Enquadramento do Regulamento Europeu da Inteligência Artificial

Introdução

Esta regulamentação emblemática segue uma abordagem «baseada no risco», o que significa que quanto maior for o risco de danos para a sociedade**,** mais rigorosas são ou deverão ser as regras. O novo Regulamento classifica diferentes tipos de inteligência artificial em função do risco. Os sistemas de IA que apresentem apenas um risco limitado estarão sujeitos a obrigações de transparência muito ligeiras, ao passo que os sistemas de IA de risco elevado serão autorizados, embora sujeitos a um conjunto de requisitos e de obrigações para obterem acesso ao mercado da UE.

Os sistemas de IA que envolvam, por exemplo, a manipulação cognitiva de comportamentos ("*as técnicas de manipulação propiciadas pela IA podem ser utilizadas para persuadir as pessoas a adotarem comportamentos indesejados, ou para as enganar incentivando-as a tomar decisões de uma forma que subverta e prejudique a sua autonomia, a sua tomada de decisões e a sua liberdade de escolha"*) e a classificação social serão proibidos na UE porque o seu risco é considerado inaceitável. O regulamento proíbe igualmente a utilização da IA para o policiamento preditivo com base na definição de perfis e em sistemas que utilizam dados biométricos para classificar as pessoas por categorias, como a raça, a religião ou a orientação sexual de uma pessoa.

Embora a abordagem baseada no risco constitua a base para um conjunto proporcionado e eficaz de regras vinculativas, é importante recordar as Orientações Éticas para uma IA de Confiança, elaboradas em 2019 pelo GPAN em IA independente nomeado pela Comissão. Nessas orientações, o GPAN em IA desenvolveu sete princípios éticos não vinculativos para a IA, que se destinam a ajudar a garantir que a IA é de confiança e eticamente correcta. Os sete princípios incluem: iniciativa e supervisão por humanos; solidez técnica e segurança; privacidade e governação dos dados; transparência; diversidade, não discriminação e equidade; bem-estar social e ambiental e responsabilização. Sem prejuízo dos requisitos juridicamente vinculativos do presente regulamento e de quaisquer outras disposições aplicáveis do direito da União, essas orientações contribuem para a concepção de uma IA coerente, de confiança e centrada no ser humano, em consonância com a Carta dos Direitos Fundamentais e com os valores em que se funda a União Europeia.

Ao mesmo tempo, visa assegurar o respeito pelos direitos fundamentais dos cidadãos da UE e estimular o investimento e a inovação em inteligência artificial na Europa. Todavia, o Regulamento IA aplica-se apenas aos domínios abrangidos pelo direito da UE e prevê isenções, por exemplo, para sistemas que são utilizados exclusivamente para fins militares e de defesa, bem como para fins de investigação científica.

Além das inúmeras utilizações benéficas da IA, essa tecnologia também pode ser utilizada indevidamente e potenciar instrumentos novos e poderosos para práticas manipuladoras, exploratórias e de controlo social. Essas práticas são particularmente prejudiciais e abusivas e deverão ser proibidas por desrespeitarem valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como os direitos fundamentais consagrados na Carta, nomeadamente o direito à não discriminação, à protecção de dados pessoais e à privacidade, e os direitos das crianças.

A dimensão das repercussões negativas causadas pelo sistema de IA nos direitos fundamentais protegidos pela Carta é particularmente importante quando se classifica um sistema de IA como sendo de risco elevado. Esses direitos incluem o direito à dignidade do ser humano, o respeito da vida privada e familiar, a protecção de dados pessoais, a liberdade de expressão e de informação, a liberdade de reunião e de associação, a não discriminação, o direito à educação, a defesa dos consumidores, os direitos dos trabalhadores, os direitos das pessoas com deficiência, a igualdade de género, os direitos de propriedade intelectual, o direito à acção e a um tribunal imparcial, o direito à defesa e a presunção de inocência e o direito a uma boa administração.

Além desses direitos, é importante salientar que as crianças têm direitos específicos, consagrados no artigo 24.º da Carta e na Convenção das Nações Unidas sobre os Direitos da Criança (desenvolvidos com mais pormenor no Comentário Geral n.º 25 da Convenção das Nações Unidas sobre os Direitos da Criança no respeitante ao ambiente digital), que exigem que as vulnerabilidades das crianças sejam tidas em conta e que estas recebem a protecção e os cuidados necessários ao seu bem-estar.

