

v. 05, n° 02 - jul/dec 2025

ISSN 2763-8685

LATIN AMERICAN JOURNAL OF EUROPEAN STUDIES

TABLE OF CONTENTS

EDITORIAL	7
-----------	---

DOSSIER - DIGITAL TRANSFORMATION AND INNOVATIVE SOLUTIONS

FROM TRANSPARENCY TO STANDARDS: THE ROLE OF THE TBT AGREEMENT IN ADDRESSING AI REGULATORY CHALLENGES	14
--	----

Milena da Fonseca Azevedo

TRANSFORMAÇÕES DIGITAIS E PATENTES: SEP E LICENÇA FRAND	41
---	----

*Luiz Otávio Pimentel
Ana Paula Gomes Pinto*

PATENTES ESENCIALES A LAS NORMAS TÉCNICAS DE SERVICIOS: SSEP DIGITALES EN EL SISTEMA MULTILATERAL DE COMERCIO	59
---	----

Fabíola Wüst Zibetti

DIGITAL SOVEREIGNTY IN THE CLOUD AND INTERNATIONAL LAW: TOWARDS A BALANCE BETWEEN STATE AUTONOMY AND TRANSNATIONAL CYBER GOVERNANCE	84
---	----

Danilo Garcia Caceres

EL CAMINO AL FORTALECIMIENTO DE LA COOPERACIÓN ESTRATÉGICA DIGITAL ENTRE LA UNIÓN EUROPEA Y AMÉRICA LATINA Y EL CARIBE	106
--	-----

Keren Susana Herrera Ciro

BETWEEN INNOVATION AND RISK:REGULATING ARTIFICIAL INTELLIGENCE UNDER BRAZILIAN BILL NO. 2,338/2023 AND THE EU AI ACT (REGULATION (EU) 2024/1689 - CHALLENGES FOR THE PROTECTION OF FUNDAMENTAL RIGHTS	140
---	-----

*Álvaro Sampaio Corrêa Neto
Cristina Mendes Bertoncini Corrêa
Desirré Dornelles de Ávila Bollmann*

A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS EM SISTEMAS DE RISCO ELEVADO NO REGULAMENTO DE INTELIGÊNCIA ARTIFICIAL DA UNIÃO EUROPEIA 174

Victória Fernandes de Moraes

ARTIFICIAL INTELLIGENCE: CHALLENGES OF EXPLAINABILITY ON DISINFORMATION THROUGH CHATBOTS 207

René Palacios Garita

LA EVOLUCIÓN Y APORTACIÓN EUROPEA EN EL RECONOCIMIENTO DE LA AUTODETERMINACIÓN INFORMATIVA Y LA PROTECCIÓN DE DATOS PERSONALES COMO DERECHOS HUMANOS, 229

Eduardo Kanahuati Fares

A PROTEÇÃO DAS GERAÇÕES FUTURAS NO CONSTITUCIONALISMO DIGITAL: SUSTENTABILIDADE, RESPONSABILIDADE E JUSTIÇA INTERGERACIONAL 256

Luis Clóvis Machado da Rocha Junior

AUTOMAÇÃO INTELIGENTE E EXCLUSÃO INTERGERACIONAL: UMA PROPOSTA DE CONTRIBUIÇÃO PARA A SEGURANÇA SOCIAL 275

Claudia Marchetti da Silva

CRIPTOMINERÍA Y SU HUELLA ECOLÓGICA: UN ESTUDIO PREVIO DE LA SITUACIÓN EN PARAGUAY 294

*Danielle de Ouro Mamed
Cecílio Arnaldo Rivas Ayala
Noelia Bernadett Ozuna González*

PROCESO DIGITAL EN EL PODER JUDICIAL BRASILEÑO: CRISIS Y OPORTUNIDADES 320

Claudio Eduardo Regis de Figueiredo e Silva

**CONCIL-IA PROJECT: FINAL FINDINGS AND DIGITAL INNOVATIONS
FOR CONFLICT RESOLUTION** **343**

*Maykon Marcos Júnior
Guilherme de Brito Santos
João Gabriel Mohr
Andressa Silveira Viana Maurmann
Luísa Bollmann
Arthur Machado Capaverde
Cristian Alexandre Alchini
Maite Fortes Vieira
Lucas de Castro Rodrigues Pereira
Isabela Cristina Sabo
Aires José Rover*

**CONTRATOS ELETRÔNICOS REALIZADOS POR MEIO DO APLICATIVO
WHATSAPP: UM ESTUDO ENTRE BRASIL E UNIÃO EUROPEIA** **370**

*Elaine Sant'Anna de Carvalho
Geanne Gschwendtner de Lima
Thainá Schroeder Ribeiro*

ARTICLES

**NOTAS SOBRE LA REFORMA DE LA CORTE INTERAMERICANA DE
DERECHOS HUMANOS** **390**

Manuel Becerra Ramírez

**EL RÉGIMEN GLOBAL DE SANCIONES DE LA UNIÓN EUROPEA COMO
INSTRUMENTO FRENTE A LAS GRAVES VIOLACIONES DE DERECHOS
HUMANOS EN AMÉRICA LATINA: FUNDAMENTOS, APLICACIÓN Y
COMPARACIÓN CON EL SISTEMA INTERAMERICANO DE DERECHOS
HUMANOS** **412**

*Carol Jazmín Orbegoso Moreno
Patricia Cristina Vega Pacheco
Jose Rodrigo Alva Gastañadui*

**LA GLOBALIZACIÓN DE LOS CONCEPTOS DEMOCRÁTICOS Y DE
ESTADO DE DERECHO DE LA UNIÓN EUROPEA: EL CASO DE AMÉRICA
LATINA Y EL CARIBE** **469**

Nuria Puentes Ruiz

A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS EM SISTEMAS DE RISCO ELEVADO NO REGULAMENTO DE INTELIGÊNCIA ARTIFICIAL DA UNIÃO EUROPEIA^{1,2}

Victória Fernandes de Moraes³

RESUMO: Em 1º de agosto de 2024 entrou em vigor o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, que estabelece regras harmonizadas sobre inteligência artificial, o denominado Regulamento de Inteligência Artificial (AI Act). Embora sua plena aplicação esteja prevista para os próximos anos, o AI Act já se consolida como um marco normativo global. Estruturado a partir de uma abordagem baseada em riscos, o regulamento busca assegurar a segurança, a transparência e o respeito aos direitos fundamentais. Por meio de revisão bibliográfica e documental, este trabalho analisa as obrigações impostas aos sistemas de risco elevado pelo AI Act, avaliando se os mecanismos de conformidade e fiscalização previstos são suficientes para garantir a proteção dos direitos fundamentais das pessoas potencialmente afetadas por seu uso. Parte-se da hipótese de que a efetividade desses instrumentos ainda é incerta no que se refere à garantia da proteção dos direitos fundamentais, sobretudo em razão da elevada complexidade técnica dos sistemas de inteligência artificial, das assimetrias entre grandes corporações e pequenos desenvolvedores e da rápida evolução tecnológica, que impõe desafios constantes à atualização e à adequação das normas vigentes. Diante da complexidade e da dinamicidade dos riscos envolvidos, conclui-se que a efetividade da proteção dos direitos fundamentais dependerá da adoção de instrumentos complementares e de revisões periódicas que assegurem respostas normativas mais ágeis e substanciais, capazes de evitar a obsolescência do AI Act frente às constantes transformações tecnológicas.

PALAVRAS-CHAVE: Direitos fundamentais; Inteligência Artificial; União Europeia.

1. Victória Fernandes de Moraes, "A proteção dos direitos fundamentais em sistemas de risco elevado no regulamento de inteligência artificial da União Europeia", *Latin American Journal of European Studies* 5, no. 2 (2025): 174 et seq.
2. Este trabalho foi agraciado com o terceiro lugar no "V Prêmio Jean Monnet de Ciências Sociais", uma iniciativa do projeto Jean Monnet Network Policy Debate "BRIDGE Watch", financiado pelo Programa Erasmus+ da Comissão Europeia.
3. Mestranda em Direito Internacional e Sustentabilidade - Universidade Federal de Santa Catarina (UFSC). Membro do Latin American Center of European Studies (LACES). <https://orcid.org/0009-0004-6093-1330>.

THE PROTECTION OF FUNDAMENTAL RIGHTS IN HIGH-RISK AI SYSTEMS UNDER THE EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT

ABSTRACT: On August 1, 2024, Regulation (EU) 2024/1689 of the European Parliament and of the Council entered into force, establishing harmonized rules on artificial intelligence, the so-called Artificial Intelligence Act (AI Act). Although its full application is scheduled for the coming years, the AI Act has already become a global regulatory milestone. Structured around a risk-based approach, the regulation seeks to ensure safety, transparency, and respect for fundamental rights. Through bibliographic and documentary review, this study analyzes the obligations imposed on high-risk AI systems under the AI Act, assessing whether the compliance and oversight mechanisms provided are sufficient to guarantee the protection of the fundamental rights of individuals potentially affected by their use. It is hypothesized that the effectiveness of these instruments remains uncertain regarding the assurance of fundamental rights protection, particularly due to the high technical complexity of artificial intelligence systems, the asymmetries between large corporations and small developers, and the rapid technological evolution, which continuously challenges the updating and adequacy of existing norms. Given the complexity and dynamism of the risks involved, it is concluded that the effectiveness of fundamental rights protection will depend on the adoption of complementary instruments and periodic reviews that ensure more agile and substantive regulatory responses, capable of preventing the AI Act from becoming obsolete in the face of constant technological transformations.

KEYWORDS: Fundamental rights; Artificial Intelligence; European Union.

SUMÁRIO: Introdução; 1. O marco regulatório para inteligência artificial da União Europeia; 1.1 O surgimento do Regulamento de Inteligência Artificial da União Europeia; 1.2 A categorização baseada em risco e a proteção dos direitos fundamentais; 2. Direitos fundamentais ameaçados: sistemas de IA de risco elevado; 2.1 A classificação dos sistemas de IA como de risco elevado; 2.2 As obrigações aplicáveis aos sistemas de IA risco elevado; 3. Mecanismos de proteção e fiscalização nos sistemas de IA risco elevado; 3.1 Mecanismos de conformidade e supervisão; Considerações finais; Referências.

