VLK ADV

E-BOOK

AI Act

20 pontos de atenção para o Brasil

Onde o Direito
impulsiona a inovação

vlklaw.com.br

Sobre nós

O VLK Advogados entende o Direito como instrumento para impulsionar a inovação, o sucesso dos negócios e uma sociedade mais próspera e justa.

Participamos ativamente da construção de marcos regulatórios e de centenas de projetos inovadores, o que nos permite antecipar tendências e gerar segurança jurídica para viabilizar negócios nas seguintes áreas:

- Governança Ética e Proteção de Dados
- Inteligência Artificial
- Segurança Cibernética e Resposta a Incidentes
- Economia Criativa e Propriedade Intelectual
- Legal Design e Visual Law
- Contencioso Estratégico

contato@vlklaw.com.br

Este documento tem como objetivo prover informações para fins educacionais e acadêmicos. Não deve ser interpretado como aconselhamento jurídico.

Sumário

Introdução ao AI Act e sua importância Global

Aplicabilidade

Riscos da IA

Regras de Governança

Sumário

Introdução ao AI Act e sua Importância Global

1) Qual é a importância da Regulação da IA?

As aplicações de Inteligência Artificial (IA) têm sido cada vez mais utilizadas por indivíduos, empresas e entes públicos pelas suas capacidades inquestionáveis de aumentar a produtividade, gerar eficiência, contribuir para a solução de grandes desafios da humanidade e para o avanço social e econômico, tornando-se tecnologia condicionante para a competitividade de empresas e nações. Contudo, o seu ritmo de evolução exponencial é o mesmo com o qual surgem os desafios para desenvolvê-las e aplicá-las de forma ética, responsável e segura.

Daí surge a discussão acerca da importância da regulação. Por mais que cada agente implemente estratégias de governança própria, condizentes com a sua estrutura interna e seus objetivos, a regulação pode ser uma forma de garantir um mínimo de padronização.

Porém, se por um lado, a regulação pode promover ambiente de maior segurança jurídica, favorecendo o ecossistema de inovação, por outro, carga regulatória excessiva pode impedir o avanço tecnológico e o desenvolvimento dos mais diversos tipos de aplicações.

Assim, é fundamental identificar o que cada modelo regulatório implica, em termos de obsolescência normativa, burocratização temerária à inovação e custo desproporcional ao risco.

Em *ranking* que avalia o nível de investimento, inovação e implementação de IA em 62 países (Tortoise), o Brasil aparece somente na 35ª posição. O relatório aponta carência em infraestrutura, pesquisa, desenvolvimento, patentes, ambiente regulatório, estratégia governamental, talentos e negócios baseados em dados e IA.

Em outra pesquisa, publicada pela Harvard Business Review, a avaliação levou em

consideração 4 fatores principais: dados (volume e complexidade para treinamento de IA), normas (acesso a dados, políticas de governança e transferência internacional), recursos (talentos, investimentos e evolução digital) e inovação (novas técnicas e aplicações, patentes e citações acadêmicas). O Brasil ocupa a 16ª posição.

Há muitos riscos estruturantes nesse cenário, como: dependência de poucos modelos estrangeiros; aumento da desigualdade a partir da transformação digital e da adoção acelerada da IA sem qualificação e capacitação da população; fuga de talentos; e assimetria competitiva entre empresas, diante de maior ou menor fonte de recursos para investir em inovação.

Atualmente, há diferentes propostas para regular o tema globalmente: algumas se limitam a estabelecer princípios gerais; outras pretendem regular cada aplicação da IA de forma setorial; e há aquelas, como o AI Act, que se propõem a estabelecer um marco geral baseado em riscos e direitos, que abrange toda e qualquer IA, e estabelece obrigações específicas de governança de acordo com os graus de risco. Portanto, agora é o momento de entender quais requisitos o AI Act impõe às empresas, pensando no que pode servir de modelo ao Brasil.

2) O que é o AI Act?

O AI Act é uma norma robusta e prescritiva da UE que visa fomentar o desenvolvimento e a adoção segura de IA, com a proteção de direitos fundamentais e classificação dos riscos associados.

O regulamento vem sendo discutido desde 2018 e passou por muitas mudanças, desde então. As mais recentes – e talvez mais impactantes – foram as novas disposições incluídas em função do surgimento de modelos como o GPT-4 da OpenAI, que são alimentados com uma infinidade de dados, não se destinam a única finalidade e podem servir de base para a construção de novos modelos: as chamadas “IAs de Uso Geral”.

No dia 02 de fevereiro de 2024 o texto passou pela aprovação unânime dos Estados-Membro da União Europeia. Esse texto foi concluído após um mês de aperfeiçoamentos técnicos, sendo resultado ade acordo político alcançado em dezembro de 2023. O documento, resultado do consenso entre a Comissão Europeia, o Parlamento Europeu e o Conselho Europeu, com apoio de várias entidades europeias, abrange ampla gama de aspectos relacionados ao desenvolvimento e uso da tecnologia de IA. Agora, falta a sua votação em plenário aguardada para abril. A Lei entrará em vigor 20 dias após a publicação no Diário Oficial da UE. As IAs proibidas/vedadas começarão a ser aplicadas após seis meses. As obrigações de governança de acordo com os modelos de IA, após um ano. As demais regras entrarão em vigor após dois anos, exceto a classificação de sistemas de IA que têm de ser submetidos a avaliações de conformidade por terceiros, que foi adiada por mais um ano.

Os principais objetivos do AI Act são:

- Melhorar o funcionamento do mercado interno, com quadro jurídico uniforme para o desenvolvimento, a comercialização, uso e serviço de sistemas de IA na União Europeia, garantindo conformidade com valores da União e promovendo a adoção de IA confiável e centrada no ser humano.

- Assegurar alto nível de proteção da

saúde, segurança, direitos fundamentais e proteção ambiental contra efeitos prejudiciais dos sistemas de IA.

- Apoiar a inovação e prevenir a fragmentação do mercado interno devido a regras nacionais divergentes sobre IA, assegurando proteção consistente e alta em toda a União.

- Reconhecer a rápida evolução da IA e seus benefícios econômicos, ambientais e sociais, mantendo simultaneamente a segurança e minimizando os riscos e danos potenciais.

3) O AI Act se restringe à União Europeia?

