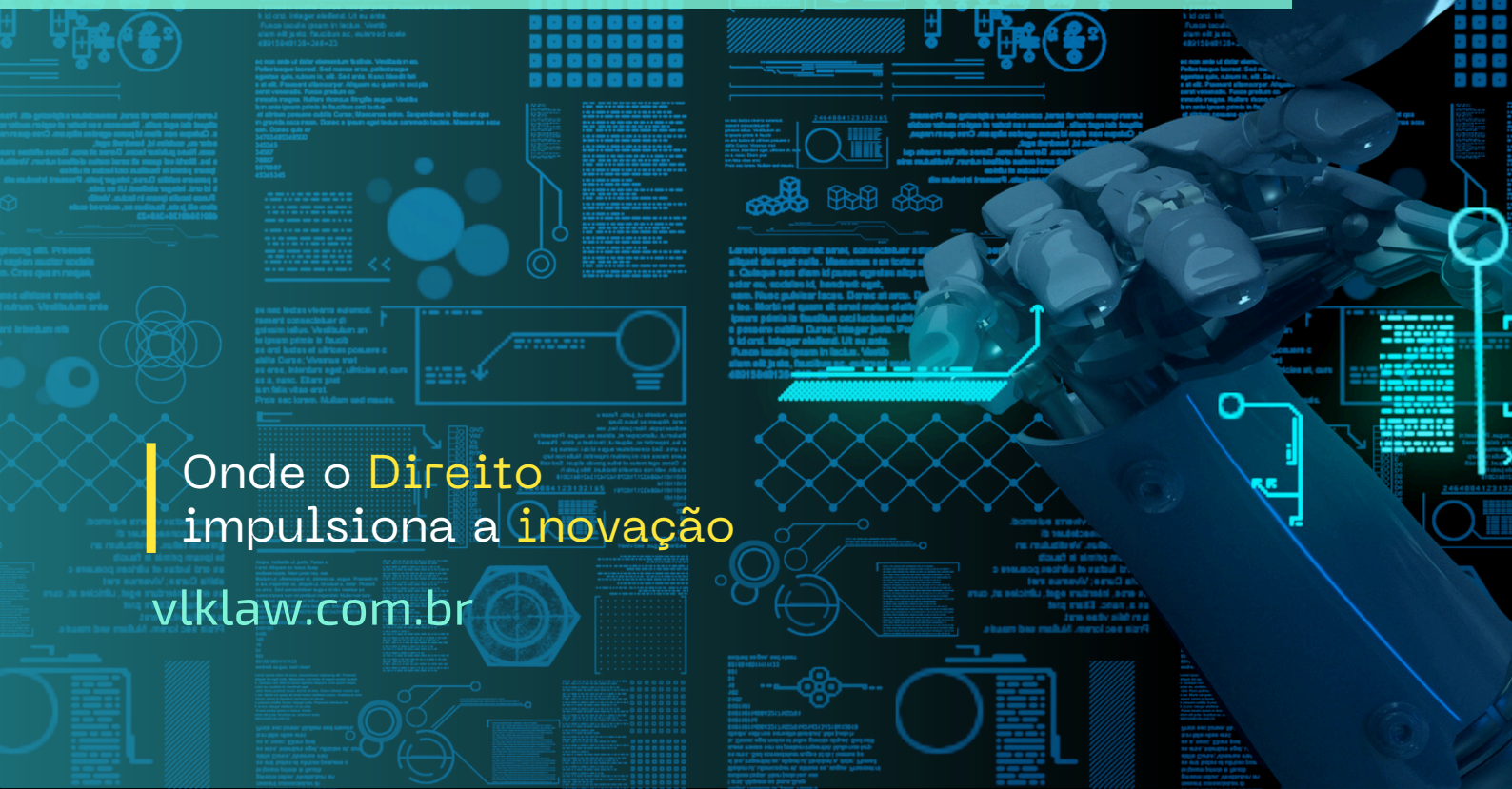
VLK ADV

E-BOOK | **2ª EDIÇÃO**

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.