INTRODUÇÃO

A inteligência artificial (IA) tem sido aplicada em diversas áreas da vida cotidiana, incluindo educação, economia, saúde e segurança pública, integrando-se cada vez mais às atividades diárias, desde assistentes virtuais que organizam tarefas pessoais até algoritmos que recomendam conteúdos ou otimizam serviços. Além de facilitar a rotina das pessoas, as soluções baseadas em IA oferecem oportunidades significativas para enfrentar desafios globais, como as mudanças climáticas, a melhoria da saúde e da educação, bem como o desenvolvimento de cidades mais seguras e sustentáveis.

No entanto, a adoção da IA também apresenta desafios substanciais. Quando utilizada para substituir ou complementar decisões humanas, ou ainda em aplicações de vigilância, a IA pode violar direitos fundamentais. Esses sistemas de IA frequentemente apresentam uma complexidade que desafia até mesmo os próprios desenvolvedores, de forma que os problemas encontrados geralmente não são resultantes de falhas intrínsecas à tecnologia, mas sim da forma como ela é projetada e aplicada. A partir disso, torna-se indispensável o debate sobre o impacto da IA nos direitos fundamentais, com destaque para a dignidade, a não discriminação, a proteção de dados e a privacidade. Em meio à rápida evolução tecnológica, a regulamentação da IA tem se consolidado como uma prioridade global, buscando assegurar que o uso dessa tecnologia seja responsável, ético e seguro.

Nesse cenário, a União Europeia (UE) despontou como pioneira na regulação da IA. Inserida na chamada “terceira onda de digitalização”, marcada pela ampla adoção de tecnologias de IA, a UE busca equilibrar a promoção da inovação com a proteção dos direitos fundamentais, conforme a Carta de Direitos Fundamentais da União Europeia.⁴ Reconhecendo a relevância dessa transformação, a Comissão Europeia (Comissão) desenvolveu a “Década Digital”, um plano que busca impulsionar a transformação digital da Europa até 2030. Esse plano estabelece metas e objetivos concretos para a transformação digital do bloco europeu, visando atualizar a legislação para enfrentar os desafios atuais.⁵

Entre as medidas mais significativas está o Regulamento de Inteligência Artificial da União Europeia (Regulamento (UE) 2024/1689), conhecido como AI Act, aprovado pelo Parlamento Europeu em março de 2024.⁶ Este marco legal

4. Parlamento Europeu, Conselho Europeu, and Comissão Europeia. *Carta dos Direitos Fundamentais da União Europeia*. Jornal Oficial da União Europeia, 2012. http://data.europa.eu/eli/treaty/char_2012/oj.

5. União Europeia. *Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 que estabelece o programa Década Digital para 2030*. Jornal Oficial da União Europeia, 2022.

6. União Europeia. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial)*. Jornal Oficial da União Europeia, 13 de junho de 2024.

estabelece um quadro jurídico dedicado à regulamentação da IA, com normas harmonizadas para o desenvolvimento e uso dessa tecnologia.

O AI Act adota uma abordagem baseada em riscos, classificando os sistemas de IA em quatro níveis distintos (inaceitável, elevado, limitado e mínimo) e estabelecendo requisitos e obrigações proporcionais para cada categoria, considerando o potencial impacto sobre a saúde, a segurança e os direitos fundamentais das pessoas afetadas.

Este Regulamento terá aplicação plena apenas em 2026, mas conta com um calendário escalonado para diferentes dispositivos. As práticas proibidas passaram a ser restritas seis meses após a adoção do regulamento, ou seja, em 2 de fevereiro de 2025. Os códigos de conduta tornaram-se aplicáveis nove meses após a entrada em vigor. As regras para sistemas de IA de uso geral passaram a valer em 2 de agosto de 2025. Já as obrigações relativas aos sistemas de risco elevado passam a ser exigidas somente em 2 de agosto de 2027.⁷

Nesse contexto, destacam-se os sistemas de IA de risco elevado, que concentram o maior volume de obrigações regulatórias, abrangendo desde requisitos técnicos e de transparência até mecanismos de supervisão contínua. Diante disso, o presente artigo tem como objetivo geral analisar as obrigações impostas a esses sistemas pelo referido regulamento, buscando avaliar se os mecanismos de conformidade e fiscalização previstos são suficientes para assegurar a proteção dos direitos fundamentais das pessoas potencialmente afetadas por sua utilização.

Dessa forma, parte-se da hipótese de que a efetividade desses instrumentos permanece incerta quanto à garantia da proteção dos direitos fundamentais. Tal incerteza decorre, sobretudo, da complexidade técnica dos sistemas de IA, das assimetrias existentes entre grandes corporações e pequenos desenvolvedores, bem como da rápida evolução tecnológica, que impõe desafios contínuos à atualização e à adequação das normas vigentes.

7. Parlamento Europeu. *Regulamento Inteligência Artificial: Parlamento aprova legislação histórica*. Comunicado de imprensa, 13 mar. 2024. <https://www.europarl.europa.eu/news/pt/press-room/20240308IPR19015/regulamento-inteligencia-artificial-parlamento-aprova-legislacao-historica>.

A pesquisa adota uma abordagem qualitativa, de caráter analítico-descritivo, voltada à análise das normas e debates sobre a regulação da inteligência artificial na União Europeia. Para tanto, são realizadas análises documentais e bibliográficas, contemplando tanto os documentos oficiais da União Europeia quanto artigos acadêmicos nacionais e internacionais relevantes ao tema, visando sustentar uma análise crítica e fundamentada do debate.

1. O MARCO REGULATÓRIO PARA INTELIGÊNCIA ARTIFICIAL DA UNIÃO EUROPEIA

A União Europeia tem priorizado o desenvolvimento digital como um de seus principais eixos estratégicos, especialmente por meio do Programa Europa Digital.⁸ Essa iniciativa reflete o compromisso do Direito da União Europeia em estabelecer princípios e diretrizes voltados à governança tecnológica e à regulamentação de tecnologias digitais emergentes, com destaque, mas não se limitando, à inteligência artificial.⁹

A importância atribuída à IA foi reafirmada ao integrá-la como prioridade na Agenda Digital para a Europa 2020-2030, que busca promover a inovação responsável, a competitividade sustentável e a inclusão digital em todo o bloco.^{10,11} O programa visa não apenas fomentar o desenvolvimento tecnológico,

8. União Europeia. *Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de abril de 2021 que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240*. Jornal Oficial da União Europeia, 29 de abril de 2021.

9. Comissão Europeia. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*. COM(2018) 237 final. Bruxelas: Comissão Europeia, 2018: “O conceito de inteligência artificial (IA) aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas – com um determinado nível de autonomia – para atingir objetivos específicos.

Os sistemas baseados em IA podem ser puramente confinados ao software, atuando no mundo virtual (por exemplo, assistentes de voz, programas de análise de imagens, motores de busca, sistemas de reconhecimento facial e de discurso), ou podem ser integrados em dispositivos físicos (por exemplo, robôs avançados, automóveis autônomos, veículos aéreos não tripulados ou aplicações da Internet das coisas).”

10. Parlamento Europeu. *Uma Agenda Digital para a Europa*. Fichas temáticas sobre a União Europeia.

11. Dora Resende Alves and Ana Carolina Assumpção Stoffel, *O Digital como Prioridade da Comissão Europeia: Breve Análise sobre a Transformação Digital no Âmbito da União Europeia* (Porto, Portugal: Instituto Iberoamericano de Estudos Jurídicos, 2022). <http://hdl.handle.net/11328/4082>.

mas também garantir que esse progresso ocorra em conformidade com valores fundamentais da União Europeia, como a proteção dos direitos humanos, a transparência, a ética e a privacidade. Nesse contexto, a UE reconhece que o avanço da IA oferece oportunidades significativas para o crescimento econômico e a melhoria dos serviços públicos, ao mesmo tempo em que impõe desafios relevantes relacionados à segurança, à equidade e à governança.¹²

1.1 O surgimento do Regulamento de Inteligência Artificial da União Europeia

A preocupação da União Europeia com os impactos éticos, sociais e jurídicos da IA tem se intensificado desde 2017, quando o Conselho da União Europeia (Conselho) destacou a urgência de lidar com as novas tecnologias emergentes. Diante desse cenário, o objetivo passou a ser assegurar um elevado nível de proteção de dados, direitos digitais e padrões éticos.

Nesse sentido, o Conselho convidou a Comissão Europeia a apresentar, até o início de 2018, uma abordagem europeia para a IA, com iniciativas voltadas ao fortalecimento do arcabouço normativo e à exploração de novos mercados digitais.¹³ A declaração conjunta sobre as prioridades legislativas da UE para 2018-2019 reforçou esse direcionamento ao reconhecer a necessidade de garantir os direitos fundamentais e princípios éticos diante dos avanços em IA e robótica.¹⁴

Assim, em março de 2018, a Comissão estabeleceu o Grupo de Peritos de Alto Nível em Inteligência Artificial (AI HLEG), formado por 52 especialistas oriundos

12. 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, 21 de maio de 2024, <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/>.

13. Conselho da União Europeia, *European Council Meeting (19 October 2017) – Conclusion EUCO 14/17*, 2017, <https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf>.

14. Comissão Europeia, *Joint Declaration on the EU's Legislative Priorities for 2018-19*, 14 de dezembro de 2017, https://commission.europa.eu/publications/joint-declaration-eus-legislative-priorities-2018-19_en?prefLang=pt.

da academia, setor privado e sociedade civil.^{15,16} Esse grupo ficou responsável pela elaboração de três documentos centrais: (i) as Diretrizes Éticas para uma IA Confiável, baseadas nos direitos fundamentais da UE; (ii) um conjunto de Recomendações de Políticas e Investimentos; e (iii) a Lista de Avaliação para uma IA Confiável (ALTAI).¹⁷ Nesse panorama, a Comissão propôs uma estratégia estruturada em três pilares: aumento do investimento público e privado, preparação para mudanças socioeconômicas e estabelecimento de um marco ético e jurídico adequado.