O AI Act possui efeitos extraterritoriais, ou seja, se destina a entidades que operam dentro ou fora da UE, desde que seus sistemas de IA impactem o mercado ou indivíduos na UE.

Além disso, existe uma tendência de que o texto da UE sirva de modelo para a elaboração de outras legislações ao redor do mundo. Tal fenômeno de "importação" dos regulamentos europeus – o que chamamos de Efeito Bruxelas – já é de praxe nas áreas do Direito que envolvem tecnologia, e não seria a primeira vez que isso aconteceria no Brasil. Basta lembrar da LGPD, que foi aprovada 2 anos após o Regulamento Geral de Proteção de Dados (RGDP ou GDPR) da UE e que fez dele verdadeiro espelho.

4) Como o Brasil está discutindo a regulação de IA e reagindo ao AI Act?

O Brasil já discute seu marco regulatório geral para a IA com alta prioridade.

Inicialmente, foi apresentado e aprovado na Câmara dos Deputados o PL 21/2020, de abordagem principiológica.

No Senado Federal, em 2023, foi apresentado texto substitutivo ao referido Projeto, o PL 2338/23, justamente utilizando abordagem correlata ao AI Act.

Nesse sentido, o PL 2338/23 também estabelece normas para o desenvolvimento e uso responsável de sistemas de IA enfatizando a proteção dos direitos fundamentais e a implementação de sistemas seguros. O projeto reflete a priorização dos interesses sociais sobre os econômicos, impondo regras rigorosas para os desenvolvedores e aplicadores de IA, com foco na centralidade da pessoa humana e em obrigações adicionais densas para sistemas de alto risco.

Atualmente, esse Substitutivo do Senado está sendo discutido junto aos PLs anteriores por Comissão Temporária, e seguirá com os ajustes até abril de 2024, quando se prevê nova sugestão de texto e votação no Senado.

Aplicabilidade

5) O que se enquadra como sistema de IA?

Nem toda tecnologia de automação que a sua empresa utiliza é sistema de IA. Por isso, entender o conceito nos ajuda a compreender que tipo de norma será aplicável.

Simplificando, a **Inteligência Artificial** é um campo da tecnologia que faz com que computadores e máquinas emulem a inteligência humana, podendo aprender com experiências, entender e responder a linguagem, reconhecer imagens e tomar decisões complexas; **algoritmos** são um conjunto de instruções para se atingir determinados objetivos, inclusive os mais simples; e **decisões automatizadas** englobam quaisquer decisões tomadas por um computador, sem intervenção humana.

O conceito de IA adotado no AI Act se baseia no mais recente documento da OCDE, que distingue IA de sistemas de software mais simples, e inclui tecnologias como as chamadas IAs Generativas (que produzem textos, imagens, áudio etc., como o ChatGPT ou o *Midjourney*):

> *"Sistema de IA é um sistema baseado em máquina projetado para operar com diferentes níveis de autonomia e que pode exibir adaptabilidade após a implantação, e que, para objetivos explícitos ou implícitos, infere, a partir dos dados de entrada que recebe, como gerar saídas (outputs), tais como previsões, conteúdo, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais." (Art 2, 5g.(1))*
>
> VLK Adv | E-book | AI Act (UE): 20 pontos de atenção para o Brasil (Fevereiro de 2024)

Algumas características-chave dos sistemas de IA são:

- A **capacidade de inferir,** ou seja, de obter as saídas a partir dos dados de entrada, usando modelos e/ou algoritmos derivados dos dados ou do conhecimento codificado.

- A **capacidade de operar com diferentes graus de autonomia**, ou seja, de ter algum grau de independência de ações da intervenção humana e de capacidade de operar sem intervenção humana.

- A **capacidade de se adaptar** após a implantação, ou seja, de ter capacidades de autoaprendizagem, permitindo que o sistema mude enquanto está em uso.

6) O que são os modelos de IA de uso geral (GPAIs)?

Antes da definição legal, é crucial entendermos a diferença entre o sistema de IA e o modelo de IA. Em linhas gerais, um modelo individual pode servir como a base sobre a qual aplicações de IA mais especializadas – aí sim, sistemas de IA - podem ser construídas. Por esse motivo, eles são conhecidos como como **modelos de base** ou **modelos de fundação** (*foundational models*).

Outro termo para defini-los, que foi o adotado pelo AI Act, é o de **modelos de IA de uso geral** (*General Purpose AI – GPAI*), que seriam aqueles que podem ser utilizados para uma série de tarefas, o que inclui os **grandes modelos de IA generativa**.

Esses modelos precisam ser treinados com grandes quantidades de dados para aprender uma ampla gama de habilidades. Então, podem ser adaptados ou "afinados" posteriormente, em processo chamado "*fine-tuning*" - para realizar tarefas específicas em diferentes domínios, como tradução de idiomas, geração de texto, e reconhecimento de imagem. Um exemplo deles é o GPT-4, que é o modelo sobre o qual foi construído o Chat-GPT, da OpenAI.

Dentre essa categoria, o AI Act escolheu dar atenção especial a modelos de IA de uso geral de **risco sistêmico,** devido à alta potência ou à ampla utilização, adotando-se como critério objetivo a potência computacional total superior a 10^25 FLOPS – um indicador que reflete a intensidade de recursos necessários para treiná-los. Tal indicador não está lapidado em pedra: o Serviço Europeu para a IA pode revisar esse limiar de acordo com o avanço tecnológico ou mesmo em estabelecer critérios adicionais para enquadrar outros modelos nessa categoria, em casos específicos. Para tais modelos, há obrigações mais rigorosas para mitigar os seus possíveis impactos mais elevados.

7) Quem estará sujeito às regras?

O AI Act tem aplicabilidade extensiva, direcionando-se não apenas a entidades da União Europeia (UE) mas também a fornecedores e usuários internacionais de sistemas de IA, sempre que os seus produtos ou serviços sejam utilizados na UE. Esta abordagem busca evitar a evasão regulatória, para garantir que todos os sistemas de IA relevantes sejam conformes, independentemente da origem.

Fornecedores são as entidades que desenvolvem ou fazem desenvolver sistemas ou modelos de IA colocando-os no mercado ou em serviço na UE, independentemente de serem gratuitos ou pagos. Este termo abrange desde autoridades públicas até empresas privadas.