O direito fundamental a um nível elevado de protecção do ambiente consagrado na Carta e aplicado nas políticas da União também deverá ser tido em conta ao avaliar a gravidade dos danos que um sistema de IA pode causar, nomeadamente em relação à saúde e à segurança das pessoas.

Relativamente aos sistemas de IA de risco elevado que são componentes de segurança de produtos ou sistemas ou que são, eles próprios, produtos ou sistemas abrangidos pelo âmbito de aplicação do Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, do Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho, do Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho, da Diretiva 2014/90/UE do Parlamento Europeu e do Conselho, da Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho, do Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho e do Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho.

Vejamos agora, melhor, alguns tópicos importantes.

Traços Genéricos do Regulamento da IA

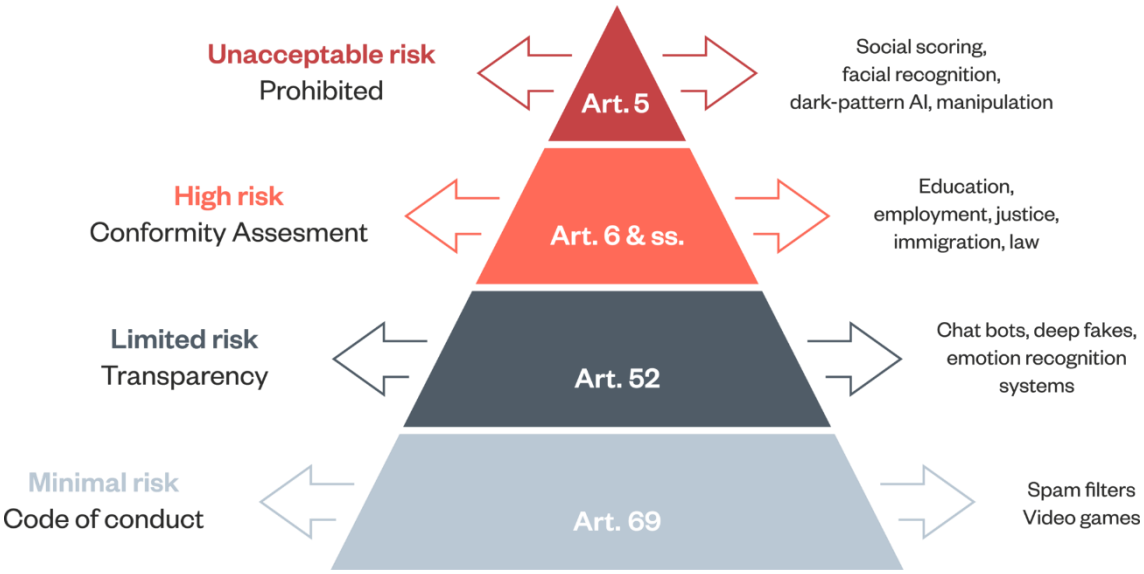
O novo Regulamento da Inteligência Artificial (IA) aprovado em 2024 pela União Europeia, também denominado e conhecido como o AI Act, estabelece um marco regulatório para a utilização de IA, com o objectivo de garantir a segurança, a transparência e a ética na aplicação dessas tecnologias.

Aqui estão os principais pontos a considerar com o novo Regulamento da Inteligência Artificial:

A. Classificação de Risco

O AI Act classifica sistemas de IA com base no risco que apresentam para os direitos fundamentais, a segurança e a saúde dos indivíduos:

- *Risco Inaceitável*: Sistemas de IA que são considerados uma ameaça à segurança, meios de subsistência e direitos das pessoas são proibidos.
  Exemplos incluem sistemas de pontuação social pelo governo e IA que manipula comportamento humano de forma prejudicial. (artigo 5)
- *Risco Alto*: Aplicações de IA em áreas críticas, como infraestruturas, saúde, emprego, aplicação da lei, administração pública e gestão de fluxos de migração. Estes sistemas estão sujeitos a regulamentações rigorosas. (artigo 6)
- *Risco Limitado*: Sistemas de IA que exigem transparência.
  Por exemplo, IA que interage com humanos deve informar que estão a interagir com uma IA. (artigo 52)
- *Risco Mínimo ou Nulo*: A maioria das aplicações de IA que apresentam baixo risco e estão sujeitas a obrigações mínimas. (artigo 69)



