

Nota Informativa

28 DEZEMBRO 2023

Digital, Privacidade e Cibersegurança

Inteligência Artificial: Obtenção de acordo provisório sobre o Regulamento IA

Em abril de 2021, foi proposto o **Regulamento Inteligência Artificial** com a finalidade de melhorar o funcionamento do mercado interno mediante o estabelecimento de um quadro jurídico uniforme para o desenvolvimento, a comercialização e a utilização da inteligência artificial em conformidade com os valores da União.

Em dezembro de 2023, após extensas negociações, os negociadores do Parlamento Europeu e do Conselho chegaram a um acordo provisório sobre as regras aplicáveis à Inteligência Artificial para a União Europeia. O acordo foi considerado histórico por manter o equilíbrio instável entre o impulsionar da inovação e o respeito pelos direitos fundamentais do cidadão.

I. Âmbito de aplicação do regulamento

- Aplica-se a intervenientes públicos e privados dentro e fora da UE se o

sistema de IA for colocado no mercado ou afetar pessoas na UE;

- Isenções para fins militares ou de defesa, investigação, inovação e utilização não profissional.

“We had one objective: To deliver a legislation that would ensure that the ecosystem of AI in Europe would develop with a human-centric approach, respecting fundamental rights and the European values.”

*Brando Benifei,
co-relator do Parlamento Europeu,
Conferência de imprensa sobre o
Regulamento IA,
9 de dezembro de 2023,
Bruxelas*

II. Elementos principais do acordo provisório

Em comparação com a proposta inicial da Comissão os novos elementos deste acordo provisório são:

- Introdução de regras sobre modelos de IA de uso geral de alto impacto que podem causar risco sistémico no futuro, bem como sobre sistemas de IA de alto risco;
- Revisão do sistema de governação, com alguns poderes de aplicação ao nível da UE;
- Extensão da lista de proibições, mas com a possibilidade de uso de identificação biométrica remota em tempo real em espaços acessíveis ao público pelas autoridades policiais, sujeito a restrições
- Obrigação para os fornecedores de sistemas de IA de risco elevado de condução de uma avaliação de impacto sobre direitos fundamentais.

III. Abordagem baseada no risco

Abordagem com quatro níveis de risco dos sistemas de IA:

1. **Risco baixo ou mínimo:** A maioria dos sistemas de IA utilizados na UE cabem dentro desta categoria. Voluntariamente, os fornecedores de tais sistemas poderão desenvolver códigos de conduta para garantir fiabilidade e transparência. *Exemplos:* filtros de spam;
2. **Risco limitado:** Estes sistemas estão sujeitos a obrigações de transparência. *Exemplos:* chat bots ou deepfakes;
3. **Risco elevado:** Exige uma avaliação da conformidade e uma avaliação de impacto sobre os direitos fundamentais. Os fornecedores

de sistemas de IA de risco elevado têm de implementar sistemas de gestão de qualidade e de risco para garantir o cumprimento das normas aplicáveis e minimizar os riscos para os utilizadores e pessoas afetadas. No caso destes sistemas serem utilizados por entidades públicas têm de ser registados numa base de dados pública a nível da UE. *Exemplos:* sistemas sensíveis ligados ao emprego, educação, gestão e funcionamento de infraestruturas críticas;

4. **Risco inaceitável:** Certas utilizações nocivas da IA, que violam os direitos fundamentais, são consideradas inaceitáveis e proibidas. *Exemplos:* classificação social (*social scoring*) assente na IA para uso geral por parte das autoridades públicas, reconhecimento de emoções no local de trabalho ou instituições de ensino, categorização biométrica para identificação de dados sensíveis como orientação sexual, política, religiosa, etc.