Implementadores referem-se às entidades que operam sistemas de IA sob sua gestão, excluídos os usos não profissionais e pessoais, garantindo que a

utilização de tais sistemas esteja em conformidade com o regulamento.

Representantes Autorizados são entidades na UE designadas por fornecedores fora da UE para assumir responsabilidades regulamentares em seu nome, facilitando a conformidade transfronteiriça.

Importadores levam sistemas de IA de fora da UE para o mercado interno, assumindo responsabilidade pela conformidade destes sistemas uma vez introduzidos no mercado.

Distribuidores são entidades que disponibilizam sistemas de IA no mercado da UE, atuando na cadeia de fornecimento além dos fornecedores ou importadores.

Operadores englobam todas as categorias acima, desde a criação até a distribuição e uso de sistemas de IA, assegurando uma responsabilidade compartilhada pela conformidade regulatória.

Essas definições amplas asseguram uma governança abrangente de sistemas de IA dentro e fora da UE, envolvendo todos os agentes econômicos na cadeia de valor de IA.

Riscos da IA

8) Quais riscos os sistemas de IA oferecem?

Como vimos, uma das características que define os sistemas de IA é a capacidade de gerar certos *outputs* com autonomia, sejam decisões simples, previsões complexas, imagens, entre outros. Essa capacidade intrínseca não apenas fomenta inovação e transformação em diversos setores, mas também acarreta uma série de riscos a direitos e garantias fundamentais. O AI Act define esses riscos como a combinação da probabilidade de ocorrência de um dano e a gravidade desse dano, e estabelece critérios objetivos para abordá-los de maneira sistemática.

- ***Outputs* Equivocados**: A possibilidade de que os sistemas de IA produzam resultados errôneos é mitigada por práticas que garantam a qualidade dos

dados utilizados para treinar e validar o sistema, reduzindo a probabilidade de sua ocorrência, e mecanismos de contestabilidade e supervisão humana, aptos a reduzir o seu impacto. Assim, por exemplo, uma pessoa que entende ter sido injustamente afetada por um sistema de IA pode solicitar a revisão de decisões automatizadas, promovendo a correção e a adaptação dos sistemas conforme necessário. Igualmente um supervisor de um sistema de IA que gerencia uma infraestrutura crítica pode optar por sobrepujar o sistema, quando ele apresenta mal funcionamento antes que este cause danos irreparáveis.

- ***Outputs* Ininteligíveis**: A questão dos *outputs* gerados por sistemas de IA que são difíceis de entender por humanos é enfrentada com mecanismos de transparência, como a elaboração de guias ou a inclusão, no próprio desenho do sistema, de explicações a respeito do significado de cada *output*. Estes garantem que os usuários possam compreender a decisão do sistema, evitando interpretações equivocadas ou não-desejadas.

- **Processo decisório ininteligível:** O risco de não se conseguir explicar como o sistema de IA chegou a uma determinada decisão (isto é, o que ele considerou e como considerou), dificultando o controle de legalidade dessa decisão (seja pela organização, seja pela sociedade), reduzindo a confiança das pessoas ao seu respeito ou mesmo a sua aceitação. Para mitigar esse risco, as organizações devem buscar construir sistemas explicáveis por *design*, balanceando explicabilidade e eficiência, podendo, ainda, utilizar ferramentas que lhes auxiliem a traduzir a lógica do sistema para linguagem humana.

- **Violações de Privacidade:** A proteção de dados desde a concepção e durante todo o ciclo de vida dos sistemas de IA é crucial. O AI Act enfatiza a importância de implementar mecanismos robustos de proteção de dados para salvaguardar a privacidade dos indivíduos e a segurança de informações sensíveis.

- **Vieses Discriminatórios:** A abordagem ao risco de vieses discriminatórios nos sistemas de IA exige esforços proativos para identificar, prevenir e eliminar preconceitos durante toda a fase de treinamento do sistema, desde a formação de equipes diversas e multidisciplinares de colaboradores, até a seleção e análise crítica dos dados e suas respectivas fontes. Isso inclui a adoção de limitações sistêmicas em comandos (*prompts*) que previsivelmente possam gerar *outputs* discriminatórios e, até mesmo, a supervisão contínua do sistema, enfatizando a necessidade de ajustes regulares nos algoritmos e nos conjuntos de dados.

- **Incidentes de Segurança**: O risco dos sistemas de IA como qualquer outro sistema, sofrerem violações à sua confidencialidade, integridade e disponibilidade. Com efeito já existem, inclusive, ataques especificamente voltados para a IA, como ataques adversariais e de envenenamento de dados, citados pelo próprio AI ACT. Para mitigar esses riscos, é importante que a equipe responsável pelo desenvolvimento do sistema conte com profissionais de Cibersegurança capacitados, hábeis a identificar os principais riscos a que o sistema se

encontra sujeito e guiar o time na adoção de controles de segurança eficazes.

Além disso, o AI Act também destaca riscos específicos associados aos modelos de **IA de Uso Geral** (*General Purpose AI* – GPAI), que implicam outras preocupações, como as **violações de direitos autorais** e a **disseminação de desinformação** ou de **discursos de ódio**, por exemplo.

Enfatiza-se a importância de práticas de uso justo (*fair* use) e de treinamento adequado (*fair training*) para prevenir infrações de direitos autorais, bem como o desenvolvimento responsável e a utilização ética dessas tecnologias para combater a desinformação.

Ainda, também visando preservar os direitos autorais, os fornecedores dos GPAIs devem disponibilizar relatórios explicando a base utilizada para treinar seus modelos, por exemplo, elencando os principais dados ou conjunto de dados usados para tal finalidade.

9) Como o AI Act categoriza e classifica os riscos associados aos sistemas de IA?

O AI Act define quatro níveis de risco para sistemas de IA, além de uma categoria específica para os modelos de uso geral. A identificação do risco se baseia na função e finalidade do sistema, com uma lista anexa ao regulamento detalhando aplicações de risco elevado.

- **Risco mínimo:** A maioria dos sistemas de IA se enquadra na categoria de **risco mínimo**, considerados de baixo ou nenhum risco significativo para os direitos e para a segurança dos indivíduos. Tais sistemas são isentos de obrigações regulatórias adicionais, mas podem aderir voluntariamente a códigos de conduta. Exemplos incluem sistemas de IA que fornecem recomendações de filmes ou música, assistentes virtuais para tarefas simples, e jogos de IA.