Ainda em 2018, 24 Estados-Membros comprometeram-se a cooperar no desenvolvimento e aplicação da IA, reforçando a necessidade de uma regulação que promovesse a inovação sem comprometer os valores da UE.^{18,19} Como parte dessa estratégia, foi criada a Aliança Europeia para a IA, uma iniciativa de diálogo político e técnico entre mais de 6.000 partes interessadas.²⁰ Neste sentido, foi lançado o Plano Coordenado para a Inteligência Artificial, que previa investimentos em infraestrutura, ambientes de teste, pesquisa e capacitação para assegurar o desenvolvimento responsável da IA.²¹

O uso crescente da IA passou a gerar preocupações quanto à proteção dos direitos fundamentais e à segurança. O relatório "Getting the Future Right – Arti-

15. Comissão Europeia. "Inteligência artificial: Comissão lança trabalho sobre relação entre tecnologia de ponta e normas éticas." Comunicado de imprensa. 8 de março de 2018. https://ec.europa.eu/commission/presscorner/detail/pt/ip_18_1381.
16. Comissão Europeia, "Commission appoints expert group on AI and launches the European AI Alliance," *Shaping Europe's digital future*, 14 de junho de 2018, <https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance>.
17. Comissão Europeia, "Inteligência artificial: Comissão lança trabalho sobre relação entre tecnologia de ponta e normas éticas," Comunicado de imprensa, 8 de março de 2018, https://ec.europa.eu/commission/presscorner/detail/pt/ip_18_1381.
18. Artigo 2.º do Tratado sobre a União Europeia: «A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos do Homem, incluindo os direitos das pessoas pertencentes a minorias.» Os Estados-Membros partilham uma «sociedade caracterizada pelo pluralismo, a não discriminação, a tolerância, a justiça, a solidariedade e a igualdade entre homens e mulheres»
19. Comissão Europeia, *Comunicação da comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões* (Documento COM(2019) 640 final), 11 de dezembro de 2019.
20. Comissão Europeia, *The European AI Alliance*, *Shaping Europe's digital future*, 14 de outubro de 2024, <https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>.
21. Comissão Europeia, *Coordinated Plan on Artificial Intelligence*, COM(2018) 795 final, 7 de dezembro de 2018.

ficial Intelligence and Fundamental Rights”, publicado pela Agência dos Direitos Fundamentais da União Europeia (FRA) em 2020, destacou a importância de avaliações de impacto prévias à implementação de sistemas de IA, uma vez que os riscos podem variar conforme o contexto, o nível de automação, a escala de aplicação e a área de uso.²²

Dessa forma, consolidou-se a proposta de um modelo regulatório baseado na gestão de riscos, como forma de garantir que os sistemas de IA fossem legais, éticos e tecnicamente robustos. Esse enfoque foi reafirmado no Livro Branco sobre a IA: Uma abordagem europeia virada para a excelência e a confiança, publicado em fevereiro de 2020, que defendeu a necessidade de uma resposta coordenada para evitar a fragmentação do mercado interno.

Após o período de consultas públicas e a revisão do Plano Coordenado, a Comissão Europeia apresentou, em abril de 2021, a proposta do Regulamento de Inteligência Artificial (AI Act), oficialmente adotada pelo Parlamento Europeu em março de 2024 e com entrada em vigor em 1º de agosto do mesmo ano.²³

1.2 A categorização baseada em risco e a proteção dos direitos fundamentais

A Avaliação de Impacto, com base em diversos estudos, identificou questões centrais relacionadas ao desenvolvimento e ao uso de sistemas de IA, as quais deveriam ser consideradas pelo AI Act. Uma das principais preocupações dizia respeito à IA como fator de ampliação do risco de violações aos direitos fundamentais dos cidadãos e aos valores da União Europeia. Ainda que seja difícil mensurar com exatidão a magnitude desses riscos, um número crescente de evidências sugere que os cidadãos da UE estão cada vez mais expostos a impactos adversos.

22. Alves, Dora Resende, e Ana Carolina Assumpção Stoffel. *O digital como prioridade da Comissão Europeia: breve análise sobre a transformação digital no âmbito da União Europeia*. Porto, Portugal: Instituto Iberoamericano de Estudos Jurídicos, 2022. <http://hdl.handle.net/11328/4082>.

23. Comissão Europeia. *The European AI Alliance*. Shaping Europe’s digital future, 14 de outubro de 2024. <https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>.

Além disso, inúmeros Estados-Membros já apresentaram jurisprudência e desafios legais envolvendo o uso de IA de forma incompatível com os direitos fundamentais. Um exemplo ocorreu no Tribunal Nacional de Não Discriminação e Igualdade da Finlândia, no qual uma instituição de crédito foi investigada por discriminação ao negar financiamento a uma pessoa com base em compras online, levando em conta fatores considerados discriminatórios, como gênero, idade e idioma.²⁴

Nesse contexto, a Avaliação de Impacto identificou, entre os principais direitos fundamentais ameaçados pelo uso da IA, os seguintes: dignidade humana e autonomia pessoal (1); privacidade e proteção de dados (2); igualdade e não discriminação (3); e acesso à justiça, julgamento justo e boa administração pública (4).²⁵

O direito à dignidade humana e à autonomia pessoal (1) pressupõe que cada indivíduo seja tratado com respeito, enquanto ser humano, e tenha sua autodeterminação preservada. O uso de IA pode comprometer esse princípio ao induzir as pessoas a crer que estão interagindo com outro ser humano, quando, na realidade, comunicam-se com uma máquina. Além disso, algoritmos com crescente capacidade de manipulação, capazes de captar e prever informações pessoais sensíveis, tornam os indivíduos mais suscetíveis à manipulação e à tomada de decisões que não refletem sua real vontade ou interesse.²⁶

No que se refere à privacidade e à proteção de dados (2), o uso indiscriminado de ferramentas algorítmicas permite práticas de vigilância em larga escala, monitoramento comportamental e avaliação automatizada de indivíduos, resultando em grave violação da privacidade e de outros direitos fundamentais. Essa prática não afeta apenas os indivíduos isoladamente, mas compromete pilares essenciais da UE, como democracia, liberdade e Estado de Direito. Um

24. Tribunal Nacional de Não Discriminação e Igualdade da Finlândia. Decisão 216/2017, 21 de março de 2017. "Discriminação múltipla na avaliação da capacidade de crédito." <https://www.vytiltk.fi/en/index/opinionsanddecisions/decisions.html>.

25. Comissão Europeia, *Impact Assessment of the Regulation on Artificial Intelligence: SWD(2021) 84 final*, Shaping Europe's digital future, 21 de abril de 2021, <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence>.

26. Comissão Europeia, *Impact Assessment of the Regulation on Artificial Intelligence*.

exemplo emblemático é o uso crescente de sistemas de identificação biométrica remota, como reconhecimento facial e de voz, em espaços públicos, cujos riscos para os direitos individuais têm gerado preocupações substanciais, ainda que alguns defendam sua aplicação em contextos limitados e proporcionalmente justificáveis.²⁷

Em relação à discriminação algorítmica (3), a Avaliação de Impacto destacou que ela pode ocorrer por múltiplas razões ao longo de diferentes etapas do processo algorítmico, sendo frequentemente difícil de detectar e corrigir. A reprodução de preconceitos inconscientes por parte de desenvolvedores, por exemplo, pode levar a classificações enviesadas que perpetuam desigualdades estruturais, sob a aparência de neutralidade científica. Essa prática é particularmente grave em setores sensíveis como o mercado de trabalho, a administração pública e o sistema de justiça, podendo comprometer direitos como educação, segurança social e acesso a serviços essenciais.²⁸

Ainda, instituições financeiras e outras organizações podem empregar IA para avaliar a solvência de indivíduos, influenciando decisões de crédito ou acesso à moradia. A opacidade desses sistemas ("caixa-preta da IA")²⁹, muitas vezes inexplicáveis mesmo para seus desenvolvedores, impede o controle social e jurídico sobre os critérios utilizados para tais decisões.^{30, 31}

Nesse sentido, o estudo "Gender Shades", realizado pelo MIT Media Lab, um laboratório do "Massachusetts Institute of Technology" (MIT), nos Estados Unidos, analisou ferramentas de reconhecimento facial e evidenciou viés discriminatório em sistemas de IA. A pesquisa mostrou que todos os sistemas avaliados apresentam melhor desempenho em homens do que em mulheres e, de forma

27. Comissão Europeia, *Impact Assessment of the Regulation on Artificial Intelligence*.

28. Comissão Europeia, *Impact Assessment of the Regulation on Artificial Intelligence*.

29. O termo "caixa-preta" ("black box") refere-se a um sistema ou modelo de IA cujos funcionamentos internos não são facilmente compreensíveis ou transparentes para os seres humanos. Isso significa que o processo de tomada de decisão do sistema é opaco e difícil de interpretar.

30. Gow, Glenn. 2021. "The EU Is Regulating Your AI. Five Ways To Prepare Now." *Forbes*, October 10, 2021. <https://www.forbes.com/sites/glenngow/2021/10/10/the-eu-is-regulating-your-ai-five-ways-to-prepare-now/>.

31. AllBusiness.com Team, "The Definition of a Black Box," *TIME*, abril 3, 2025. <https://time.com/collections/the-ai-dictionary-from-allbusiness-com/7273935/definition-of-black-box/>.

geral, funcionam melhor com indivíduos de pele clara do que com indivíduos de pele escura. Ao examinar subgrupos interseccionais, homens claros, mulheres claras, homens escuros e mulheres escuras, os piores resultados foram observados para mulheres negras, demonstrando como a interseccionalidade amplifica desigualdades em sistemas automatizados.³²

O direito a uma solução efetiva, a um julgamento justo e a uma boa administração pública (4) é igualmente afetado. A falta de acesso a informações relevantes sobre os sistemas de IA dificulta o direito de contestação e defesa. O uso de decisões automatizadas em processos judiciais pode comprometer o acesso à justiça e a imparcialidade do julgamento. A opacidade, a ausência de supervisão humana e a falta de salvaguardas reforçam os riscos.

