APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO

RECOMENDAÇÃO

Consulta pública da Comissão Europeia em matéria de Inteligência Artificial

29 de julho de 2021

Áreas principais que requerem revisão ou esclarecimento

1. Esclarecer o balanço de responsabilidades entre prestadores de IA, distribuidores e utilizadores, especialmente para API's de propósito geral e modelos de open source: como foi explanado, o AIA não distingue suficientemente as responsabilidades dos utilizadores de IA quando no desempenho do papel de distribuidor e as responsabilidades dos prestadores para com os seus consumidores. A não ser que tal seja claro na medida razoável, arrisca-se a ter um efeito dissuasor na publicação de modelos em open source e em API's, que é tão importante para a inovação de IA e na sua adoção pela indústria. Deixamos algumas recomendações:

- A diretiva de IA não fornece uma definição de "distribuidor". Por questões de clareza, seria útil que o fizesse. Uma definição sensata seria a de "distribuidor" para nos referirmos à entidade que faz com que o sistema de IA esteja disponível para uso num contexto operacional específico. Por vezes (ex: se o sistema está

construído de forma personalizada para o distribuidor pelo programador) o distribuidor pode ser o mesmo que o prestador. Mas, noutros casos, tal não acontecerá se sistemas IA de propósito geral forem utilizados.

- Os distribuidores devem suportar a responsabilidade primária de observância, conformidade, avaliação e monitorização post-market, pois só eles podem verificar as aplicações finais para as quais os seus sistemas estão a ser usados e outra informação adicional que tenha sido introduzida da formação do seu sistema. Ao contrário, seria igual a responsabilizar os fabricantes de tijolo por assegurar a integridade estrutural de uma torre, ao invés de os arquitetos, engenheiros e construtores que desenharam e construíram a mesma.
    - Para ser claro, o ónus deve ser colocado aos distribuidores em todas as circunstâncias, independentemente da marca ou da maneira precisa em que o sistema de IA foi obtido. Caso se esteja a utilizar IA de propósito geral, tirado da prateleira, numa operação de alto risco ou caso o sistema tenha sido modificado, só a organização que utiliza o sistema de IA é que terá conhecimento sobre como estará a ser utilizado o sistema.

2. Rever a linguagem usada em standards inviáveis: É importante manter requisitos realistas, em concordância com as boas práticas e práticas viáveis da indústria. Enquanto concordamos com a direção dos requisitos para sistemas de IA de risco elevado, consideramos que alguma linguagem utilizada merece atenção acrescida de forma a evitar a criação de standards que são de facto impossíveis para qualquer fornecedor alcançar. Em particular:

- O artigo 10 (3) indica que "Os conjuntos de dados de treino, validação e teste devem ser pertinentes, representativos, isentos de erros e completos." No entanto, é impossível garantir este nível de perfeição e consequentemente impossível de alcançar este requisito, pois algumas técnicas de privacidade introduzem deliberadamente erros (em forma de ruído) nos conjuntos de dados. Adicionalmente, é impossível a compleição total de conjuntos de dados, uma vez que a natureza destes conjuntos materializa-se numa amostra da realidade e porventura não inclui todos os dados disponíveis. Sugerimos uma frase mais

realista como "Devem ser garantidos esforços adequados de forma a garantir um conjunto de dados relevante, representativo, livre de erros e completo".

- O artigo 14 (4a) afirma que indivíduos responsáveis por supervisão humana devem "compreender completamente as capacidades e limitações do sistema de IA de risco elevado". Consideramos este requisito injustificadamente elevado visto ser impossível atender a este nível de compreensão quando se fala de redes neurais complexas. Sugerimos um requisito mais realista que requer indivíduos a ter "um entendimento apropriado das capacidades e limitações…".

3. Esclarecer praticalidades de 'due diligence': existem várias áreas onde é necessária uma maior orientação quanto às expectativas de conformidade. Por exemplo:

- O artigo 10 - Dados e governação de dados: Por vezes, sistemas de IA são construídos utilizando conjuntos de dados providenciados por terceiros, incluindo os de *open-source*. Ao avaliar a conformidade com o artigo 10, quanta confiança pode ser colocada nas representações feitas pelos criadores dos conjuntos de dados, relativamente ao consentimento, privacidade, etc.? Quais as expectativas de *due diligence* caso não haja nenhuma informação sobre a proveniência do conjunto de dados?
- O artigo 12 - Manutenção de registos: Para certos serviços, pode haver preocupações sobre conectividade ou privacidade que resultam num sistema de IA a ser construído para utilizar *on-device learning* (em vez de na *Cloud*). Como deve a manutenção de registos ser cumprida nestas circunstâncias, quando não há uma referência centralizada? De um modo geral, o cumprimento das obrigações de registo parecem violar o princípio da minimização dos dados presente no RGPD - na prática, como deve ser isto equilibrado?

4. Reenquadrar requisitos desproporcionais. Em alguns casos, os requisitos são geralmente, ou até extremamente, desproporcionais, devendo ser alterados.

Especificamente:

- O Artigo 64 (2) refere que "...mediante pedido fundamentado, deve ser concedido às autoridades de fiscalização do mercado o acesso ao código-fonte do sistema de

IA". Porém o código-fonte encontra-se protegido pela diretiva europeia de segredos comerciais, havendo sempre a possibilidade de métodos alternativos para verificar a performance de um sistema de IA (ex. auditorias internas/externas) tornando o acesso ao código-fonte supérfluo.

- Consideramos como melhor opção a alteração parcial do nº2 do artigo 64 para o seguinte: "após solicitação justificada, os operadores ou implantadores de IA devem apoiar e equipar autoridades de fiscalização de mercado com os meios necessários de forma a facilitar uma testagem robusta (ex. auditoria internas/externas) nos casos que exijam conformidade com os requisitos".

SOBRE A APDSI

Criada em 2001, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) tem por objetivo a promoção e desenvolvimento da transformação e inclusão digital em Portugal, reunindo com este interesse comum profissionais, académicos, empresas, organismos públicos e cidadãos em geral.

Na linha destes propósitos a APDSI tem vindo a desenvolver diversas atividades em torno de causas tecnológicas e societais, que se traduzem num conjunto de eventos, recomendações e estudos realizados por grupos de trabalho multidisciplinares em diversas áreas de intervenção, como a Segurança, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, a Governação das TIC, a Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação e as Competências digitais.

Em todos estes trabalhos a APDSI procura identificar as tendências de evolução e também as interações entre as tecnologias e outras dimensões sociais e económicas, contribuindo com uma visão mais aberta para a discussão e tendo como meta a eficaz perceção e implementação destes conceitos na Sociedade Portuguesa. A APDSI tem o Estatuto de Utilidade Pública e foi em 2008 reconhecida como ONGD.

APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO

Associação de Utilidade Pública

ONG – Organização Não Governamental

Rua Alexandre Cabral, 2C – Loja A
1600-803 Lisboa – Portugal
URL: www.apdsi.pt

Tel.: (+351) 217 510 762
Fax: (+351) 217 570 516
E-mail: secretariado@apdsi.pt

Patrocinadores Globais da APDSI

accenture aws Google