- **Risco limitado:** Sistemas classificados como de **risco limitado** são aqueles que exigem que os usuários sejam claramente informados de que estão interagindo com uma máquina. Esta categoria impõe apenas requisitos básicos de transparência. Exemplos de sistemas de risco limitado podem incluir *chatbots* de atendimento ao cliente, com os quais há um risco de manipulação, mas que não afeta significativamente os direitos fundamentais dos usuários.

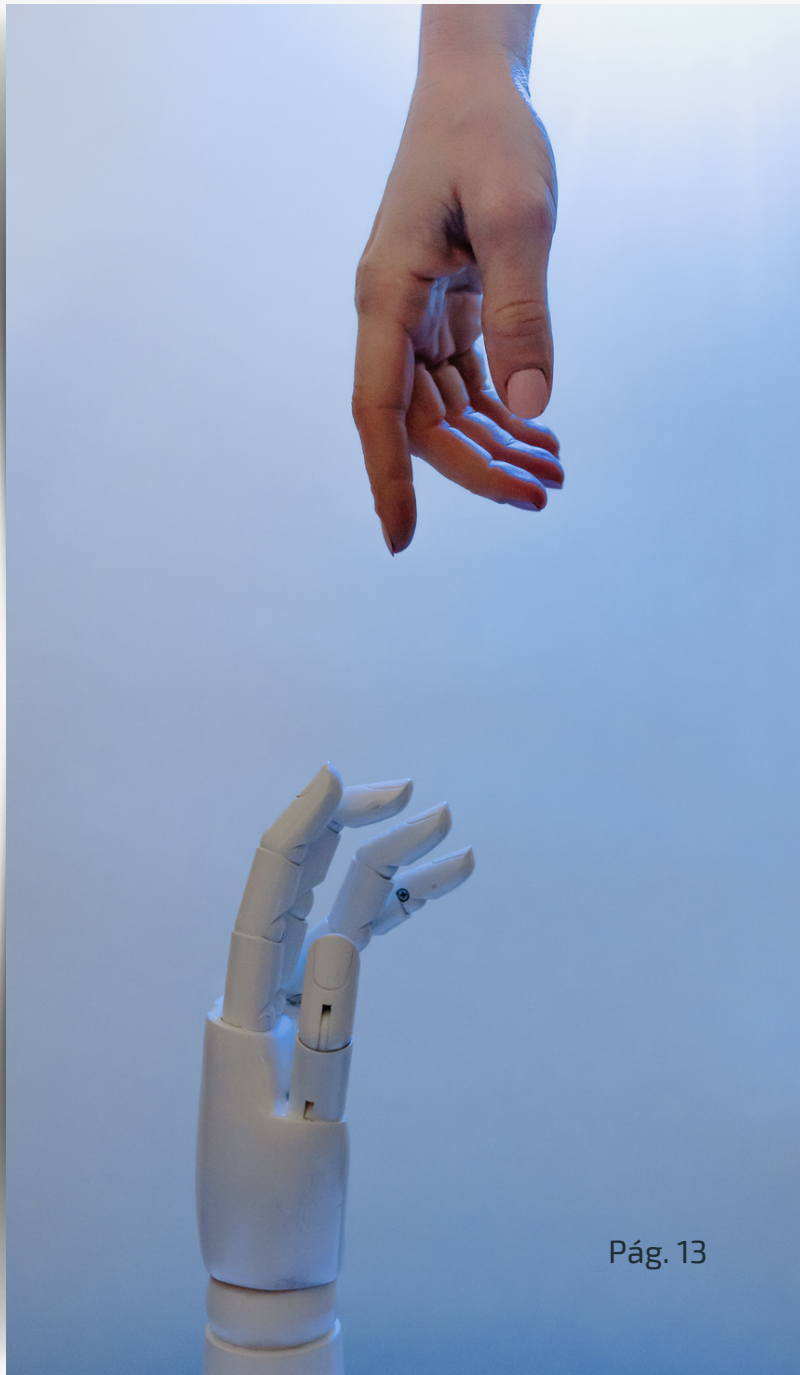
- **Risco elevado:** Já os sistemas de IA que têm um potencial impacto significativo na segurança e nos direitos fundamentais das pessoas são considerados de **risco elevado** . Para esses sistemas, o AI Act exige governança rigorosa, incluindo avaliações de conformidade antes da entrada no mercado, que abordam aspectos como a qualidade dos dados e transparência. Os fornecedores desses sistemas podem demonstrar conformidade através de adesão a códigos de conduta voluntários. Exemplos nesta categoria incluem sistemas de IA utilizados em infraestruturas críticas, processos de recrutamento e seleção de emprego, decisões educacionais, acesso a serviços essenciais como crédito e habitação, e na aplicação da lei.

- **Risco inaceitável:** Existem ainda usos de IA estritamente que **são proibidos** por violarem diretamente direitos

fundamentais: a categoria de **risco inaceitável.** Exemplos de aplicações proibidas incluem sistemas de manipulação cognitiva-comportamental que possam explorar vulnerabilidades de indivíduos, coleta indiscriminada de imagens faciais em espaços públicos, reconhecimento emocional em ambientes de trabalho ou educacionais, sistemas de classificação social que discriminam entre cidadãos, categorização biométrica remota para inferir características sensíveis, e certas formas de policiamento preditivo baseadas em perfis comportamentais ou demográficos.

- **Risco sistêmico:** Paralelamente a essas 4 categorias, certos modelos de IAs de uso geral, incluindo grandes modelos de IA generativa, ainda podem ser enquadrados na categoria de **risco sistêmico.** Esse indicador aponta para modelos que, em razão da alta potência ou da sua ampla utilização, apresentam mais chances de causar graves acidentes, violações a direitos autorais, usos abusivos para grandes ataques cibernéticos, ou ainda a propagação de informações falsas ou discursos de ódio, por exemplo.

Regras de Governança



10) Quais são as obrigações de transparência do AI Act?

As obrigações de transparência estabelecidas pelo AI Act para fornecedores e implantadores de sistemas de IA e modelos de uso geral são delineadas no Art. 52 do texto consolidado do regulamento. Estas obrigações incluem:

- **Avaliar o grau de risco do sistema**: Fornecedores devem avaliar se o sistema de IA é um sistema de risco elevado, com base nas listas constantes nos anexos II e III e, em caso de enquadramento no Anexo III, nas exceções legais apresentadas. Caso se entenda, com base nas exceções legais, que o sistema não é

de grau elevado, essa avaliação deve ser documentada e registrada na base de dados da União Europeia para Sistemas de Alto risco.

