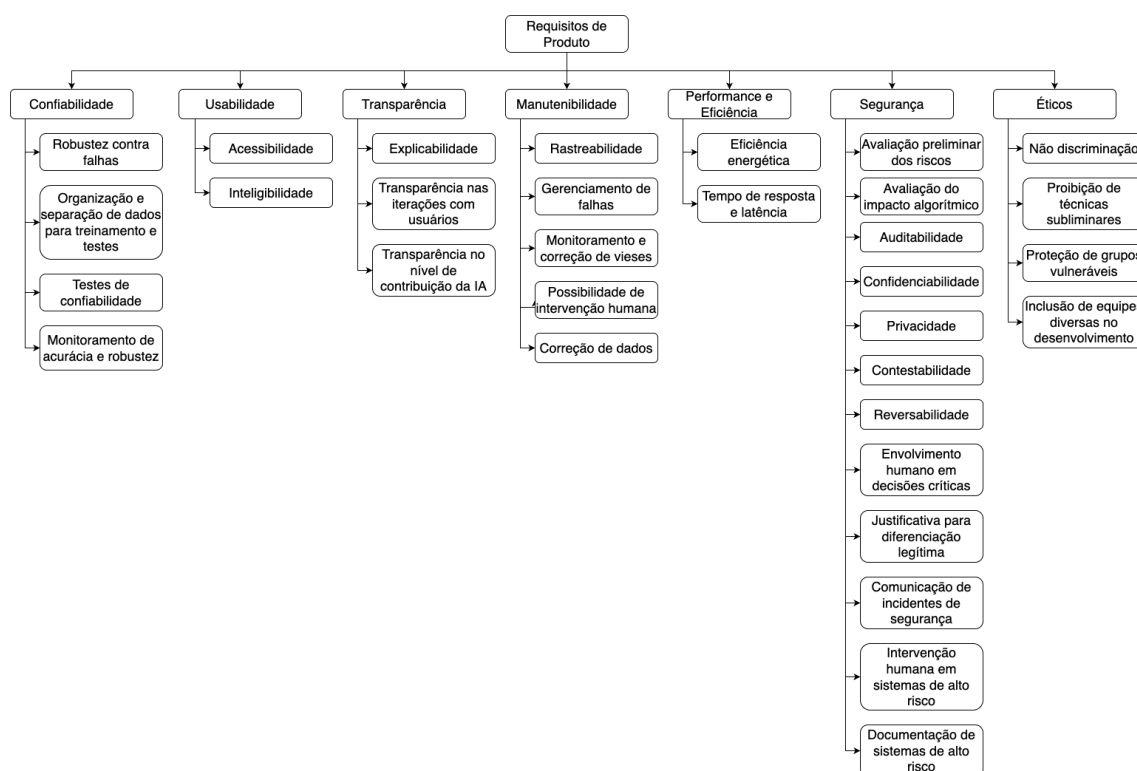


Figure 2. RNFs propostos em aderência ao PL 2338/2023

Foram mapeados 32 RNFs baseados no PL 2338/2023. A Tabela 1 apresenta a relação de cada RNF com os Artigos propostos no projeto de regulamentação. De

¹<https://github.com/GiovanniBru/rnf-pl-regulamentacao-ia>

modo geral os RNFs identificados estão alinhados também com a literatura especializada. Por exemplo, os requisitos de transparência dizem respeito a técnicas de explicabilidade e clareza de autonomia para os usuários de sistemas baseados em IA [BELLE and PAPANTONIS 2021]. Bem como os requisitos éticos estão diretamente relacionados com trabalhos sobre o impacto da diversidade de times e em como podemos usar técnicas de equidade algorítmica para mitigar discriminações nos modelos criados [LEAVY 2018, SANTOS et al. 2024].