B. Requisitos para Sistemas de Alto Risco

Sistemas de IA considerados de alto risco estão sujeitos a uma série de requisitos rigorosos, incluindo:

- *Gestão de Risco*: deve ser implementado um sistema de gestão de risco ao longo do ciclo de vida do sistema de IA.
- *Governança de Dados*: requisitos rigorosos sobre a qualidade dos dados utilizados, incluindo precisão, integridade e representatividade.
- *Documentação e Registo*: manutenção de documentação técnica detalhada e registos das actividades do sistema de IA.
- *Transparência e Fornecimento de Informações*: os usuários devem ser claramente informados sobre o funcionamento do sistema de IA e suas limitações.
- *Supervisão Humana*: implementação de medidas para garantir que haja supervisão humana sobre os sistemas de IA de alto risco.
- *Cibersegurança*: requisitos para garantir a segurança e a resiliência dos sistemas de IA contra ataques cibernéticos.

C. Proibições Específicas

O regulamento proíbe explicitamente certas práticas de IA:

- *Vigilância Biométrica Remota em Tempo Real em Espaços Públicos*: salvo excepções estritamente definidas para a aplicação da lei.
- *Sistemas de IA que Exploram Vulnerabilidades de Grupos Específicos*: como crianças ou pessoas com deficiências.
- *Sistemas de IA que Avaliam ou Classificam a Confiança Social*: feitos por governos ou terceiros.

D. Transparência e Direitos dos Usuários

- *Direito à Informação*: usuários devem ser informados quando estão a interagir com sistemas de IA.
- *Explicabilidade*: os sistemas de IA devem ser suficientemente transparentes para permitir que os usuários os compreendam.
- *Recursos*: usuários devem ter acesso a mecanismos de recurso em caso de decisões adversas tomadas por sistemas de IA.

E. Conformidade e Fiscalização

- *Órgãos de Supervisão Nacional*: cada Estado-Membro deve designar uma autoridade competente para supervisionar a aplicação do regulamento.
- *Conformidade e Avaliação*: sistemas de IA de alto risco devem passar por avaliações de conformidade antes de serem colocados no mercado.
- *Multas e Penalidades*: o regulamento prevê penalidades substanciais para a não conformidade, incluindo multas significativas que podem atingir até 6% do volume de negócios anual global da empresa.

F. Inovação e Apoio às PME

- *Sandboxes Regulamentares*: criação de ambientes controlados para testes de IA, permitindo inovação enquanto se garante a conformidade regulatória.
- *Apoio às PME*: medidas específicas para apoiar pequenas e médias empresas na implementação e conformidade com o regulamento.

G. Impacto Global e Harmonização

- *Harmonização*: busca harmonizar as leis de IA entre os Estados-Membros, evitando fragmentação no mercado interno.

H. Educação e Capacitação

- *Capacitação de Profissionais*: incentivo à formação e capacitação de profissionais em IA para assegurar que a força de trabalho esteja preparada para lidar com as novas tecnologias.
- *Educação Pública*: campanhas e programas educacionais para aumentar a literacia digital e a compreensão pública sobre IA e seus impactos.

Crítica a estes Traços Genéricos

- *Vulnerabilidade humana*

O Regulamento da UE sobre IA tem dezasseis referências à vulnerabilidade humana. Apesar destas referências, este conceito de vulnerabilidade humana é, no entanto, difícil de compreender e delimitar. Isto enfatiza a necessidade de fornecer definições precisas e completas para conceitos como "vulnerabilidade". Isto garantiria que todas as formas de vulnerabilidade fossem cobertas e ajudaria a melhorar a forma como é aplicado. Assim, além de formas imediatamente reconhecidas, como a menor idade ou a deficiência, há também outras menos visíveis, como a iliteracia e as carências sociais ou económicas.

- *Excesso de regulamentação e impacto global*

A comunidade empresarial alerta que o Regulamento pode levar a uma regulamentação excessiva, o que poderá não só abrandar a inovação tecnológica, mas também estabelecer um precedente restritivo a nível mundial. O texto final do Regulamento não discute explicitamente o excesso de regulamentação ou o seu impacto global. No entanto, centra-se na harmonização das regras em toda a UE para evitar regulamentações nacionais divergentes que possam fragmentar o mercado, limitar o desenvolvimento, estabelecer discriminações e impedir a implantação da IA.