- **Transparência na Interação Direta**: Fornecedores devem garantir que sistemas de IA destinados a interagir diretamente com pessoas sejam projetados e desenvolvidos de forma que as pessoas sejam informadas de que estão interagindo com um sistema de IA. Exceto nos casos em que seja óbvio, sob a perspectiva de uma pessoa razoavelmente bem-informada e atenta, levando em consideração as circunstâncias e o contexto de uso.

- **Marcação de Conteúdo Gerado por IA**: Fornecedores de sistemas de IA, incluindo sistemas GPAI (Uso Geral) que geram conteúdo sintético de áudio, imagem, vídeo ou texto, devem assegurar que os *outputs* dos sistemas de IA sejam marcados em um formato legível por máquina e detectáveis como artificialmente gerados ou manipulados. Isso deve ser feito de forma eficaz, interoperável, robusta e confiável, dentro do que é tecnicamente viável.

- **Obrigações para Sistemas de Reconhecimento de Emoções e Categorização Biométrica**: Implementadores de sistemas de reconhecimento de emoções ou de categorização biométrica devem informar às pessoas expostas a tais sistemas sobre sua operação e tratar os dados pessoais de acordo com as regulamentações aplicáveis da UE.

- **Divulgação de Conteúdo *Deep Fake***: Implementadores de sistemas de IA que geram ou manipulam conteúdo de imagem, áudio ou vídeo que constitui um deep fake devem divulgar que o conteúdo foi artificialmente gerado ou manipulado. Essa obrigação tem exceções específicas, como quando o uso é autorizado por lei para detectar, prevenir, investigar e processar crimes, ou quando o conteúdo faz parte de um trabalho evidentemente artístico, criativo, satírico, fictício ou análogo.

Todas essas informações devem ser fornecidas às pessoas naturais interessadas de maneira clara e distinguível, no mais tardar no momento da primeira interação ou exposição, respeitando os requisitos de acessibilidade aplicáveis. Além disso, essas obrigações de transparência não afetam outros requisitos e obrigações estabelecidos no regulamento e devem ser consideradas sem prejuízo de outras obrigações de transparência para usuários de sistemas de IA previstas na lei da UE ou de cada Estado-membro.

11) Quais são as obrigações para os sistemas de IA de risco elevado?

O AI Act estabelece um **conjunto rigoroso de obrigações para os diferentes sujeitos** envolvidos nos sistemas de IA classificados como de risco elevado, com o intuito de garantir a segurança, transparência e conformidade com os direitos fundamentais. Cita-se, aqui, apenas algumas das obrigações para fins de contextualização da longa jornada de conformidade necessária.

Os sujeitos devem estabelecer um **sistema de gestão de riscos** robusto, que deve ser documentado, implementado, e mantido ao longo do ciclo de vida do sistema de IA de alto risco. Este sistema

deve incluir a identificação, análise, e avaliação dos riscos conhecidos e previsíveis, além de medidas de gestão de riscos apropriadas para endereçá-los (Art.9). Além disso, a **governança e gestão de dados** (que não se confunde com a governança de privacidade) são essenciais, exigindo que os sistemas de IA de alto risco sejam desenvolvidos com base em conjuntos de dados de treinamento, validação, e teste que cumpram critérios de qualidade específicos, abordando desde a coleta até a preparação de dados e a mitigação de vieses (Art. 10).

A avaliação detalhada do sistema de IA de alto risco deve ser **preparada antes da colocação no mercado ou da entrada em serviço**, contendo todas as informações necessárias para demonstrar a conformidade com os requisitos regulamentares, tanto por implementadores (Art. 11), quanto por importadores (Art. 26) e fornecedores (Art. 27). Isso pode incluir, entre outros, detalhes sobre o propósito pretendido do sistema, o nível de precisão, robustez, cibersegurança, e as medidas de supervisão humana implementadas.

Os sistemas de IA de alto risco devem permitir a **gravação automática de eventos** ('*logs*') ao longo de sua vida útil, para garantir a rastreabilidade do funcionamento do sistema, o que é crucial para identificar situações de risco e facilitar o monitoramento pós-mercado (Arts. 12 e 20).

Além disso, é imperativo assegurar a **transparência e fornecer informações** aos implementadores, para que possam interpretar corretamente os *outputs* do sistema e utilizá-los de maneira adequada. As instruções de uso devem conter informações claras, concisas, e completas sobre as capacidades, limitações de desempenho, e medidas de supervisão humana do sistema (Art. 13).

A **supervisão humana** é enfatizada como um requisito fundamental, garantindo que os sistemas de IA de alto risco sejam efetivamente supervisionados por pessoas naturais durante o uso, com medidas proporcionais ao nível de risco, autonomia, e contexto de uso do sistema de IA (Art. 14).

Finalmente, os sistemas devem ser projetados e desenvolvidos para atingir um nível apropriado de **precisão, robustez e cibersegurança**, funcionando de forma consistente em todos esses aspectos ao longo de seu ciclo de vida (Art.15).

Além disso, destacam-se as disposições a respeito da **cooperação com autoridades** por todos os sujeitos envolvidos (Arts. 23, 25 (2)c, 26 (5)a), 29). As autoridades de fiscalização monitorarão a conformidade, realizando auditorias e permitindo que fornecedores comuniquem incidentes graves ou violações de direitos fundamentais. E em caso de infração, as autoridades nacionais poderão acessar informações necessárias para investigar a legalidade do uso de sistemas de IA.

Empresas que adotam sistemas de IA de alto risco e que, estejam sujeitas ao regulamento, precisam estar cientes das obrigações detalhadas no AI Act, garantindo que os sistemas em suas operações estejam em total conformidade, seja diante do desenvolvimento adequado, ou da escolha cuidadosa de sistemas que já tenham sido avaliados e atestados quanto à conformidade com esses requisitos rigorosos.

12) O que é uma Avaliação de Impacto sobre Direitos Fundamentais?