Nesse sentido, buscando assegurar a proteção dos direitos fundamentais, a construção do AI Act seguiu os princípios e metodologias da Agenda "Better Regulation", que orienta a formulação de políticas com base em dados concretos, participação de múltiplos atores e redução de encargos desnecessários.³³

³⁴ O modelo de regulação baseada em risco já é familiar no direito digital da UE, tendo sido aplicado previamente em áreas como cibersegurança, plataformas online e proteção de dados. Assim, a adoção desse modelo pelo AI Act reflete a tentativa de alinhar a governança tecnológica aos desafios complexos da era digital.^{35,36}

Todavia, um dos desafios cruciais para qualquer abordagem baseada em risco é alcançar um consenso sobre quais riscos devem ser priorizados e qual sua gravidade, considerando probabilidade, impacto ou ambos. Durante as

32. Gender Shades. 2018. *Gender Shades*. MIT Media Lab. <http://gendershades.org/overview.html>.

33. Almeida, Maria Candida. 2023. "Regulação da inteligência artificial baseada em riscos e a sua responsividade." *Journal of Law and Regulation* 9, no. 2: 44–72. <https://periodicos.unb.br/index.php/rdsr/article/view/43251>.

34. Comissão Europeia. 2024. *Legislar melhor: porquê e como*. Comissão Europeia, 28 de outubro de 2024. https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation_pt.

35. Conselho Europeu e Conselho da União Europeia. 2020. "Mercado único digital na Europa." 21 de setembro de 2020.

36. Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU's AI Act." June 19, 2024. <http://dx.doi.org/10.2139/ssrn.4870387>.

negociações do AI Act, houve um debate ativo sobre os critérios para determinar quando a IA representa riscos inaceitáveis para a sociedade e para os indivíduos e sobre quais sistemas de IA possuem risco elevado e podem ser permitidos no mercado, desde que certas salvaguardas sejam implementadas. Esse debate ilustra a complexidade desse processo, especialmente quando a avaliação não se baseia de forma consistente em evidências empíricas e em uma metodologia clara.³⁷

Dessa forma, em consonância com a “Década Digital da Europa 2030” e aspirando uma abordagem centrada no ser humano, o AI Act organiza os sistemas de IA segundo uma abordagem baseada em risco, composta por quatro níveis: risco inaceitável, risco elevado, risco limitado e risco mínimo.^{38, 39}

É importante mencionar que o AI Act não nomeia todos os quatro níveis de risco explicitamente. São estabelecidas disposições específicas para sistemas de IA de risco inaceitável, ou seja, práticas proibidas de IA (Capítulo II); para sistemas de IA de risco elevado (Capítulo III), que acionam um conjunto de obrigações detalhadas, complexas e rigorosas, ocupando grande parte do AI Act; e para sistemas de IA de risco limitado (Capítulo IV), que incluem obrigações de transparência associadas. Os sistemas de risco mínimo não são regulamentados. Todavia, o AI Act menciona que “O desenvolvimento de outros sistemas de IA, que não sejam sistemas de IA de risco elevado de acordo com os requisitos do presente regulamento pode conduzir a uma maior utilização de IA ética e de confiança na União [...]”⁴⁰, sendo as partes interessadas incentivadas a construir códigos de conduta voluntários.⁴¹ Dessa forma, entende-se como sistema de IA de risco mínimo todo aquele que o AI Act não aborda explicitamente.

37. Ebers, Martin. “Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU’s AI Act.”

38. De acordo com o art. 3º do AI Act, “Risco é a combinação da probabilidade de ocorrência de danos com a gravidade desses danos.”

39. EU AI Act. 2024. “Key Issues.” EU AI Act, 28 de outubro de 2024. <https://www.euaiact.com/key-issue/3>.

40. REGULAMENTO (UE) 2024/1689, Considerando 165.

41. EU Artificial Intelligence Act. *High-level summary of the AI Act*. EU Artificial Intelligence Act. <https://artificialintelligenceact.eu/high-level-summary/>.

Enquanto os sistemas de risco mínimo ficam fora do escopo do AI Act, os sistemas que apresentam maior grau de risco são submetidos a obrigações graduais, considerando seu impacto sobre a saúde, a segurança e os direitos fundamentais. No entanto, essa abordagem baseada em risco tem sido criticada por estudiosos que defendem uma perspectiva estritamente centrada em direitos, argumentando que os direitos humanos são inegociáveis e não podem ser relativizados com base em avaliações de risco. Segundo esses especialistas, medidas como a autoavaliação de riscos pelas empresas podem comprometer a proteção efetiva dos direitos, colocando-os em desequilíbrio frente aos interesses econômicos.^{42, 43}

Nesse sentido, a abordagem baseada em riscos seria útil em ambientes técnicos, nos quais as empresas precisam avaliar seus próprios riscos operacionais. Contudo, ao exigir que essas avaliações considerem também os direitos fundamentais das pessoas, a abordagem da União Europeia põe em questão a natureza inegociável dos direitos humanos, uma vez que eles não podem ser colocados em equilíbrio com os interesses das empresas.⁴⁴

A aplicação de sistemas automatizados em áreas como segurança pública, educação e análise de crédito evidencia riscos reais e crescentes. Tecnologias aparentemente inofensivas, como ferramentas de reconhecimento automático de gênero, têm gerado resultados discriminatórios contra pessoas trans que não se conformam com os padrões de gênero, seja atribuindo erroneamente um gênero ou impondo uma identidade de gênero que não corresponde à identidade verdadeira da pessoa.^{45, 46} Esses exemplos reforçam a necessidade

42. EU AI ACT. *Key Issues*. EU AI Act, 28 out. 2024. <https://www.euaiact.com/key-issue/3>.

43. Ezeani, Gabriella, Ansgar Koene, Richa Kumar, Nicole Santiago, David Wright, e Ernst & Young LLP. *A Survey of Artificial Intelligence Risk Assessment Methodologies: The Global State of Play and Leading Practices Identified*. Trilateral Research Ethical AI, dezembro 2021. <https://www.trilateralresearch.com/wp-content/uploads/2022/01/A-survey-of-AI-Risk-Assessment-Methodologies-full-report.pdf>.

44. Fanny Hidvegi, Daniel Leufer e Estelle Massé, *The EU Should Regulate AI on the Basis of Rights, Not Risks*, last Update January 2022, <https://www.accessnow.org/eu-regulation-ai-risk-based-approach/>.

45. Fanny Hidvegi, Daniel Leufer e Estelle Massé, *The EU Should Regulate AI on the Basis of Rights, Not Risks*.

46. Keyes, Os. „The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition.” *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW, Article 88 (No-

de avaliações robustas de impacto sobre os direitos humanos, conduzidas por autoridades independentes e especializadas, tanto antes quanto após a implementação dos sistemas.

2. DIREITOS FUNDAMENTAIS AMEAÇADOS: SISTEMAS DE IA DE RISCO ELEVADO

O AI Act estabelece que os sistemas de risco elevado só podem ser comercializados, implementados ou utilizados na União Europeia se cumprirem uma série de requisitos obrigatórios, enquanto os sistemas de risco inaceitável são proibidos.

Para definir o que se enquadra como um sistema de IA de risco elevado, o Livro Branco sobre a Inteligência Artificial propôs dois critérios cumulativos. O primeiro critério considerou o setor de aplicação: sistemas de IA utilizados em áreas em que, pelas características das atividades típicas, se pode esperar a ocorrência de riscos significativos, como nos setores de transporte, energia ou em determinadas funções do setor público. A Comissão Europeia sugeriu que esses setores fossem listados de forma específica e exaustiva no novo marco regulatório, com possibilidade de revisão periódica.

O segundo critério estabeleceu que uma aplicação de IA deve ser considerada de risco elevado quando seu modo concreto de utilização tornar provável o surgimento de riscos relevantes, mesmo que esteja inserida em um setor crítico. Isso ocorre porque nem todas as aplicações de IA em setores sensíveis implicam, por si só, riscos elevados. Dessa forma, a avaliação deve levar em conta o impacto da utilização sobre os direitos e interesses das partes afetadas. A combinação desses dois critérios visa garantir uma delimitação clara do âmbito de aplicação do regulamento, promovendo segurança jurídica e proporcionalidade regulatória.

2.1 A classificação dos sistemas de IA como de risco elevado

A classificação de um sistema de IA como de risco elevado depende da análise de seus impactos potenciais sobre a saúde, a segurança e os direitos fundamentais consagrados na Carta de Direitos Fundamentais da União Europeia, incluindo, entre outros, a dignidade humana, a proteção de dados, a não discriminação, a liberdade de expressão e o direito a um julgamento justo. Para orientar essa avaliação, a Seção 1 do Capítulo III do AI Act estabelece os critérios específicos para a classificação de sistemas de risco elevado. Conforme o Artigo 6.º, essas regras definem:

Classificação de sistemas de IA como sendo de risco elevado

1. Independentemente de a colocação no mercado ou a colocação em serviço de um sistema de IA ser feita separadamente dos produtos a que se referem as alíneas a) e b), esse sistema de IA é considerado de risco elevado sempre que se estejam preenchidas ambas as seguintes condições:

- a) O sistema de IA destina-se a ser utilizado como um componente de segurança de um produto ou o sistema de IA é, ele próprio, um produto abrangido pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I;
- b) O produto cujo componente de segurança nos termos da alínea a) é o sistema de IA, ou o próprio sistema de IA enquanto produto, tem de ser sujeito a uma avaliação da conformidade por terceiros com vista à sua colocação no mercado ou colocação em serviço nos termos dos atos enumerados na lista da legislação de harmonização da União constante do anexo I.

2. Além dos sistemas de IA de risco elevado a que se refere o n.º 1, os sistemas de IA a que se refere o anexo III são também considerados de risco elevado.