- *Perturbação do mercado*

❖ Impacto nas pequenas e médias empresas

A ampla aplicação do Regulamento pode afectar desproporcionalmente as *startups* e as pequenas e médias empresas (PME), que podem considerar os requisitos demasiado

rigorosos ou onerosos. Os críticos do Regulamento da IA argumentam que os custos de conformidade e os encargos administrativos podem impedir as PME de inovar ou mesmo de adoptar tecnologias de IA, afectando assim o seu potencial de crescimento e o avanço tecnológico global na EU, para além de serem factor de discriminação entre estas e as grandes empresas. O Regulamento da IA contém passagens específicas sobre as PME. A lei visa aumentar a competitividade e garantir que as pequenas e médias empresas possam navegar no ambiente regulamentar sem enfrentar encargos desproporcionais.

- ❖ O domínio das grandes empresas de tecnologia

A terceirização vertical em IA, como os investimentos da Microsoft em OpenAI e a colaboração com a empresa Mistral, escapa actualmente à regulamentação de fusões. Isto permite que as grandes corporações obtenham vantagens competitivas que podem ser injustas, limitando a concorrência e concentrando o mercado, o que prejudica a concorrência, a inovação e os consumidores.

Os modelos de IA de alto risco devem ser abrangidos pela regulamentação da UE em matéria de concorrência. Dada a importância potencial destes modelos e os grandes recursos necessários para o desenvolvimento e operação, as autoridades da concorrência serão ou terão de ser capazes de regular mais rigorosamente as suas operações.

Isto impede que as empresas exerçam controlo sobre os modelos de IA, bem como sobre outras tecnologias e plataformas que possam promover actividades injustas e abusivas, sobretudo impedindo o seu uso normal ou acesso simplificado e a custos adequados a terceiros.

- *Desafios de aplicação*

O sucesso do Regulamento depende da sua aplicação rigorosa, eficaz e eficiente. Parece difícil a implementação de um novo gabinete europeu de IA considerando os recursos que seriam necessários para garantir a conformidade. Há também um debate contínuo sobre a regulamentação de sistemas de IA de uso geral (GPAI), como o ChatGPT, uma categoria separada foi incluída no Regulamento de IA para esse fim. Estes sistemas avançados de IA estão a evoluir rapidamente. Este crescimento é impulsionado principalmente por avanços exponenciais no poder computacional para treinar sistemas avançados de IA. Isto significa que o actual Regulamento pode rapidamente ficar desactualizado à medida que a tecnologia avança. O poder computacional pode ser uma métrica útil para priorizar a aplicação da IA e classificar a próxima geração de modelos GPAI potencialmente mais desenvolvidos, mas também geradores de maiores riscos.

Algumas Consequências para Advogados e Sociedades de Advogados

Para advogados e sociedades de advogados este Regulamento é-lhes igualmente aplicável uma vez que, de acordo com o seu âmbito de aplicação previsto no seu artigo 2º, as sociedades de advogados podem integrar este mesmo âmbito desde que utilizem mecanismos de IA na sua actividade.

Sendo o desempenho das actividades dos advogados enquadrado no ramo da Justiça, todas as ferramentas de IA utilizadas para o normal desempenho da sua actividade profissional serão ou poderão ser consideradas como de risco elevado.

Exemplos: IA em recrutamento de magistrados, de advogados, de colaboradores que pode discriminar candidatos com base em critérios injustos; sistemas de IA usados em procedimentos judiciais para avaliar a credibilidade dos relatos de partes, sujeitos processuais, assistentes, arguidos, vítimas, demandantes e demandados civis, órgãos de polícia criminal, funcionários judiciais, solicitadores, agentes de execução, testemunhas, peritos, consultores técnicos, intervenientes acidentais; etc.

O AI Act apresenta tópicos de particular relevância que impactam directamente com as suas actividades, bem como geram responsabilidades, desde que relacionadas com o uso de inteligência artificial (IA). Do raciocínio supramencionado, os principais tópicos do AI Act que devem ser considerados são:

1. Classificação de Risco e Conformidade

- *Identificação de Sistemas de Alto Risco*: advogados devem estar cientes de quais sistemas de IA utilizados na sua actividade são classificados como de alto risco e garantir que esses sistemas cumpram os requisitos de conformidade.

- *Gestão de Risco*: implementação de sistemas de gestão de risco para monitorar e mitigar riscos associados ao uso de IA.