A Avaliação de Impacto sobre Direitos Fundamentais é exigida de entidades que implantam sistemas de IA de risco elevado e, além disso, sejam organismos de direito público ou operadores privados que prestam serviços públicos, ou operadores que implantam sistemas de análise de crédito (exceto para detecção de fraude) ou utilizados para avaliação de riscos e precificação de seguro de vida e de saúde. A avaliação detalha o uso previsto do sistema, identifica as populações afetadas e os riscos potenciais aos direitos fundamentais, devendo os resultados serem notificados à autoridade nacional competente. Quando uma Avaliação de Impacto sobre a Proteção de Dados já foi realizada, a avaliação sobre direitos fundamentais deve ser integrada a ela, assegurando uma análise compreensiva dos impactos da implementação de sistemas de IA.

No Brasil, o PL 2338 possui uma previsão equivalente: após a avaliação preliminar que determinaria o grau de risco do sistema (art. 13), os sistemas que considerados como de alto risco notificariam a autoridade competente do resultado dela, e então procederiam a uma avaliação de impacto algorítmico (AIA), nos ditames dos arts. 22 a 24 do regulamento e das determinações da autoridade competente. A AIA seria realizada por um profissional ou conjunto de profissionais com a devida qualificação e com independência funcional, seguindo as etapas mínimas de: (i) preparação; (ii) cognição do risco; (iii) mitigação dos riscos encontrados; e (iv) monitoramento. Ela consistiria em um processo iterativo contínuo ao longo de todo o ciclo de vida dos sistemas, com atualizações periódicas; e com as conclusões sendo públicas, garantidos os segredos industrial e comercial.

13) Quais são as regras para as IAs de Uso Geral?

No AI Act, fornecedores de modelos de IA de uso geral, ou seja, que possam ser utilizados por uma série de tarefas, incluindo os grandes modelos de IA generativa, devem seguir diretrizes específicas, incluindo a divulgação de informações sobre o treinamento e o respeito à legislação de direitos autorais.

O regulamento exige que esses fornecedores cumpram requisitos de transparência, com o compartilhamento de informações específicas com os demais fornecedores na cadeia de suprimentos, aumentando a transparência e entendimento dos modelos. especialmente aqueles que, por sua potência ou uso extenso, apresentam riscos sistêmicos. Ainda, também visando preservar os direitos autorais, os fornecedores dos GPAIs devem disponibilizar relatórios explicando a base utilizada para treinar seus modelos, por exemplo, elencando os principais dados ou conjunto de dados usados para tal finalidade, especialmente aqueles que, por sua potência ou uso extenso, apresentam riscos sistêmicos.

14) Quais são as regras adicionais para as IAs de Uso Geral de Risco Sistêmico?

As IAs de Uso Geral de Risco Sistêmico, categoria das IAs de Uso Geral, estão sujeitas a requisitos adicionais, devido ao seu potencial impacto mais significativo. Fornecedores desses modelos são obrigados a: executar uma avaliação do modelo, de acordo com protocolos e ferramentas padronizadas que reflitam a melhor prática existente; elaborar

documentação de testes adversariais, para identificar e mitigar riscos; avaliar e mitigar possíveis riscos sistêmicos a nível da União Europeia, que possam resultar de sua colocação no mercado; reportar incidentes graves; realizar testes, garantir cibersegurança; e informar sobre o consumo de energia dos modelos.

O AI Act encoraja os fornecedores a colaborarem com o Serviço Europeu da Inteligência Artificial na criação de códigos de conduta junto a peritos, com a supervisão de um painel científico.

Tendo em vista a rigidez, tais regras certamente trarão discussões a respeito das interpretações de soberania nacional em relação aos segredos de negócio de empresas internacionais e a aplicação extraterritorial do AI Act.

15) E no Brasil, como o PL 2338 aborda essas questões de classificação e obrigações?

O Projeto de Lei nº 2338/23 no Brasil propõe uma abordagem mais rigorosa em comparação ao AI Act europeu no que diz respeito às obrigações de governança para sistemas de inteligência artificial.

De início, uma característica distintiva do PL 2338 é a exigência de uma **avaliação preliminar** para determinar o grau de risco de **qualquer** sistema de IA antes do seu uso e da colocação em mercado. Ou seja, mesmo um sistema de finalidade mais simples, que não se enquadre no rol exemplificativo dos sistemas de alto risco, deve passar por essa avaliação.

Além disso, enquanto os sistemas de risco mínimo do AI Act não enfrentam obrigações significativas de governança, os sistemas de baixo risco do PL 2338 estão sujeitos a uma carga de obrigações gerais bastante onerosas.

Não bastasse, a categoria de alto risco no PL 2338 engloba tanto o que o AI Act entende como risco limitado quanto como risco elevado, ou seja, não há uma categoria intermediária limitada a obrigações de transparência. Mais do que isso, as obrigações exigidas dos sistemas de baixo risco no projeto brasileiro já vão muito além das obrigações de transparência do AI Act. Logo, todos os sistemas de IA que circulassem no Brasil teriam mais restrições do que os sistemas no segundo nível de risco na Europa.

Por fim, o PL 2338 **exige Avaliações de Impacto Algorítmico (AIA)** e **supervisão humana** para sistemas considerados de alto risco, reforçando a necessidade de uma análise criteriosa e medidas de controle para mitigar possíveis impactos negativos.

Essas exigências sublinham o enfoque excessivamente rigoroso do Brasil nas questões de governança de IA, impondo que mesmo sistemas de IA de baixo risco estejam sujeitos a requisitos regulatórios mais estritos do que os estabelecidos pelo projeto europeu para sistemas de risco limitado. Teme-se que essas regras desmedidas, em vez de proteger os direitos fundamentais dos cidadãos, acabe por privá-los dos benefícios sociais advindos da IA, uma vez que inviabilizariam qualquer avanço tecnológico no país, dado o ambiente regulatório hostil aos empreendimentos.

Autoridades e Sanções

16) Quem regulará a IA na União Europeia?

Na União Europeia, a regulação da inteligência artificial será supervisionada tanto pelos Estados-Membros quanto por uma estrutura centralizada da UE, chamada "Serviço Europeu para a Inteligência Artificial" ou "Serviço IA" (*AI Office*).

Cada Estado-Membro designará autoridades nacionais para supervisionar a aplicação do regulamento e realizar a fiscalização do mercado. Os Estados-Membros devem assegurar que suas autoridades tenham recursos adequados (Art. 59(4)). Autoridades de vigilância do mercado são obrigadas a notificar sobre incidentes graves (Art. 9) e cumprir com o Regulamento 2019/1020. Cada Estado-Membro deve designar autoridades notificadoras e de vigilância do mercado independentes e imparciais (Art. 59), promovendo uma aplicação harmonizada e eficaz das regras de IA.