Além dos critérios estabelecidos no número 1 do referido artigo, o Anexo III do AI Act especifica categorias adicionais de sistemas que devem ser tratados como de risco elevado. Esses sistemas incluem aqueles concebidos para finalidades como: dados biométricos (1); infraestruturas críticas (2); educação e formação profissional (3); emprego, gestão de trabalhadores e acesso ao emprego por conta própria (4); acesso a serviços privados essenciais e a serviços e prestações públicos essenciais (5); aplicação da lei (6); gestão da migração, do asilo e do controlo das fronteiras (7); e administração da justiça e processos democráticos

(8). Destaca-se, no entanto, que esses sistemas só podem ser considerados de risco elevado se representarem um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais dos indivíduos, nomeadamente se influenciarem de forma significativa o resultado da tomada de decisões.

Nesse contexto, há uma exceção para os sistemas de IA previstos no Anexo III, nos casos em que o sistema se destina a realizar uma tarefa processual restrita; melhorar o resultado de uma atividade humana previamente concluída; detectar padrões de tomada de decisão ou desvios em relação a padrões anteriores, e não se destina a substituir nem influenciar uma avaliação humana previamente realizada sem a devida verificação por um ser humano; ou realizar uma tarefa preparatória para uma avaliação relevante dentro dos casos de uso listados no Anexo III. Contudo, os sistemas de IA mencionados no Anexo III devem sempre ser considerados de risco elevado quando utilizados para a definição de perfis de pessoas singulares, isto é, o processamento automatizado de dados pessoais para avaliar diversos aspectos da vida de uma pessoa, como desempenho profissional, situação econômica, saúde, preferências, interesses, confiabilidade, comportamento, localização ou deslocamento.⁴⁷

Dentre os sistemas de IA que utilizam dados biométricos (1) estão os de identificação biométrica à distância, o que não inclui aqueles concebidos para verificação biométrica com o único objetivo de confirmar a identidade declarada de uma pessoa singular.⁴⁸ Também são incluídos os sistemas de IA destinados à categorização biométrica com base em atributos ou características sensíveis ou protegidos com base na inferência desses atributos ou características, bem como os sistemas projetados para o reconhecimento de emoções.

As exceções restritas ao uso de sistemas de IA que empregam dados biométricos estão condicionadas à autorização prévia por um órgão judicial ou por outra entidade independente, bem como à observância de limites adequados em termos de tempo, alcance geográfico e bases de dados consultadas. No

47. EU Artificial Intelligence Act, *High-level Summary of the AI Act*, EU Artificial Intelligence Act. <https://artificialintelligenceact.eu/high-level-summary/>.

48. Comissão Europeia. *Regulamento Inteligência Artificial*. Shaping Europe's digital future, 2024. <https://digital-strategy.ec.europa.eu/pt/policies/regulatory-framework-ai>.

entanto, segundo a “European Digital Rights”, coletivo de ONGs, o AI Act ainda apresenta diversas brechas em relação à biometria, ao policiamento e à segurança nacional, de modo que os legisladores devem se dedicar a fechar essas lacunas.⁴⁹

Algumas dessas lacunas e ambiguidades estão relacionadas ao fato de que certos sistemas de identificação biométrica à distância são considerados de risco inaceitável e, portanto, proibidos pelo AI Act, o que torna frequentemente difícil determinar a qual categoria de risco tais sistemas pertencem.⁵⁰ Mais de 200 organizações da sociedade civil, na Europa e em âmbito global, já alertaram para a ameaça inaceitável que o uso da identificação biométrica à distância em espaços públicos representa para os direitos fundamentais, o que reforça a necessidade de clarificação normativa e mecanismos de fiscalização mais robustos, a fim de assegurar a proteção efetiva desses direitos.⁵¹

No que diz respeito às infraestruturas críticas (2), consideram-se de risco elevado os sistemas de IA desenvolvidos para atuar como componentes de segurança na gestão e controle de infraestruturas digitais essenciais, como redes de tráfego rodoviário e sistemas de fornecimento de água, gás, aquecimento ou eletricidade.

Na área da educação e formação profissional (3), também se enquadram como de risco elevado os sistemas de IA concebidos para determinar o acesso, admissão ou afetação de indivíduos a instituições de ensino em todos os níveis. Incluem-se ainda os sistemas destinados à avaliação de resultados de aprendizagem, sobretudo quando tais resultados orientam o processo educativo, bem como os utilizados para definir o nível de educação apropriado a cada pessoa.

49. Anna Desmarais, “What Should We Expect as the EU’s AI Act Comes into Force?,” *Euronews*, 1 ago. 2024. <https://www.euronews.com/next/2024/08/01/what-to-expect-as-the-eus-ai-act-comes-into-force>.

50. Lawne, Richard. 2025. “Biometrics in the EU: Navigating the GDPR, AI Act.” IAPP, April 23, 2025. <https://iapp.org/news/a/biometrics-in-the-eu-navigating-the-gdpr-ai-act>.

51. European Digital Rights (EDRi), ARTICLE19, Bits of Freedom, Chaos Computer Club (CCC), Digitale Gesellschaft CH, e IT-Political Association of Denmark (IT-Pol). *Prohibit All Remote Biometric Identification (RBI) in Publicly Accessible Spaces*. Novembro de 2021. <https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf>.

Sistemas voltados ao controle e detecção de práticas proibidas em exames educacionais também integram essa categoria.

No contexto do emprego, da gestão de trabalhadores e do acesso ao trabalho autônomo (4), são considerados de risco elevado os sistemas de IA utilizados em atividades de recrutamento, como a divulgação de vagas, triagem de candidaturas e avaliação de perfis. A classificação abrange ainda os sistemas que influenciam decisões relacionadas às condições de trabalho, promoções, demissões, atribuição de tarefas com base em características individuais, e os utilizados para monitoramento e avaliação de desempenho e conduta.

Atualmente, é crescente o uso de sistemas automatizados para contratar, avaliar e dispensar trabalhadores com pouca ou nenhuma supervisão humana. Surgem, nesse contexto, os chamados “chefes algorítmicos”, que automatizam processos decisórios como contratações, definição de salários e até demissões, sob a alegação de ganhos em eficiência.^{52,53} No entanto, esses sistemas são considerados de risco elevado por poderem afetar significativamente as perspectivas profissionais, a subsistência e os direitos fundamentais dos trabalhadores. Em processos de recrutamento, promoção ou retenção, esses sistemas podem reproduzir discriminações históricas contra mulheres, pessoas com deficiência, certos grupos etários ou com determinada origem racial, étnica ou orientação sexual. Além disso, o monitoramento algorítmico do desempenho e da conduta pode comprometer os direitos à privacidade e à proteção de dados.

Nesse contexto, pesquisas de 2024 da Universidade Cornell, nos Estados Unidos, indicam que ferramentas de inteligência artificial utilizadas para monitorar o comportamento e a produtividade dos funcionários podem, na prática, reduzir a produtividade e aumentar as taxas de desligamento. Esses sistemas de vigilância, cada vez mais empregados para analisar expressões faciais, tom

52. Francesca Bria, “Algorithms Are Hiring and Firing Us Now – But Tougher EU Laws Could Protect Workers,” *The Guardian*, 12 out. 2023. <https://www.theguardian.com/commentisfree/2023/oct/12/algorithms-eu-law-workers-ai-data>.

53. Fennell, Andrew. 2025. “Inteligência Artificial Não Apenas Automatiza Tarefas, Mas Pode Ser Sua Nova Chefe.” *Forbes Brasil*, julho 2025. <https://forbes.com.br/carreira/2025/07/inteligencia-artificial-nao-apenas-automatiza-tarefas-mas-pode-ser-sua-nova-chefe/>.

de voz e comunicação verbal e escrita, tendem a gerar uma maior sensação de perda de autonomia em comparação à supervisão realizada por humanos.⁵⁴

Dando continuidade à análise dos sistemas que podem ser considerados de risco elevado no AI Act, incluem-se aqueles destinados ao acesso a serviços privados essenciais e a serviços e prestações públicas (5), também se enquadram como de risco elevado os sistemas de IA utilizados por autoridades públicas (ou em seu nome) para avaliar a elegibilidade de indivíduos a benefícios sociais, serviços de saúde, ou para concessão e revisão desses serviços. Essa classificação inclui ainda os sistemas usados para avaliação de solvência e classificação de crédito, com exceção dos voltados à detecção de fraudes, os empregados na precificação de seguros de vida e saúde, os utilizados para classificar chamadas de emergência e os que realizam triagem de pacientes em serviços de saúde emergenciais.

No setor financeiro, especialmente na avaliação de crédito, discute-se a necessidade de orientações mais específicas para evitar discriminações e mitigar riscos. Apesar do potencial da IA para identificar transações suspeitas ou abusos de mercado, bases de dados mal construídas podem gerar decisões discriminatórias. Em 2011, por exemplo, o TJUE considerou ilegal diferenciar preços de seguros com base no gênero. No entanto, algoritmos de precificação podem reproduzir esse tipo de discriminação de forma opaca, dificultando a responsabilização.^{55,56}

Na área da aplicação da lei (6), e desde que amparados pelo direito da UE ou por legislação nacional, são considerados de risco elevado os sistemas de IA utilizados por autoridades policiais, ou em seu nome, para avaliar o risco de vitimização de indivíduos, verificar a confiabilidade de provas, prever reincidência

54. Dean, James. 2024. "More Complaints, Worse Performance When AI Monitors Work." *Cornell Chronicle*, July 2, 2024, <https://news.cornell.edu/stories/2024/07/more-complaints-worse-performance-when-ai-monitors-work>.

55. Tribunal Europeu Veta Seguro de Carro Mais Barato para Mulheres," *BBC News Brasil*, 1 mar. 2011, https://www.bbc.com/portuguese/noticias/2011/03/110301_europa_seguro_rp.

56. Jack Schickler e Cynthia Kroet, "Commission Probes AI Finance Risk as It Finalises Sweeping New Law," *Euronews*, 18 jun. 2024, <https://www.euronews.com/business/2024/06/18/commission-probes-ai-finance-risk-as-it-finalises-sweeping-new-law>.

criminal ou traçar perfis de comportamento. Isso inclui instrumentos como polígrafos ou outros mecanismos para análise de personalidade e histórico criminal.