2. Requisitos para Sistemas de Alto Risco

- *Documentação e Auditoria*: manter documentação detalhada e registos das actividades dos sistemas de IA utilizados, além de estar preparado para auditorias de conformidade perante a autoridade competente.

- *Supervisão Humana*: garantir a supervisão humana e adequada sobre os sistemas de IA, especialmente aqueles usados para tomar decisões legais ou que possam afectar directamente os clientes ou os visados pelo sistema de justiça.

3. Transparência e Direitos dos Usuários

- *Informação aos Clientes*: advogados têm agora o dever de informar os seus clientes de quando estão a interagir com sistemas de IA e a providenciar explicações acessíveis/compreensíveis sobre como essas tecnologias estão a ser utilizadas.

- *Argumentação*: advogados devem ser capazes de explicar as decisões tomadas por sistemas de IA, especialmente em contextos jurídicos onde a clareza e a transparência são essenciais.

4. Protecção de Dados e Privacidade

- *Governance de Dados*: garantir a qualidade, a integridade e a representatividade dos dados utilizados pelos sistemas de IA, seguindo rigorosamente as regulamentações de protecção de dados, como o RGPD e o actual AI Act e as normas de direito interno.

-Segurança: implementar medidas robustas de segurança para proteger dados sensíveis e garantir o anonimato dos dados quando aplicável. Através de medidas de cibersegurança é possível garantir que os sistemas de IA são protegidos de ataques cibernéticos e de outras ameaças internas ou externas à segurança e à fiabilidade da informação.

5. Ética e Responsabilidade

- *Responsabilidade Legal*: acaba por não se prever neste Regulamento a responsabilidade directa por erro no uso ou aproveitamento das ferramentas de IA, contudo assume-se que na contratação de seguro de responsabilidade civil profissional seja possível negociar a inserção de tal cláusula específica sem o que haverá ou poderá haver um vazio de protecção. Como tal, importa compreender e definir claramente a responsabilidade legal em casos de danos ou violações de direitos causados por sistemas de IA. E importa ainda, pelo menos, actualizar as cláusulas gerais e as cláusulas especiais do seguro da Ordem dos Advogados e dos seguros complementares.

6. Formação e Capacitação

- *Formação Inicial, Complementar e Contínua*: Investir em formação para inicial, complementar e contínua para advogados-estagiários e advogados, bem como para colaboradores de escritórios e sociedades de modo a garantir que estejam actualizados sobre as melhores práticas e requisitos regulatórios relacionados com a IA. Isto permite desenvolver conhecimento técnico suficiente para avaliar, implementar e supervisionar sistemas de IA de maneira eficaz.

Perante o Regulamento o que devem fazer Advogados e Sociedades de Advogados?

Avaliação de Impacto e Conformidade

Obviamente que as associações representativas dos advogados, designadamente a Ordem dos Advogados, têm aqui responsabilidades acrescidas e poderiam e deveriam ter a liderança activa nestas matérias. Enquanto isso não sucede, os advogados e as sociedades de advogados devem começar a avaliar o impacto potencial das soluções de IA em termos de classificação de risco, adoptando uma abordagem proactiva para garantir conformidade com os padrões internacionais, europeus e nacionais emergentes. Isso inclui realizar avaliações de impacto tecnológico, organizacional, ético e de risco para sistemas de IA, especialmente para aqueles que podem ser considerados de alto risco.

Transparência e Governance de IA

Desenvolver e implementar políticas internas de *governance* de IA que promovam conhecimento dos algoritmos, transparência de procedimentos, capacidade de explicação e medidas efectivas de responsabilidade. Isso pode incluir a documentação detalhada de processos de IA, tal como mecanismos para auditar e rever sistemas de IA em termos de defesa da legalidade, de garantia ética, de salvaguarda da deontologia profissional e de medição do impacto profissional, individual e social.

Capacidade e Conhecimento Regulatório

Investir na capacidade das pessoas e das equipas sobre os regulamentos de IA e de privacidade de dados. Manter-se informado sobre as tendências regulatórias globais pode ajudar as empresas a antecipar mudanças na legislação portuguesa e adaptar as suas práticas de desenvolvimento e comercialização de ferramentas de IA. Este será um desafio de inovação e de modernidade, mas também de sobrevivência e de evolução da profissão e de qualificação e capacitação dos seus agentes. É uma responsabilidade individual e colectiva a que todos e cada um teremos de responder.

Carlos Pinto de Abreu

Bruno Martins