Além disso, será designada uma autoridade nacional de controle para representar cada país no Comitê Europeu para a Inteligência Artificial, que trabalhará em conjunto com um novo Serviço Europeu da Inteligência Artificial, criado para supervisionar especificamente os modelos de IA de uso geral e facilitar a aplicação harmonizada do regulamento em toda a UE. Este arranjo visa garantir uma aplicação eficaz, consistente e transparente das novas regras de IA, e envolve uma ampla gama de stakeholders e promovendo a colaboração internacional.

As empresas também podem influenciar as regras relacionadas à IA na União Europeia participando no Fórum Consultivo, que é composto por membros da indústria, startups, PMEs, sociedade civil e academia. O fórum serve para fornecer conhecimento técnico e consultoria tanto à Comissão Europeia quanto ao Conselho Europeu de Inteligência Artificial, ajudando na implementação eficaz da regulamentação

a partir de uma representação diversificada de interesses comerciais e não comerciais. Quais são as possíveis consequências para as empresas que descumprirem as regras?

No Brasil, o PL 2338/23 prevê uma autoridade competente, a ser designada pelo Poder Executivo, para zelar pela implementação e fiscalização da Lei que dispõe sobre IA. A ANPD tem se posicionado publicamente como a autoridade competente a ser designada para exercer a função de órgão regulador central, tendo em vista pontos de intersecção entre o PL nº 2338/2023 e a LGPD (a tutela de direitos, a abordagem regulatória baseada em riscos, os mecanismos de governança, os comunicados de incidentes e a coordenação com outros órgãos e autoridades) e experiências internacionais.

17) Quais são as possíveis consequências para as empresas que descumprirem as regras?

As empresas que violarem o AI Act enfrentarão multas significativas, cujos valores variam de acordo com a natureza da infração. Infrações graves, como em decorrência de práticas proibidas ou falhas nos requisitos de dados, podem resultar em multas de até 35 milhões de euros ou 7% do faturamento global anual, o que for maior. Outras violações podem levar a multas de até 15 milhões de euros ou 3% do faturamento global.

Há também disposições para compensar indivíduos afetados, permitindo-lhes buscar indenizações por danos causados por sistemas de IA de alto risco. A Diretiva Responsabilidade da IA propõe medidas para facilitar a compensação por danos causados por sistemas de IA, enfatizando a responsabilidade e a transparência no uso da IA.

Impactos Regulatórios

18) Como o AI Act pretende estimular a inovação e o desenvolvimento de IA nas empresas?

O AI Act visa estimular a inovação e o desenvolvimento de IA nas empresas ao criar um ambiente regulatório que aumenta a confiança dos usuários e harmoniza as regras, facilitando o acesso a mercados maiores. A confiança gerada pela conformidade com o regulamento encoraja a adoção de IA por empresas e autoridades públicas, enquanto a segurança jurídica e a simplificação dos processos regulatórios minimizam os encargos para os operadores econômicos. Além disso, o regulamento incentiva a experimentação responsável, permitindo testes em condições reais de sistemas de IA de risco elevado por até 12 meses, com supervisão adequada e consentimento dos usuários, assegurando que os efeitos dos testes sejam reversíveis e que a proteção de dados seja garantida.

Adicionalmente, o AI Act fomenta a criação de ambientes de *sandboxes* regulatórios, que consistem em testagens regulatória e de testes no mundo real, oferecendo às empresas, incluindo PMEs e startups, a oportunidade de testar inovações tecnológicas em um ambiente controlado, sob o cumprimento do regulamento.

Essa abordagem é reforçada por iniciativas como redes de centros de excelência em IA e parcerias público-privadas, que promovem a colaboração entre os setores e facilitam o acesso a infraestruturas de inovação digital e instalações de teste. Essas medidas coletivas criam condições favoráveis para que as empresas desenvolvam e implementem soluções de IA, impulsionando a excelência e a confiança no ecossistema europeu de IA.

No Brasil, o PL 2338 também prevê a possibilidade de *sandboxes* e recentemente a ANPD abriu uma consulta pública sobre o estudo a respeito da criação de *sandboxes* de IA e proteção de dados no Brasil. A iniciativa é fruto de colaboração com o Banco de

Desenvolvimento da América Latina e do Caribe (CAF) e prevê o aumento da transparência algorítmica e o fomento à inovação responsável em IA.

Sandboxes já são largamente utilizados no setor financeiro e parecem ser um caminho viável para que autoridades reguladoras participem do desenvolvimento de novos negócios de forma segura, sem barrar a inovação, em uma experimentação colaborativa entre o regulador e o agente regulado, por meio de uma metodologia estruturada.

19) Quais são os custos de conformidade estimados para as empresas na União Europeia?

Em Relatório de Avaliação de Impacto sobre a regulação de IA publicado pela Comissão Europeia, em 2021, empresas ou autoridades públicas teriam o custo total agregado da conformidade estimado entre € 100 milhões e € 500 milhões até 2025, representando até 4-5% do investimento em IA de alto risco. Além disso, os custos de verificação poderiam atingir entre 2% e 5% do investimento em IA de alto risco.

Para as empresas ou autoridades públicas envolvidas com aplicativos de IA não classificados como de alto risco, nenhum custo seria imposto, embora elas pudessem optar por aderir a códigos de conduta voluntários, cujos custos seriam, no máximo, comparáveis aos de aplicativos de alto risco.

Os impactos sobre as PMEs e a competitividade foram destacados no Relatório, considerando que PMEs poderiam se beneficiar de um nível mais alto de confiança nos sistemas de IA, mas aquelas que desenvolvem aplicativos de alto risco enfrentariam custos semelhantes aos das grandes empresas.

Tais estudos foram feitos antes das GPAIs e não necessariamente refletem a situação econômica atual das empresas europeias, e tão pouco o cenário brasileiro, mas podem ser um ponto de partida, assim como os custos de governança com LGPD e cibersegurança pelas empresas.

20) Como as empresas brasileiras podem se preparar para possíveis mudanças legislativas, considerando o AI Act?