No contexto da gestão da migração, do asilo e do controle de fronteiras (7), também sob respaldo legal da União ou dos Estados-Membros, incluem-se como de risco elevado os sistemas de IA voltados à análise de pedidos de asilo, vistos ou autorizações de residência, à avaliação da confiabilidade de documentos e à verificação de riscos relacionados à segurança, saúde ou migração irregular. Esses sistemas impactam diretamente populações vulneráveis e devem, por isso, ser precisos, transparentes e não discriminatórios, garantindo direitos fundamentais como a não discriminação, a livre circulação, a privacidade e a boa administração. Um exemplo notório de violação ocorreu no Reino Unido, em 2020, quando um sistema de triagem automatizada de pedidos de visto foi acusado de racismo algorítmico por priorizar requerentes de países predominantemente brancos. Diante da controvérsia, o Ministério do Interior anunciou o redesenho do sistema.^{57,58}

Quanto à administração da justiça e aos processos democráticos (8), classificam-se como de risco elevado os sistemas de IA empregados por autoridades judiciais para auxiliar na investigação, interpretação dos fatos e aplicação da lei, bem como aqueles utilizados na resolução alternativa de litígios. Também se enquadram nessa categoria os sistemas destinados a influenciar o resultado de eleições ou referendos, ou o comportamento de eleitores. Contudo, não se incluem os sistemas usados apenas para fins administrativos ou logísticos de campanhas eleitorais.

Caso um prestador avalie que um sistema listado no Anexo III não deva ser considerado de risco elevado, deve documentar essa avaliação antes de colocá-lo no mercado. Além disso, é necessário realizar o registro do sistema e do

57. *Automating Society Report 2020*, Algorithm Watch, 2020. <https://automatingsociety.algorithmwatch.org/>.

58. *Home Office Says It Will Abandon Its Racist Visa Algorithm – After We Sued Them*, Foxglove, 4 ago. 2020, <https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/>.

próprio prestador na base de dados da UE. Sempre que solicitado, a documentação deverá ser disponibilizada às autoridades competentes.

Considerando que as normas referentes aos sistemas de risco elevado só entrarão em vigor em agosto de 2027, a Comissão Europeia deverá fornecer orientações práticas sobre a classificação desses sistemas. Essas diretrizes incluirão exemplos concretos para facilitar a interpretação e a implementação do regulamento. Nesse contexto, em junho de 2025, a Comissão lançou uma consulta pública sobre sistemas de IA de risco elevado, com o objetivo de coletar casos práticos e esclarecer questões relacionadas à aplicação desses sistemas, contribuindo para uma implementação mais segura e uniforme do AI Act em toda a União Europeia.⁵⁹

Ainda que a vigência integral pareça distante, empresas de tecnologia já se movimentam para alinhar suas práticas ao AI Act. Nesse sentido, a chefe de IA responsável da empresa de consultoria UST sugeriu a criação de conselhos internos de governança de IA, com especialistas jurídicos, técnicos e de segurança, para assegurar a conformidade regulatória. No entanto, Risto Uuk, do "Future of Life Institute", aponta que ainda restam dúvidas quanto ao grau de risco associado a determinadas tecnologias, exigindo esclarecimentos adicionais por parte da Comissão.⁶⁰

A Comissão possui a prerrogativa de adotar atos delegados para incluir novas condições ou modificar as já existentes referentes aos sistemas de IA de risco elevado, desde que haja provas concretas e confiáveis de que certos sistemas, embora abrangidos pelo Anexo III, não apresentam riscos significativos à saúde, segurança ou direitos fundamentais das pessoas. Da mesma forma, essas alterações podem ser realizadas quando necessário para assegurar o nível de proteção desses valores, conforme previsto no AI Act. Importante destacar que

59. Comissão Europeia. 2025. "Comissão Lança Consulta Pública sobre Sistemas de IA de Risco Elevado." *Digital Strategy*, 6 de junho de 2025. <https://digital-strategy.ec.europa.eu/pt/news/commission-launches-public-consultation-high-risk-ai-systems>.

60. Anna Desmarais, "What Should We Expect as the EU's AI Act Comes into Force?," *Euronews*, 1 ago. 2024, <https://www.euronews.com/next/2024/08/01/what-to-expect-as-the-eus-ai-act-comes-into-force>.

qualquer modificação deve respeitar o nível geral de proteção estabelecido e considerar a evolução tecnológica e do mercado.

Apesar dos esforços da UE para mitigar os riscos associados aos sistemas de IA de risco elevado, há quem sustente que a classificação atual ainda é insuficiente frente a certas aplicações, como a identificação biométrica remota e outras formas de previsão comportamental. Nesses casos, mesmo sob a categoria de risco elevado, as salvaguardas previstas podem ser insuficientes diante do potencial de vigilância em massa, discriminação algorítmica e erosão de direitos fundamentais, como o direito à privacidade, à não discriminação e à liberdade de expressão.

Nesse sentido, argumenta-se que tratar o problema em termos de risco pode levar à falsa ideia de que salvaguardas ou diretrizes éticas poderiam “reduzir o risco”, quando, na realidade, alguns sistemas violam nossos direitos e nossa dignidade de forma intrínseca, sem possibilidade de mitigação.⁶¹

2.2 As obrigações aplicáveis aos sistemas de IA de risco elevado

Como já mencionado, os sistemas de inteligência artificial classificados como de risco elevado estão sujeitos a um conjunto rigoroso de obrigações regulatórias, conforme previsto na Seção 2 do Capítulo III do AI Act. A adoção dessas normas busca não apenas garantir a conformidade legal, mas também promover uma utilização responsável e ética da IA assegurando que seu impacto seja monitorado e controlado de forma proporcional ao grau de risco associado.

Uma das principais exigências é a implementação de um sistema de gestão de riscos (artigo 9º), compreendido como um processo contínuo e iterativo, executado ao longo de todo o ciclo de vida do sistema. Esse processo deve ser periodicamente revisado e atualizado, englobando: a identificação e análise de riscos previsíveis à saúde, segurança ou aos direitos fundamentais, considerando o uso conforme a finalidade prevista; a avaliação de riscos decorrentes de uso

61. *The EU Should Regulate AI on the Basis of Rights, Not Risks*, Access 17 February 2021. <https://www.accessnow.org/eu-regulation-ai-risk-based-approach/>.

indevido razoavelmente previsível; a avaliação de novos riscos com base em dados coletados por meio do sistema de acompanhamento pós-comercialização (art. 72); a adoção de medidas específicas e proporcionais para mitigar os riscos identificados.

Ao implementar esse sistema, os prestadores devem avaliar o potencial impacto sobre grupos vulneráveis, especialmente crianças e adolescentes. Sempre que possível, os riscos devem ser eliminados; caso contrário, devem ser aplicadas medidas de atenuação. Também é necessário fornecer as informações exigidas pelo AI Act e capacitar os responsáveis pela implantação dos sistemas. Testes técnicos devem ser realizados para identificar as medidas mais adequadas de mitigação de riscos.

Outra obrigação é a elaboração e manutenção da documentação técnica, a ser produzida antes da comercialização ou entrada em operação do sistema. Também é exigida a manutenção de registros automáticos de eventos ao longo do ciclo de vida do sistema, assegurando rastreabilidade e alinhamento à sua finalidade prevista.

Quanto à transparência, os sistemas devem ser projetados de forma a permitir que seus resultados possam ser interpretados e utilizados adequadamente pelos responsáveis pela implantação. Devem estar acompanhados de instruções claras e acessíveis, em formato digital ou equivalente.

Além disso, é essencial garantir a supervisão humana eficaz durante o uso do sistema, com o objetivo de prevenir ou mitigar riscos à saúde, à segurança ou aos direitos fundamentais, tanto no uso conforme a finalidade prevista quanto no uso indevido previsível. As medidas de supervisão devem ser compatíveis com o nível de risco, grau de autonomia e contexto de aplicação do sistema.

No que tange à exatidão, solidez e cibersegurança, o AI Act exige que os sistemas de IA de risco elevado sejam desenvolvidos para garantir desempenho consistente, resistência a acessos não autorizados e proteção contra explorações de vulnerabilidades.

A seção 3 do Capítulo III trata das obrigações dos prestadores, responsáveis pela implantação, importadores, distribuidores e outras partes. Qualquer entidade que coloque seu nome ou marca em um sistema de IA de risco elevado; modifique substancialmente um sistema já em operação; altere sua finalidade prevista, é considerada prestadora, assumindo, portanto, obrigações legais. Esses prestadores devem também implementar sistemas de gestão da qualidade e de riscos, mesmo após a entrada do sistema no mercado, incluindo políticas, procedimentos e instruções documentadas.

Ao regulamentar as avaliações de impacto dos sistemas de IA de risco elevado sobre os direitos fundamentais, o AI Act determina que, antes de implementarem um sistema de IA de risco elevado estipulado pelo Anexo III, à exceção dos sistemas de IA de risco elevado destinados a ser utilizados nos domínios de infraestruturas críticas, os responsáveis pela implantação, sejam organismos de direito público, ou entidades privadas que prestam serviços públicos e responsáveis pela implantação de sistemas de IA de risco elevado a que se refere o anexo III, ponto 5, alíneas b)⁶² e c)⁶³, devem realizar uma avaliação do impacto que o uso desse sistema possa ter nos direitos fundamentais. Para isso, os responsáveis pela implantação devem realizar uma avaliação que inclua seis pontos.