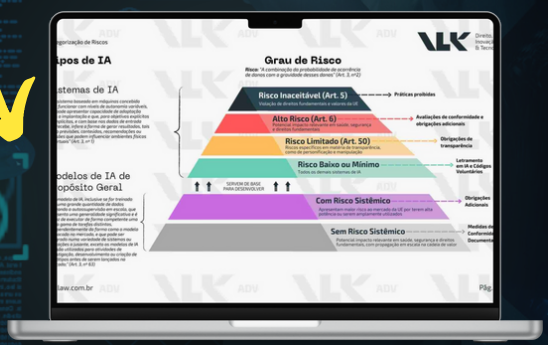
Participamos ativamente da construção de marcos regulatórios e de centenas de projetos inovadores, o que nos permite antecipar tendências e gerar segurança jurídica para viabilizar negócios nas seguintes áreas:

- 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.

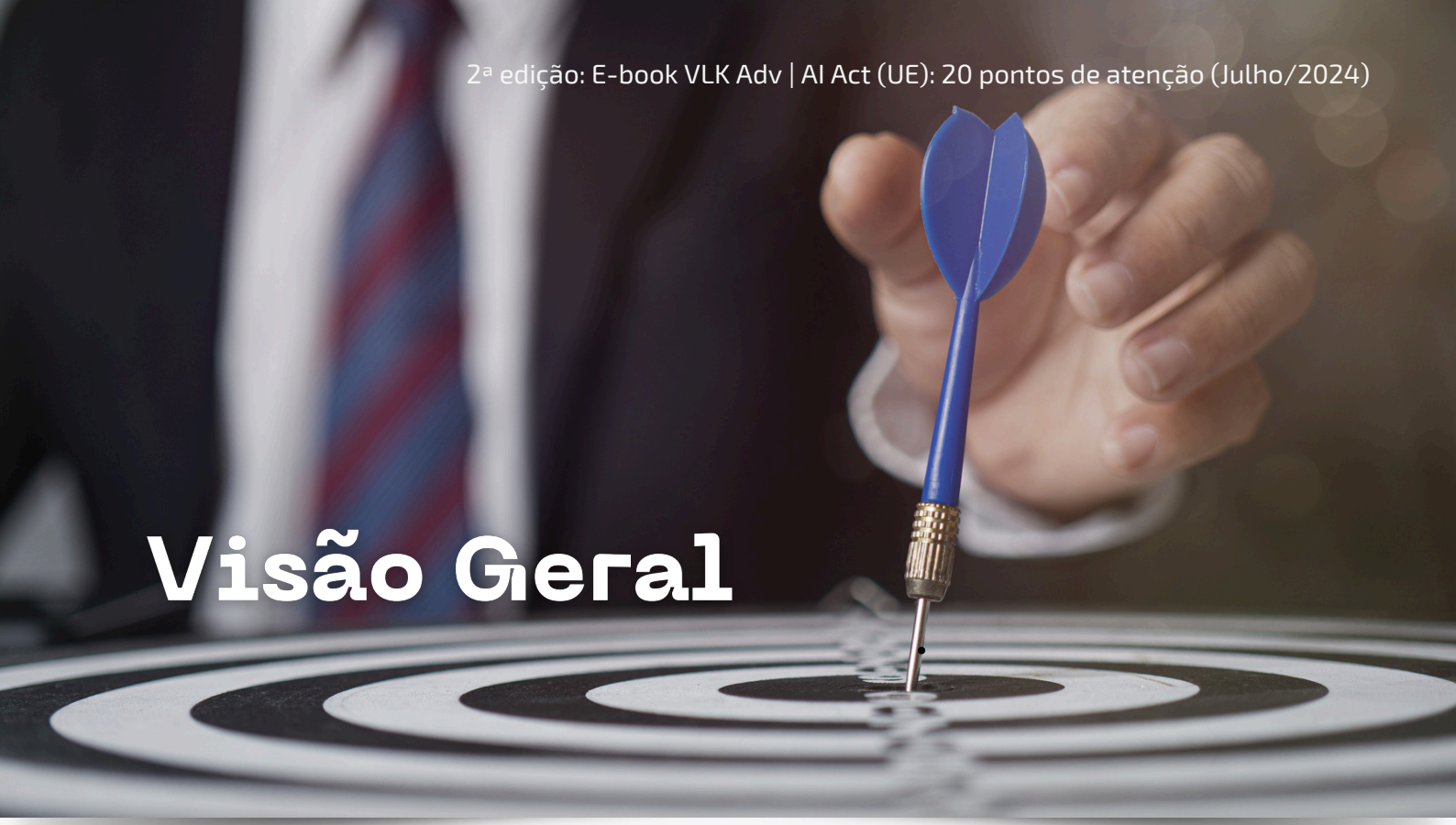
MATERIAL INÉDITO!
Clique aqui para fazer o download.