IV. Modelos de ia de uso geral

Os fornecedores de modelos de IA de uso geral, incluindo grandes modelos de IA generativa, devem:

- Ser transparentes, divulgando informações essenciais;
- Elaborar um código de boas práticas;
- Elaboração de políticas que garantam o respeito dos direitos de autor quando treinam os modelos de IA;
- Avaliar e atenuar os riscos, comunicar incidentes graves, efetuar testes e avaliações, garantir a cibersegurança e fornecer informação sobre o consumo de energia no caso de

modelos de IA com riscos sistémicos (ou seja, com poder de computação total de mais de 10^{25} FLOPs).

IV. Regulamentação da identificação biométrica

- A identificação biométrica remota em tempo real em espaços acessíveis ao público (ex. reconhecimento facial utilizando *CCTV*) pelas autoridades policiais é restrita, com exceções específicas;
- A identificação de pessoas em material videográfico previamente recolhido de pessoas sob investigação requer autorização prévia de uma autoridade judicial ou administrativa independente e a notificação da autoridade de proteção de dados e da autoridade de fiscalização do mercado.

VI. Entrada em vigor

Entrará em vigor no 20º dia seguinte ao da sua publicação no Jornal Oficial. Será plenamente aplicável 24 meses após a entrada em vigor de maneira gradual:

- Após **6** meses: os EM eliminarão os sistemas de IA proibidos;
- Após **12** meses: Obrigações para modelos de IA de uso geral tornam-se aplicáveis;
- Após **24** meses: Todas as regras passam a ser aplicáveis, incluindo as obrigações relativas aos sistemas de alto risco definidos no anexo III.
- Após **36** meses: Aplicam-se as obrigações relativas aos sistemas de alto risco definidas no anexo II.

VII. Controlo da execução do regulamento IA

1. Autoridades Nacionais Competentes irão supervisionar a aplicação e execução, fiscalizar o mercado e representar o país no Comité Europeu da IA;
2. Fórum Consultivo irá fornecer as competências técnicas adicionais;
3. Gabinete Europeu de IA irá supervisionar modelos de IA de uso geral, cooperará com o Comité Europeu de IA e será apoiado por um painel científico de peritos independentes.


VIII. Sanções

As sanções são calculadas com base no volume de negócios mundial anual das empresas infratoras/teto máximo, tipo de sistema de IA e gravidade da infração:

- Até € 35 milhões ou 7% do volume de negócios mundial correspondente ao ano financeiro anterior por infrações a práticas proibidas ou incumprimento relacionado com os requisitos em matéria de dados;
- Até € 15 milhões ou 3% do volume de negócios mundial correspondente ao ano financeiro anterior pelo não cumprimento de qualquer outro requisito ou obrigação do Regulamento; e
- Até € 7,5 milhões ou 1,5% do volume de negócios mundial correspondente ao ano financeiro anterior pela prestação de informações incorretas, incompletas ou enganosas às entidades competentes.

Sem prejuízo, sanções aplicáveis a pequenas e médias empresas ou *start-ups* terão limites proporcionais.

IX. Atuação perante uma violação do regulamento IA

- Apresentação de queixa junto de uma autoridade nacional;
- Fiscalização do mercado pelas autoridades nacionais competentes;
- Divulgação de provas sobre sistemas específicos de IA de alto risco que se suspeite terem causado danos, no caso de tentativa de obtenção de indemnização por danos causados por sistemas de IA de alto risco;
- Possibilidade de indemnização das pessoas que sofram morte, lesões corporais ou danos materiais causados por sistemas de IA defeituosos na UE. 

Contactos



Pedro Vidigal Monteiro
Sócio
p.vidigalmonteiro@telles.pt



Ana Ferreira Neves
Of Counsel
a.neves@telles.pt

O presente documento destina-se a ser distribuído entre Clientes e Colegas e as informações nele contidas são de carácter geral e abstrato e não dispensam aconselhamento

jurídico para a resolução de questões concretas. Esta informação não pode ser reproduzida, no todo ou em parte, sem o consentimento expresso da TELLES.