ID	Requisito	Classificação	Princípio Regulatório
RFN.C01	Robustez contra falhas	Confiabilidade	Art. 3º
RFN.C02	Organização e separação de dados para treinamento e testes	Confiabilidade	Art. 19º
RFN.C03	Testes de confiabilidade periódicos	Confiabilidade	Art. 20º
RFN.C04	Monitoramento de acurácia e robustez	Confiabilidade	Art. 20º
RFN.U01	Acessibilidade	Usabilidade	Art. 2º e Art. 3º
RFN.U02	Inteligibilidade	Usabilidade	Art. 3º
RFN.T01	Explicabilidade	Transparência	Art. 3º, Art. 5º, Art. 7º, Art. 8º, Art. 9º e Art. 20º
RFN.T02	Transparência nas interações com usuários	Transparência	Art. 19º
RFN.T03	Transparência no nível de contribuição da IA	Transparência	Art. 19º
RFN.M01	Rastreabilidade	Manutenibilidade	Art. 3º e Art. 7º
RFN.M02	Gerenciamento de falhas	Manutenibilidade	Art. 3º
RFN.M03	Monitoramento e correção de vieses	Manutenibilidade	Art. 5º e Art. 19º
RFN.M04	Possibilidade de intervenção ou revisão humana	Manutenibilidade	Art. 8º e Art. 10º
RFN.M05	Correção de dados	Manutenibilidade	Art. 9º
RFN.P01	Eficiência energética	Performance	Art. 2º
RFN.P02	Tempo de resposta e latência	Performance	Art. 2º
RFN.E01	Avaliação preliminar de riscos	Segurança	Art. 13º
RFN.E02	Avaliação de impacto algorítmico	Segurança	Art. 22º
RFN.E03	Auditabilidade	Segurança	Art. 3º
RFN.E04	Confidencialidade	Segurança	Art. 3º e Art. 5º
RFN.E05	Privacidade	Segurança	Art. 3º e Art. 19º
RFN.E06	Contestabilidade	Segurança	Art. 5º e Art. 9º
RFN.E07	Reversabilidade	Segurança	Art. 5º
RFN.E08	Envolvimento humano em decisões críticas	Segurança	Art. 11º
RFN.E09	Justificativa para diferenciação legítima	Segurança	Art. 12º
RFN.E10	Comunicação de incidentes de segurança	Segurança	Art. 31º
RFN.E11	Intervenção humana em sistemas de alto risco	Segurança	Art. 20º
RFN.E12	Documentação de sistemas de alto risco	Segurança	Art. 20º
RFN.E01	Não-discriminação	Éticos	Art. 2º, Art. 3º, Art. 5º, Art. 7º, Art. 9º, Art. 12º e Art. 20º
RFN.E02	Proibição de técnicas subliminares	Éticos	Art. 14º
RFN.E03	Proteção de grupos vulneráveis	Éticos	Art. 14º
RFN.E04	Inclusão de equipes diversas no desenvolvimento	Éticos	Art. 20º

Table 1. Relação entre os RNFs e os princípios regulatórios do PL 2338/2023

Para exemplificar o uso prático dos RNFs apresentados podemos detalhar alguns dos requisitos propostos. Por exemplo, o requisito de monitoramento e correção de vieses diz que “O sistema de IA deve ter mecanismos de monitoramento contínuo para identificar e corrigir vieses discriminatórios, assegurando que os resultados sejam justos e imparciais para todos os grupos”.

Considerando tal RNF um time de desenvolvimento pode elencar métricas de justiça algorítmica para avaliação, identificar quais atributos devem ser classificados como atributos protegidos, bem como identificar quais os grupos (majoritários e minoritários) nesses atributos. Além disso, o time pode estabelecer o limiar em que as métricas monitoradas devem performar, assim permitindo que a equipe possa garantir tal monitoramento. Sendo estes aspectos totalmente relacionados com técnicas e práticas recomendadas pela comunidade [MEHRABI et al. 2019, DE LIMA et al. 2024].

Exemplificando agora o RNF sobre eficiência energética que tem como descrição “O sistema de IA deve ser projetado para otimizar o uso de recursos computacionais, minimizando o impacto ambiental por meio de práticas sustentáveis de desenvolvimento e operação”. Tal requisito está alinhado com a literatura no que diz respeito

aos impactos ambientais do treinamento dos modelos de aprendizado de máquina [BENDER et al. 2021]. Com este requisito os responsáveis podem elencar o consumo médio que uma rodada de treinamento do modelo deve apresentar. Podendo ser uma métrica norteadora, inclusive, para a escolha do algoritmo que será treinado.

5.2. Vantagens e desafios da conformidade

Garantir a conformidade dos sistemas de inteligência artificial com os requisitos não funcionais não apenas mitiga riscos legais e sanções previstas no PL 2338/2023, mas também traz vantagens estratégicas para as organizações. Primeiramente, a compatibilidade com regulamentações internacionais, como o RGPD e o EU AI Act, fortalece a competitividade global das empresas brasileiras, ampliando suas oportunidades de mercado. Além disso, a conformidade melhora a confiança do público e dos consumidores, especialmente em setores sensíveis, ao demonstrar compromisso com transparência, segurança e ética.

A conformidade pode aprimorar a eficiência operacional e a sustentabilidade financeira, pois a adoção de práticas rigorosas de segurança e monitoramento reduz falhas inesperadas, minimizando custos com correções e evitando danos à reputação da empresa. Manter a aderência aos RNFs também torna as organizações mais resilientes a mudanças regulatórias, garantindo uma adaptação mais ágil a novas exigências legais e do mercado.

No entanto, a busca pela conformidade apresenta desafios. A implementação dos RNFs exige investimentos em infraestrutura tecnológica, auditorias contínuas e equipes especializadas para monitoramento e adaptação dos sistemas. Modelos complexos de IA, especialmente aqueles baseados em *deep learning*, podem dificultar a explicabilidade e a rastreabilidade das decisões, tornando a transparência um obstáculo técnico relevante. Além disso, corrigir vieses algorítmicos e garantir a segurança dos sistemas são processos contínuos, que demandam recursos e metodologias adequadas.

Dessa forma, a conformidade com a regulamentação de IA não deve ser vista apenas como um custo ou uma exigência regulatória, mas como uma prática estratégica que equilibra inovação e responsabilidade, mitigando riscos e promovendo um ambiente mais seguro e confiável para o desenvolvimento e uso da inteligência artificial.