Governança, princípios, políticas, ferramentas, processos e cultura para desenvolver, implantar ou utilizar sistemas de IA de forma segura, confiável, lícita, ética e para o bem dos indivíduos e da sociedade, ao mesmo tempo em que gera impacto empresarial transformador, independem de legislação específica.

É essencial focar em programas de governança para a conformidade com as regras existentes e ponderar as futuras. Isso envolve avaliar os modelos já desenvolvidos de governança em Proteção de Dados e Cibersegurança, e práticas de IA responsável, incluindo mapeamento dos usos de IA e finalidades, protocolos de monitoramento e adesão aos padrões de boas práticas de mercado (ISO, NIST, IEEE, AIGA, HAI, AI Act e PL 2.338/23).

A elaboração de matriz de risco dinâmica, de acordo com os seguintes critérios, ajuda a identificá-los e mitigá-los: Segurança Cibernética e Proteção de dados; Violação de direitos de terceiros (no input e output); Data Loss Prevention; Direito de exploração do conteúdo gerado; Qualidade e precisão do conteúdo no output; Vieses discriminatórios; Ausência de transparência; Explicabilidade; e Continuidade dos negócios.

Além disso, uma boa governança, implica

no desenvolvimento melhor e mais eficiente das organizações. A Gartner prevê que até 2026 as organizações que operacionalizarem IA de forma ética e responsável verão seus modelos alcançarem melhoria de 50% nos resultados de negócios e na aceitação do usuário.

Em outros termos, o avanço do uso de modelos de IA imputa às organizações novos desafios principiológicos, que extrapolam a conformidade legal. É crítico adequar a cultura corporativa ao inédito ambiente de negócio caracterizado por agilidade, volatilidade e tecnologias complexas.

Para identificar oportunidades e responsabilidades, é crucial também contemplar nos conselhos de inovação e/ou conselhos de ética perspectivas heterogêneas de pensamento, construindo condições favoráveis para a colaboração entre as ciências exatas e as ciências humanas.

Considerações finais

No Brasil, não deveria haver urgência normativa, especialmente diante do risco de obsolescência regulatória e do impacto nocivo à inovação. Ainda, de acordo com o uso de IA, já há legislação aplicável, como o Código Civil, Código de Defesa do Consumidor, Lei Geral de Proteção de Dados e Marco Civil da Internet, além da própria Constituição Federal.

Enquanto o mundo discute o melhor modelo regulatório, nós não precisamos servir de cobaia. Podemos observar as mais variadas alternativas e seus impactos em outros países para depois avaliar a tropicalização do modelo mais adequado.

Fato é que, assim como a eletricidade e a internet, a IA é uma tecnologia de propósito geral que está em pleno e constante desenvolvimento. Eventual regulação, assim, deve ser suficientemente flexível e adaptável às suas rápidas mudanças e usos,

permitindo experimentação, inovação e evolução contínua dos sistemas de IA. A abordagem principiológica e menos prescritiva do Marco Civil da Internet (2014), por exemplo, é reconhecida no mundo inteiro como um ótimo modelo regulatório.

É plausível que sejam traçados parâmetros gerais para avaliação de risco no uso da IA para que a sua definição, no âmbito normativo, se dê de maneira contextual, bem como se privilegie balizas de governança em alto nível, deixando a análise fática para o caso concreto e o entendimento dos órgãos reguladores setoriais. O sucesso da regulação de um objeto em constante transformação depende da combinação de *soft law* com flexibilidade regulatória. Fora isso, esses parâmetros mínimos podem orientar a autorregulação e o desenvolvimento de códigos de conduta para diferentes setores de atividade econômica, podendo ser reconhecidos posteriormente pelos órgãos e autoridades públicas setoriais competentes.

Reino Unido, Japão, Cingapura e Austrália optaram por uma abordagem cautelosa na governança de IA, buscando preservar a inovação e a competitividade por meio de múltiplos instrumentos.

Nos EUA, o Presidente Joe Biden recentemente assinou ordem executiva, estabelecendo políticas públicas e diretrizes de IA para as agências federais. Ou seja, uma abordagem regulatória setorial, que pode ser objeto de estudo pelo Brasil.

Os membros do G7, grupo das maiores economias do mundo, acolheram favoravelmente princípios orientadores internacionais na matéria e um código de conduta voluntário para os criadores de IA.

A ONU, no início de novembro, instalou órgão consultivo, com 38 membros, com o objetivo de propor diretrizes para governança da IA, e, eventualmente, uma agência global. O Brasil está ali muito bem representado, com a secretária de Direitos Digitais do Ministério da Justiça, Estela Aranha.

Uma das principais características da economia digital é que suas cadeias de valor são inerentemente dinâmicas e globalizadas. É de grande relevância que o Brasil tenha participação ativa e voz nesses fóruns internacionais para a discussão das melhores práticas e de uma governança global da IA, em especial para que tenhamos convergência em termos de padrões e regulações.

Existe consenso entre os *stakeholders* sobre a necessidade de regulação, mas as discussões sobre o momento (*pacing problem*) e abordagem regulatória adequada ainda estão incipientes no país. Importar legislações estrangeiras sem considerar a realidade brasileira não parece ser a solução. Precisamos de muita cautela, letramento sobre como funcionam os novos negócios digitais e análise prévia de impacto regulatório antes da aprovação de qualquer marco regulatório da IA no Brasil. A prioridade deveria ser um plano de nação para qualificar mão de obra, com recursos e infraestrutura para criar ecossistemas em torno da capacidade humana, além de diminuir a barreira de entrada para pequenas e médias empresas. O nosso intelecto e a IA devem coexistir em sua máxima potência, se quisermos participar e atuar da vibrante e próspera economia digital, protagonizada pela IA.

Como regular IA? Não nos precipitando.

Conheça nossos autores

Rony Vainzof
Sócio-fundador

Caio Lima
Sócio-fundador

Alexandra Lopes
Advogada

Jean Santana
Advogado

Mateus Lamonica
Estagiário

Onde o Direito impulsiona a inovação

FICHA TÉCNICA:

E-book AI Act (UE): 20 pontos de atenção para o Brasil, Edição 1 de 07 fevereiro de 2024

Para mais informações ou para questões relacionadas à publicação, entre em contato conosco atráves do e-mail contato@vlklaw.com.br.

Produção Gráfica:
Jennifer Santos

vlklaw.com.br