2ª edição: E-book VLK Adv | AI Act (UE): 20 pontos de atenção (Julho/2024)

Sumário

Sumário



Visão Geral

I - Disposições Gerais (Arts. 1 a 4)

- Objeto;
- Âmbito de Aplicação da Lei;
- Definições;
- Letramento em IA.

II - Prática de IA proibidas (Art. 5)

Sistemas de IA de Risco Inaceitável.

III - SISTEMAS DE IA DE ALTO RISCO (Arts. 6 a 49)

- Classificação, Requisitos e Obrigações Associadas aos Sistemas de IA de Alto Risco;
- Autoridades Notificadoras e Organismos Notificados;
- Normas, Avaliação da Conformidade, Certificados, Registro.

IV - OBRIGAÇÕES DE TRANSPARÊNCIA (Art. 50)

Obrigações de transparência para fornecedores e usuários de certos sistemas de IA e modelos de GPAI.

V - MEDIDAS DE APOIO À INOVAÇÃO (Arts. 57 a 63)

- Regras, Modalidades e funcionamento de *sandboxes* regulatórios de IA;
- Processamento adicional de dados pessoais para sistemas de IA de interesse público;
- Teste de sistemas de IA de alto risco em condições reais fora dos *sandboxes*;
- Medidas para fornecedores e implementadores, em particular PMEs e *startups*;
- Derrogações para operadores específicos (Art. 55a).

VI – GOVERNANÇA PÚBLICA (Arts. 64 a 70)

Papéis de Conselho Europeu de IA, Painel Científico de Especialistas Independentes e Autoridades Nacionais Competentes.

VII - BASE DE DADOS DA UE PARA SISTEMAS DE IA DE ALTO RISCO LISTADOS NO ANEXO III (Art. 71)

- Base de dados da UE, Monitoramento Pós-Mercado e Supervisão;
- Compartilhamento de Informações sobre Incidentes Graves;
- Regras para Fornecedores de GPAI.

VIII - MODELOS DE IA DE PROPÓSITO GERAL (Arts. 51 a 56)

- Regras de Classificação de Modelos de IA de Propósito Geral ("GPAI") e de GPAIs com risco sistêmico;
- Procedimentos e Obrigações para Fornecedores dos Modelos;
- Representante autorizado;
- Códigos de práticas.

IX – ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO, COMPARTILHAMENTO DE INFORMAÇÕES, FISCALIZAÇÃO DO MERCADO (Arts. 72 a 94)

X - CÓDIGOS DE CONDUTA E ORIENTAÇÕES (Arts. 95 e 96)

- Modelo e incentivos a códigos de conduta voluntários.

XI – DELEGAÇÃO DE PODERES E PROCEDIMENTO DE COMITÊ (Arts. 97 e 98)