O primeiro ponto refere-se à descrição detalhada dos processos do responsável pela implantação, assegurando que o sistema de IA de risco elevado seja utilizado de acordo com sua finalidade prevista. O segundo ponto diz respeito à descrição do período em que o sistema será utilizado e à frequência de sua aplicação. O terceiro ponto trata da identificação das categorias de pessoas singulares e grupos suscetíveis de serem impactados pela utilização do sistema, considerando o contexto específico em questão. O quarto ponto aborda os riscos específicos de danos que possam afetar essas categorias. O quinto ponto exige a descrição da aplicação de medidas de supervisão humana, conforme

62. b) Sistemas de IA concebidos para serem utilizados para avaliar a capacidade de solvabilidade de pessoas singulares ou estabelecer a sua classificação de crédito, com exceção dos sistemas de IA utilizados para efeitos de deteção de fraude financeira;

63. c) Sistemas de IA concebidos para serem utilizados nas avaliações de risco e na fixação de preços em relação a pessoas singulares no caso de seguros de vida e de saúde;

as orientações de utilização do sistema. Por fim, devem ser apresentadas as medidas a serem adotadas caso os riscos se materializem, incluindo disposições sobre a governança interna e os mecanismos de apresentação de queixas.

Após realizar a avaliação de impacto sobre os direitos fundamentais, o responsável pela implantação do sistema de IA deve notificar a autoridade de fiscalização do mercado sobre os resultados obtidos. No entanto, essa obrigação de notificação pode ser dispensada em situações excepcionais em que a ativação de determinados sistemas de IA de risco elevado no território de um Estado-Membro seja justificada por motivos de segurança pública, proteção da vida e da saúde das pessoas, preservação do meio ambiente ou proteção de ativos industriais e infraestruturas essenciais. A dispensa deve ser solicitada por meio de um pedido devidamente fundamentado, e a autorização será concedida por um período limitado, enquanto os procedimentos necessários para a avaliação da conformidade estiverem em andamento, considerando as circunstâncias excepcionais que motivaram a derrogação.

Em síntese, o modelo regulatório proposto pelo AI Act reflete uma tentativa da União Europeia de estabelecer uma governança estruturada e cooperativa para os sistemas de IA de risco elevado, articulando responsabilidades entre autoridades notificadoras, organismos de avaliação e os próprios operadores desses sistemas.

3. MECANISMOS DE PROTEÇÃO E FISCALIZAÇÃO NOS SISTEMAS DE IA DE RISCO ELEVADO

Ainda que o regulamento avance na definição de obrigações e procedimentos, persistem incertezas quanto à aplicação prática das avaliações de impacto e à efetividade dos mecanismos de conformidade, especialmente diante da complexidade técnica e da rápida evolução dessas tecnologias. Assim, a implementação concreta do AI Act dependerá não apenas da clareza normativa, mas também da capacidade institucional dos Estados-Membros e da adaptação contínua dos instrumentos regulatórios frente aos desafios emergentes.

3.1 Mecanismos de conformidade e supervisão

A Seção 5 do capítulo III estabelece normas relativas à avaliação da conformidade, certificações e registro de sistemas de IA. Nessa perspectiva, o AI Act exige que o fornecedor elabore, para cada sistema de IA de risco elevado, uma declaração de conformidade da UE legível por máquina, assinada manual ou eletronicamente. Essa declaração deve identificar claramente o sistema e permanecer acessível às autoridades nacionais competentes por um período mínimo de 10 anos, a contar da data de sua colocação no mercado ou entrada em operação. Uma cópia da declaração deve ser fornecida às autoridades sempre que solicitada.

Nesse sentido, em resumo, antes que um sistema de IA de risco elevado seja introduzido no mercado, quatro etapas principais devem ser cumpridas, aplicáveis inclusive aos componentes individuais. A primeira etapa é o desenvolvimento, que deve contemplar avaliações internas *ex ante* de impacto e, idealmente, seguir Códigos de Conduta, sob a supervisão de equipes multidisciplinares e inclusivas. Em seguida, ocorre a avaliação de conformidade, um processo contínuo de verificação da aderência aos requisitos do AI Act ao longo de todo o ciclo de vida do sistema. Dependendo do caso, essa avaliação poderá envolver a atuação de um organismo notificado externo. Caso o sistema sofra alterações significativas, uma nova avaliação deverá ser realizada. A terceira etapa consiste no registro do sistema em um banco de dados centralizado da UE. Por fim, na quarta etapa, o fornecedor assina a declaração de conformidade e aplica a marcação CE (*Conformité Européenne*), atestando a adequação do sistema às normas europeias. Somente após esse processo o sistema poderá ser comercializado no território da União Europeia.

Contudo, as obrigações dos fornecedores não cessam com a entrada do sistema no mercado. Conforme previsto no regulamento, as responsabilidades passam a ser compartilhadas entre diversos atores. As autoridades competentes da UE e dos Estados-Membros assumem a vigilância de mercado, enquanto os

usuários finais devem garantir a supervisão humana contínua. Por sua vez, os fornecedores devem manter um sistema ativo de monitoramento pós-mercado e, junto aos usuários, são responsáveis por comunicar falhas de funcionamento e incidentes graves.

Esse modelo regulatório baseado em risco, embora essencial para a proteção de direitos fundamentais, impõe um ônus administrativo considerável. As exigências vão desde a produção de planos, certificações e notificações, até a elaboração de documentação técnica e a implementação de marcações. Os custos decorrentes recaem sobre os operadores econômicos, independentemente do porte da organização ou do tipo específico de aplicação da IA. Consequentemente, enquanto grandes empresas tendem a ter mais recursos para cumprir essas obrigações, pequenas empresas e startups enfrentam desafios desproporcionais, especialmente no que se refere à viabilidade econômica e à capacidade técnica para atender às exigências regulatórias.

Para mitigar parte desses desafios, o Serviço para a IA deverá desenvolver um modelo de questionário, preferencialmente por meio de sistema automatizado, que simplifique o cumprimento das obrigações regulatórias por parte dos responsáveis pela implementação dos sistemas e pela avaliação dos impactos sobre os direitos fundamentais.⁶⁴ Apesar dessa previsão, persistem incertezas quanto aos métodos específicos que serão utilizados nessas avaliações, bem como sobre a justificativa para sua aplicação restrita apenas aos sistemas de risco elevado.⁶⁵

Por fim, a Seção 4 do capítulo III trata das autoridades notificadoras e dos organismos notificados. Cada Estado-Membro deve designar ou instituir pelo menos uma autoridade notificadora, encarregada de estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação dos organismos de avaliação da conformidade, além de fiscalizar suas atividades. Esses

64. Comissão Europeia. 2025. "European AI Office." *Shaping Europe's Digital Future*. <https://digital-strategy.ec.europa.eu/en/policies/ai-office>.

65. Davies, Pascale. *Are AI companies complying with the EU AI Act? A new 'LLM Checker' can find out*. Euronews, 16 out. 2024. <https://www.euronews.com/next/2024/10/16/are-ai-companies-complying-with-the-eu-ai-act-a-new-llm-checker-can-find-out>.

procedimentos devem ser desenvolvidos em cooperação com as autoridades notificadoras dos demais Estados-Membros, assegurando uma abordagem harmonizada em todo o território da UE.

Nessa perspectiva, as obrigações impostas pelo AI Act têm gerado reações ambíguas por parte das empresas. Grandes corporações de tecnologia, embora expressem apoio à legislação em termos gerais, demonstram cautela em relação aos detalhes específicos do regulamento. A Amazon, por exemplo, declarou seu compromisso em colaborar com a União Europeia para fomentar um desenvolvimento seguro e responsável da inteligência artificial. Por outro lado, a Meta, de Mark Zuckerberg, manifestou preocupação com um possível excesso de regulação, alertando para os riscos de se comprometer o potencial inovador da IA no contexto europeu.⁶⁶

Diante desse cenário, se a União Europeia deseja de fato afirmar sua liderança na regulação ética e democrática da inteligência artificial, protegendo os direitos fundamentais e promovendo os valores europeus como referências globais, não pode limitar-se à emissão de certificações técnicas baseadas em normas definidas por organismos de padronização. A consolidação de uma atuação normativa robusta exige ir além de uma abordagem meramente organizacional e procedimental, enfrentando os desafios estruturais ainda não solucionados pela legislação vigente.⁶⁷

CONSIDERAÇÕES FINAIS

A União Europeia destacou-se como pioneira ao assumir a vanguarda na regulamentação da inteligência artificial, uma tecnologia que tem se tornado central nas dinâmicas sociais, econômicas e políticas contemporâneas. A IA permeia múltiplas esferas da vida cotidiana, da educação e da saúde à segurança e à gestão pública, oferecendo soluções inovadoras, mas também apresentando

66. Dan Milmo e Alex Hern, "What Will the EU's Proposed Act to Regulate AI Mean for Consumers?," *The Guardian*, 14 mar. 2024. <https://www.theguardian.com/technology/2024/mar/14/what-will-eu-proposed-regulation-ai-mean-consumers>.

67. Finocchiaro, Giusella. *The regulation of artificial intelligence*. *AI & Soc* 39, 1961–1968 (2024). <https://doi.org/10.1007/s00146-023-01650-z>.

desafios éticos e jurídicos de grande complexidade. Reconhecida como uma das tecnologias mais estratégicas do século XXI, a IA suscita preocupações globais quanto aos seus impactos sobre os direitos fundamentais, especialmente no que se refere à privacidade, à dignidade humana e à não discriminação.

Nesse contexto, a União Europeia apresentou, em 2021, a Proposta de Regulamento de Inteligência Artificial, culminando na aprovação, em 13 de março de 2024, da resolução legislativa do Parlamento Europeu que estabelece o Regulamento de Inteligência Artificial (AI Act). Este instrumento normativo inaugurou um marco global na governança da IA, ao propor regras harmonizadas, claras e abrangentes, baseadas em uma abordagem baseada em riscos.

Constatou-se, contudo, que o AI Act, embora represente um avanço regulatório sem precedentes, não constitui uma solução definitiva para os desafios que emergem da interação entre IA e direitos fundamentais no que diz respeito aos sistemas de AI classificados como de risco elevado. Sua eficácia dependerá não apenas da robustez de sua estrutura normativa, mas também da capacidade dos Estados-membros e das instituições europeias de implementar, fiscalizar e atualizar continuamente suas disposições diante da velocidade das inovações tecnológicas.