6. Conclusões

O presente trabalho abordou a proposta de um conjunto de requisitos não funcionais para sistemas de inteligência artificial, embasados na proposta regulamentação brasileira (PL 2338/2023). Através de uma análise detalhada da lei, foram identificados 32 RNFs distintos, os quais foram organizados em sete categorias principais, baseando-se em uma taxonomia unificada de RNFs proposta na literatura.

Esse mapeamento teve como objetivo proporcionar uma estrutura de governança para a implementação de sistemas de IA que estejam em conformidade com as diretrizes nacionais, oferecendo, assim, maior segurança jurídica, ética e técnica para esses sistemas. Portanto, mesmo sem a aprovação do projeto de lei, a aplicação dessa estrutura de governança é útil para o aprimoramento da eficiência organizacional e para garantir a confiança do usuário.

Dada a amplitude do tema e o ritmo acelerado das atualizações regulatórias e tecnológicas, há diversas oportunidades para o aprofundamento deste estudo. Primeiramente, para mitigar a limitação que este trabalho apresentou em relação ao baixo

número de avaliadores consultados, pode-se realizar entrevistas com um maior conjunto de profissionais e acadêmicos, visando validar os requisitos não funcionais propostos neste trabalho e obter uma perspectiva prática sobre sua aplicabilidade no contexto da regulamentação brasileira, como também a identificação de métricas que suportem a validação dos RNFs identificados.

Ainda este sentido também pode-se realizar avaliações com usuários de sistemas baseados em IA buscando validar se o uso dos RNFs propostos no desenvolvimento de sistema computacionais tem relevância para aumentar a sua confiança em relação ao uso de tais sistemas. Por fim, ainda elencamos outra linha promissora de pesquisa que envolve o acompanhamento das emendas que venham a ser aprovadas após a votação da PL 2338/2023. As atualizações legais podem impactar diretamente os requisitos de conformidade e segurança, além de afetar as sanções e procedimentos de governança.

References

- ANGWIN, J., LARSON, J., MATTU, S., and KIRCHNER, L. (2016). Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks.
- BELLE, V. and PAPANTONIS, I. (2021). Principles and practice of explainable machine learning. *Frontiers in big Data*, 4:688969.
- BENDER, E. M., GEBRU, T., MCMILLAN-MAJOR, A., and SHMITCHELL, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, FAccT '21, page 610–623, New York, NY, USA. Association for Computing Machinery.
- BENITTI, F. B. V. and RHODEN, J. S. (2015). Uma taxonomia unificada para requisitos não funcionais. *Revista Electronica de Sistemas de Informacao*, 14(3):1.
- DE LIMA, L. F. F. P., RICARTE, D. R. D., and SIEBRA, C. A. (2024). A benchmark proposal for non-generative fair adversarial learning strategies using a fairness-utility trade-off metric. *Computational Intelligence*, 40(5):e70003.
- FALCÃO, C. (2021). Lentes racistas: Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial.
- FLORIDI, L. et al. (2018). Ai4people—an ethical framework for a good ai society: Opportunities, risks, principles, and recommendations. *Minds and machines*, 28(4):689–707.
- ISO/IEC-25010:2010 (2010). Systems and software engineering — systems and software quality requirements and evaluation (square) — system and software quality models. <https://www.iso.org/standard/35733.html>.
- KEARNS, M. and ROTH, A. (2019). *The ethical algorithm: The science of socially aware algorithm design*. Oxford University Press.
- LEAVY, S. (2018). Gender bias in artificial intelligence: The need for diversity and gender theory in machine learning. In *Proceedings of the 1st international workshop on gender equality in software engineering*, pages 14–16.
- LUDGERO, P. R. (2024). Desafios da regulamentação da inteligência artificial: Uma análise crítica das propostas legislativas.

- <https://www.jusbrasil.com.br/artigos/desafios-da-regulamentacao-da-inteligencia-artificial-uma-analise-critica-das-propostas-legislativas/2293750067>.
- MEHRABI, N. et al. (2019). A survey on bias and fairness in machine learning. *arXiv preprint arXiv:1908.09635*.
- PL-2338/2023 (2023). "https://www25.senado.leg.br/web/atividade/materias/-/materia/157233".
- RUSSEL, S. and NORVIG, P. (2021). *Artificial intelligence: a modern approach*. Person, 4rd edition.
- SANTOS, R. S., DE LIMA, L. F. F. P., BALDASSARRE, M. T., and SPÍNOLA, R. (2024). Preliminary insights on industry practices for addressing fairness debt. In *Proceedings of the 18th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, pages 566–571.
- SILVA, K. L. and ALVES, L. H. (2023). Um estudo da regulamentação da inteligência artificial no brasil no contexto dos projetos de lei nº 5.051/2019, 21/2020, 872/2021 e 2.338/2023. <https://repositorio.animaeducacao.com.br/handle/ANIMA/33863>.
- SOMMERVILLE, I. (2007). *Engenharia de software*. Addison Wesley, 8 edition.