PRIVUS MONTH INSIGHTS · Nº 4 · OUTUBRO 2026

AI ACT · AI GOVERNANCE · PROTEÇÃO DE DADOS

A sua empresa utiliza IA. Mas sabe que responsabilidade está a assumir?

Entre utilização, adaptação e integração: a fronteira entre provider e deployer no AI Act.

Uma empresa contrata uma solução de inteligência artificial, liga-a aos seus dados e adapta-a ao seu negócio. O modelo pertence a um fornecedor externo. A integração é feita por um prestador especializado. As decisões sobre a utilização ficam dentro da empresa.

Quando surge uma falha, cada interveniente conhece a sua parte. Nem sempre alguém consegue responder pelo conjunto.

É aqui que a distinção entre quem fornece e quem utiliza IA revela uma dificuldade prática: **há empresas que intervêm significativamente num sistema sem controlar todos os componentes de que ele depende.**

Defendemos que essa intervenção merece um reconhecimento mais explícito. A classificação jurídica deve permitir identificar responsabilidades concretas ao longo da cadeia, incluindo as de quem integra e adapta tecnologia de terceiros.

1. O espaço entre fornecer e utilizar

O AI Act distingue o fornecedor (*provider*) do responsável pela implantação (*deployer*) e reconhece outros operadores, como importadores e distribuidores. Contudo, não estabelece uma categoria autónoma e transversal para o integrador.

Quem combina componentes, configura comportamentos ou adapta uma solução precisa de encontrar o seu enquadramento nas categorias existentes. E a condição de fornecedor não está reservada a quem desenvolve o código: pode abranger quem manda desenvolver um sistema e o coloca em serviço sob o seu nome. [1]

A dificuldade está na distância entre essas categorias e a distribuição real do trabalho. Uma organização pode controlar os dados e a configuração, depender de terceiros para testar o modelo e assumir perante o cliente a solução final.

É essa falta de granularidade que questionamos. Reconhecer expressamente a função de integração ajudaria a tornar visíveis as suas obrigações. Para ser útil, esse reconhecimento teria de preservar uma responsabilidade identificável pela conformidade do sistema.

2. Uma adaptação pode mudar a posição da empresa

Imagine-se uma empresa que encomenda uma ferramenta para apoiar a seleção de candidatos. O prestador integra um modelo externo, a empresa define os critérios de avaliação e o fornecedor do modelo mantém o controlo sobre a sua evolução.

Antes de discutir quem responde por uma decisão inadequada, há perguntas mais imediatas: quem validou a ferramenta para aquela finalidade? Quem aprovou os critérios? Uma atualização do modelo exige novos testes?

Para os sistemas de risco elevado, o regime previsto no artigo 25.º contempla situações em que um responsável pela implantação ou outro interveniente passa a ser considerado fornecedor. Entre elas estão determinadas modificações substanciais e alterações de finalidade que tornam o sistema de risco elevado. O artigo também prevê cooperação e acordos escritos na cadeia de valor. [2]

Nem toda a configuração produz esse efeito. A modificação substancial tem uma definição própria, ligada à avaliação de conformidade inicial e ao impacto da alteração nos requisitos aplicáveis ou na finalidade prevista. [1]

Por isso, o enquadramento deve ser revisto quando a intervenção muda. Um contrato assinado no início do projeto pode deixar de descrever adequadamente a realidade da operação.

3. O que outros referenciais permitem ver

A comparação com outros referenciais ajuda a perceber como esta distribuição pode ganhar precisão.

ISO/IEC 42001: reconhecer as funções existentes

A ISO/IEC 42001 inclui, na nota explicativa da cláusula 4.1, diferentes papéis organizacionais, entre eles integradores de sistemas e fornecedores de dados. Admite também que uma organização desempenhe várias funções.

Esta abordagem permite descrever com maior detalhe a participação de cada entidade. Enquanto norma de gestão, não altera os estatutos legais do AI Act. Oferece, porém, uma base útil para organizar responsabilidades que uma classificação jurídica, isoladamente, não consegue detalhar. [3]

RGPD: olhar para quem decide

Na proteção de dados, a qualificação exige perceber quem determina as finalidades e os meios do tratamento. A responsabilidade conjunta admite intervenções diferentes, sem pressupor uma participação igual.

A lição é relevante para a governação da IA: os contratos devem refletir as decisões efetivas. Isso exige análises separadas. Ser *provider* não determina automaticamente a condição de responsável pelo tratamento; ser *deployer* também não significa ser subcontratante. [4]

Brasil: distribuir deveres pelo ciclo de vida

O texto do PL 2338/2023 remetido pelo Senado à Câmara distingue desenvolvedor, distribuidor e aplicador. Relaciona ainda as medidas de governação com a fase do ciclo de vida e o conhecimento de cada agente.

A proposta também prevê a passagem a desenvolvedor em caso de modificação substancial ou alteração da finalidade. Não elimina, portanto, a questão da mudança de estatuto.

O contributo está na atenção dada à participação de cada interveniente. Trata-se de uma proposta em tramitação, não de legislação vigente nem de três graus sucessivos de responsabilidade. [5]

4. O que deve ficar decidido antes da integração

Para uma empresa, esta discussão tem consequências na contratação e na aprovação dos projetos. Há quatro questões que devem ficar documentadas:

01 **Papel jurídico**

Em que qualidade intervém cada entidade no sistema concreto?

02 **Poder de decisão**

Quem escolhe os dados, aprova configurações e autoriza alterações?

03 **Capacidade de verificação**

Quem fornece a documentação e realiza os testes necessários?

04 **Resposta a falhas**

Quem investiga, corrige e pode suspender a utilização?

Uma cláusula genérica de cumprimento da legislação dificilmente resolve estas questões. É preciso acordar entregáveis, acesso à informação e mecanismos de cooperação.

Também não basta declarar que o modelo pertence a um terceiro. Quando a informação disponível é insuficiente para sustentar a utilização pretendida, essa limitação deve pesar na decisão de contratar ou avançar.

A responsabilidade precisa de acompanhar a intervenção

Defendemos um reconhecimento mais explícito da função de integração, com deveres ajustados à intervenção de cada entidade e uma responsabilidade clara pela conformidade do sistema.

As empresas podem começar já por tornar essa distribuição visível nos seus contratos e processos. Isso implica saber quem decide, quem verifica e quem tem condições para corrigir.

Antes de colocar uma solução de IA em funcionamento, a empresa deve conseguir explicar que responsabilidade assumiu - e demonstrar que dispõe dos meios para a cumprir.

Fontes e referências

1. AI Act, artigo 3.º, pontos 3, 4, 8 e 23. Definições de fornecedor, responsável pela implantação, operador e modificação substancial.

2. AI Act, artigo 25.º, n.os 1, 2 e 4. Responsabilidades na cadeia de valor. As obrigações devem ser lidas com o calendário de aplicação do artigo 113.º.

3. ISO/IEC 42001:2023, cláusula 4.1, nota 1. Contexto da organização e papéis no ecossistema de IA, com remissão para ISO/IEC 22989.

4. EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, versão 2.1; RGPD, artigos 4.º, pontos 7 e 8, 26.º e 28.º.

5. Brasil, PL 2338/2023, texto remetido pelo Senado à Câmara em março de 2025, artigos 4.º e 18.º, §§ 4.º e 5.º. Tramitação legislativa, consultada em 4 de outubro de 2026.

Conteúdo informativo e geral. Não constitui parecer jurídico, auditoria, certificação ou recomendação aplicável sem análise do contexto concreto.

Para conversar sobre o contexto da sua organização: contacto@privuskuzola.pt · +351 936 246 971