Além disso, observa-se que o regulamento tende a privilegiar mecanismos técnicos de conformidade e certificação, o que pode ser insuficiente para lidar com os efeitos imprevisíveis e potencialmente discriminatórios dos sistemas de IA, sobretudo quando aplicados em contextos sensíveis, como migração, segurança pública e processos seletivos automatizados. A natureza opaca e autônoma desses sistemas exige um acompanhamento constante e uma governança que vá além da mera verificação técnica.

Ademais, a ausência de critérios suficientemente claros para a classificação dos sistemas de IA gera incertezas e ambiguidades quanto à identificação do nível de risco ao qual pertencem.

Portanto, para que o AI Act concretize seu propósito de promover uma inteligência artificial centrada no ser humano, será essencial que documentos com-

plementares e futuras revisões contribuam para o fortalecimento e a robustez do regulamento. Nesse sentido, o AI Act marca, assim, um passo decisivo, mas inicial, na construção de uma governança global da inteligência artificial, cuja evolução requer vigilância, flexibilidade e um compromisso permanente com a proteção dos direitos humanos.

REFERÊNCIAS

Agência dos Direitos Fundamentais da União Europeia (FRA). 2019. *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, 27 de novembro. <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>.

Agência dos Direitos Fundamentais da União Europeia (FRA). 2020. *Getting the Future Right: Artificial Intelligence and Fundamental Rights*. FRA. <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>.

Alves, Dora Resende, e Ana Carolina Assumpção Stoffel. *O digital como prioridade da Comissão Europeia: breve análise sobre a transformação digital no âmbito da União Europeia*. Porto, Portugal: Instituto Iberoamericano de Estudos Jurídicos, 2022. <http://hdl.handle.net/11328/4082>.

Automating Society Report 2020. Algorithm Watch, [s. l.], 2020. <https://automatingsociety.algorithmwatch.org/>.

BBC News Brasil. "Tribunal Europeu Veta Seguro de Carro Mais Barato para Mulheres." 1 mar. 2011. https://www.bbc.com/portuguese/noticias/2011/03/110301_europa_seguro_rp.

Bicheno, Scott. 2024. „Meta, Ericsson, and Many Others Sign Open Letter to EU over AI Regulation.” *Telecoms.com*, 19 de setembro. <https://www.telecoms.com/ai/meta-ericsson-and-many-others-sign-open-letter-to-eu-over-ai-regulation>.

Bria, Francesca. "Algorithms Are Hiring and Firing Us Now – But Tougher EU Laws Could Protect Workers." *The Guardian*, 12 out. 2023. <https://www.theguardian.com/commentisfree/2023/oct/12/algorithms-eu-law-workers-ai-data>.

Carta dos Direitos Fundamentais da União Europeia. 2012. (2012/C 326/02), 26 de outubro. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

Comissão Europeia. 2025. "Comissão Lança Consulta Pública sobre Sistemas de IA de Risco Elevado." *Digital Strategy*, 6 de junho de 2025. <https://digital-strategy.ec.europa.eu/pt/news/commission-launches-public-consultation-high-risk-ai-systems>

Comissão Europeia. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*. COM(2018) 237 final. Bruxelas: Comissão Europeia, 2018.

Comissão Europeia. *Comunicação da comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das*

Regiões (Documento COM(2019) 640 final). [s.l.], 11 dez. 2019. <https://eur-lex.europa.eu/legal-content/pt/txt/?uri=com%3a2019%3a640%3afin>.

Comissão Europeia. *Coordinated Plan on Artificial Intelligence*. COM(2018) 795 final, [s.l.], 7 dez. 2018. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795>.

Comissão Europeia. *Impact Assessment of the Regulation on Artificial Intelligence: SWD(2021) 84 final*. Shaping Europe's digital future, [s.l.], 21 abr. 2021. <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence>.

Comissão Europeia. *Inteligência artificial: Comissão lança trabalho sobre relação entre tecnologia de ponta e normas éticas*. Comunicado de imprensa, [s.l.], 8 mar. 2018. https://ec.europa.eu/commission/presscorner/detail/pt/ip_18_1381.

Comissão Europeia. *Joint Declaration on the EU's Legislative Priorities for 2018-19*, [s.l.], 14 dez. 2017. https://commission.europa.eu/publications/joint-declaration-eus-legislative-priorities-2018-19_en?prefLang=pt.

Comissão Europeia. *The European AI Alliance*. Shaping Europe's digital future, 14 out. 2024. <https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>.

Conselho da União Europeia. "European Council Meeting (19 October 2017) – Conclusion EUCO 14/17," 2017. <https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf>.

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, [s.l.], 21 mai. 2024. <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/>.

Davies, Pascale. *Are AI companies complying with the EU AI Act? A new 'LLM Checker' can find out*. Euronews, 16 out. 2024. <https://www.euronews.com/next/2024/10/16/are-ai-companies-complying-with-the-eu-ai-act-a-new-llm-checker-can-find-out>.

Dean, James. 2024. "More Complaints, Worse Performance When AI Monitors Work." *Cornell Chronicle*, July 2, 2024. <https://news.cornell.edu/stories/2024/07/more-complaints-worse-performance-when-ai-monitors-work>

Desmarais, Anna. "What Should We Expect as the EU's AI Act Comes into Force?" *Euronews*, 1 ago. 2024. <https://www.euronews.com/next/2024/08/01/what-to-expect-as-the-eus-ai-act-comes-into-force>.

Ezeani, Gabriella, Ansgar Koene, Richa Kumar, Nicole Santiago, David Wright, e Ernst & Young LLP. *A Survey of Artificial Intelligence Risk Assessment Methodologies: The Global State of Play and Leading Practices Identified*. Trilateral Research Ethical AI, dez. 2021. <https://www.trilateralresearch.com/wp-content/uploads/2022/01/A-survey-of-AI-Risk-Assessment-Methodologies-full-report.pdf>.

European Digital Rights (EDRi), Article19, Bits of Freedom, Chaos Computer Club (CCC), Digitale Gesellschaft CH, e IT-Political Association of Denmark (IT-Pol). *Prohibit All Remote Biometric Identification (RBI) in Publicly Accessible Spaces*.

Novembro de 2021. <https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf>

EU AI Act. 2024. "Key Issues." *EU AI Act*, 28 de outubro. [S.l.]. <https://www.euaiact.com/key-issue/1>.

EU AI Act. 2024. "Key Issues." *EU AI Act*, 28 de outubro. [S.l.]. <https://www.euaiact.com/key-issue/3>.

Hidvegi, Fanni; Leufer, Daniel ; Massé, Estelle. "The EU Should Regulate AI on the Basis of Rights, Not Risks." Access 17 February 2021. <https://www.accessnow.org/eu-regulation-ai-risk-based-approach/>.

Fennell, Andrew. 2025. "Inteligência Artificial Não Apenas Automatiza Tarefas, Mas Pode Ser Sua Nova Chefe." *Forbes Brasil*, julho 2025. <https://forbes.com.br/carreira/2025/07/inteligencia-artificial-nao- apenas- automatiza- tarefas- mas- pode- ser- sua- nova- chefe/>

Finocchiaro, Giusella. *The regulation of artificial intelligence*. *AI & Soc* 39, 1961–1968 (2024). <https://doi.org/10.1007/s00146-023-01650-z>.

Forvis Mazars. 2024. "EU AI Act: Different Risk Levels of AI Systems." <https://www.forvismazars.com/ie/en/insights/news-opinions/eu-ai-act-different-risk-levels-of-ai-systems>.

Foxglove. "Home Office Says It Will Abandon Its Racist Visa Algorithm – After We Sued Them." [s.l.], 4 ago. 2020. <https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/>.

Milmo, Dan, e Alex Hern. "What Will the EU's Proposed Act to Regulate AI Mean for Consumers?" *The Guardian*, 14 mar. 2024. <https://www.theguardian.com/technology/2024/mar/14/what-will-eu-proposed-regulation-ai-mean-consumers>.

Moura, Aline Beltrame de. 2024. "Inteligencia Artificial y Organizaciones de Integración Regionales: Ley de IA de la UE." In *Inteligencia Artificial y Diplomacia: Las Relaciones Internacionales en la Era de las Tecnologías Disruptivas*. [S.l.]: Sistema Económico Latinoamericano y del Caribe – SELA. <https://www.sela.org/es/publicaciones/listado-publicaciones/bdd/96978/ia-y-diplomacia-las-relaciones-internacionales-en-la-era-de-las-tecnologias-disruptivas>.

Novelli, C., F. Casolari, A. Rotolo, et al. 2024. "Taking AI Risks Seriously: A New Assessment Model for the AI Act." *AI & Society* 39: 2493–2497. <https://rdcu.be/d1pBv>.

Parlamento Europeu. *Uma Agenda Digital para a Europa*. Fichas temáticas sobre a União Europeia. [S.l.], 2024. <https://www.europarl.europa.eu/factsheets/pt/sheet/64/digital-agenda-for-europe#:~:text=O%20regulamento%20foi%20publicado%20no,confian%C3%A7a%20na%20partilha%20de%20dados>.

Parlamento Europeu, Conselho Europeu, e Comissão Europeia. *Carta dos Direitos Fundamentais da União Europeia*. Jornal Oficial da União Europeia, 2012. Acessado em 4 ago. 2024. http://data.europa.eu/eli/treaty/char_2012/oj.

Tribunal Nacional de Não Discriminação e Igualdade da Finlândia. Decisão 216/2017, 21 mar. 2017. "Discriminação múltipla na avaliação da capacidade de crédito." <https://www.yvtltk.fi/en/index/opinionsanddecisions/decisions.html>.

The EU Should Regulate AI on the Basis of Rights, Not Risks. [S.I.], 17 de fevereiro de 2021. <https://www.accessnow.org/eu-regulation-ai-risk-based-approach/>.

União Europeia. *Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 que estabelece o programa Década Digital para 2030.* Jornal Oficial da União Europeia, 2022.

União Europeia. *Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de abril de 2021 que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240.* Jornal Oficial da União Europeia, 29 abr. 2021.

União Europeia. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de março de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial).* Jornal Oficial da União Europeia, 2024.

União Europeia. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).* Jornal Oficial da União Europeia, 13 jun. 2024.

Received on 15/10/2025

Approved on 15/10/2025