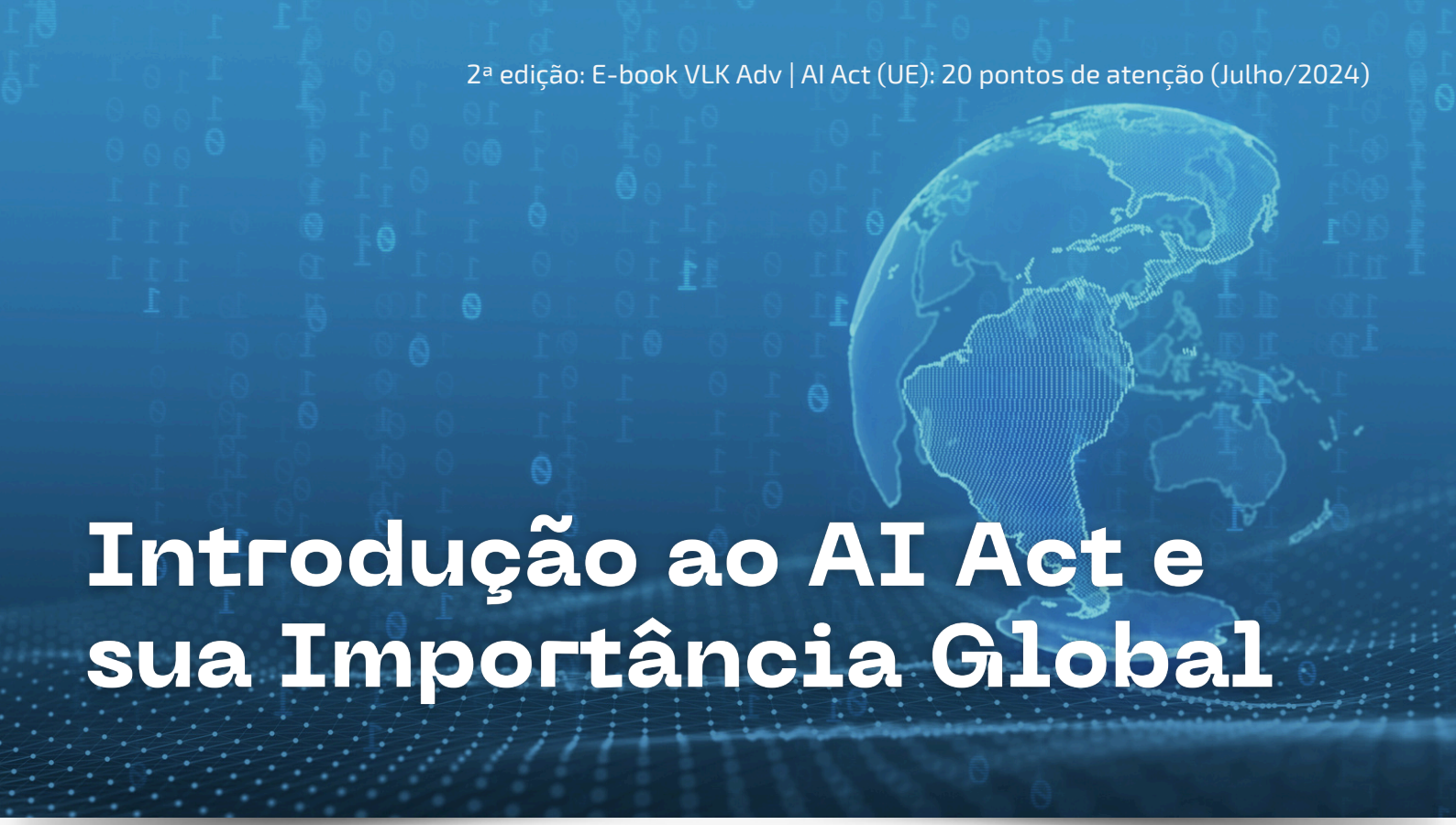
- Regras de Confidencialidade;
- Multas administrativas em entes da União;
- Multas para fornecedores de GPAIs;
- Exercício da delegação e Procedimento de comitê.

XII - SANÇÕES (Arts. 99 a 101)

- Exercício da delegação e Procedimento de comitê.

XIII - DISPOSIÇÕES FINAIS (Arts. 102 a 113)

- Atualizações de Regulamentos e Diretivas da UE e Diretrizes da Comissão sobre a implementação;
- Sistemas de IA já colocados no mercado ou postos em serviço;
- Avaliação e revisão;
- Entrada em vigor e aplicação.



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, uma 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.

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, 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 são os requisitos do AI Act e como as empresas, inclusive as brasileiras, podem ser afetadas, , e pensar 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 Propósito Geral”.

Em 13 de março de 2024 o Parlamento Europeu tornou pública a última versão do AI Act, **o qual foi publicado no diário oficial em 12/07/24**. O texto, resultado do consenso entre a Comissão Europeia, o Parlamento Europeu e o Conselho da UE, com apoio de várias entidades europeias, abrange ampla gama de aspectos relacionados ao desenvolvimento e uso da tecnologia de IA. Aprovado pelo Parlamento Europeu em março e pelo Conselho da EU em maio de 2024, o regulamento será publicado no Diário Oficial da Eu e entrará em vigor após 20 dias, porém sua aplicação se dará em fases (Art. 113).

A proibição das IAs vedadas começa a ser aplicável após seis meses. As obrigações de governança serão exigíveis 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 (Art. 113).

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 (Art. 2), 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. Mais especificamente, o regulamento é aplicável a fornecedores ou implantadores de sistemas de IA, desde que haja previsão de que os resultados (outputs) produzidos pelos sistemas sejam utilizados na União Europeia (Art. 2, 1, c, c/c Considerando nº 22).

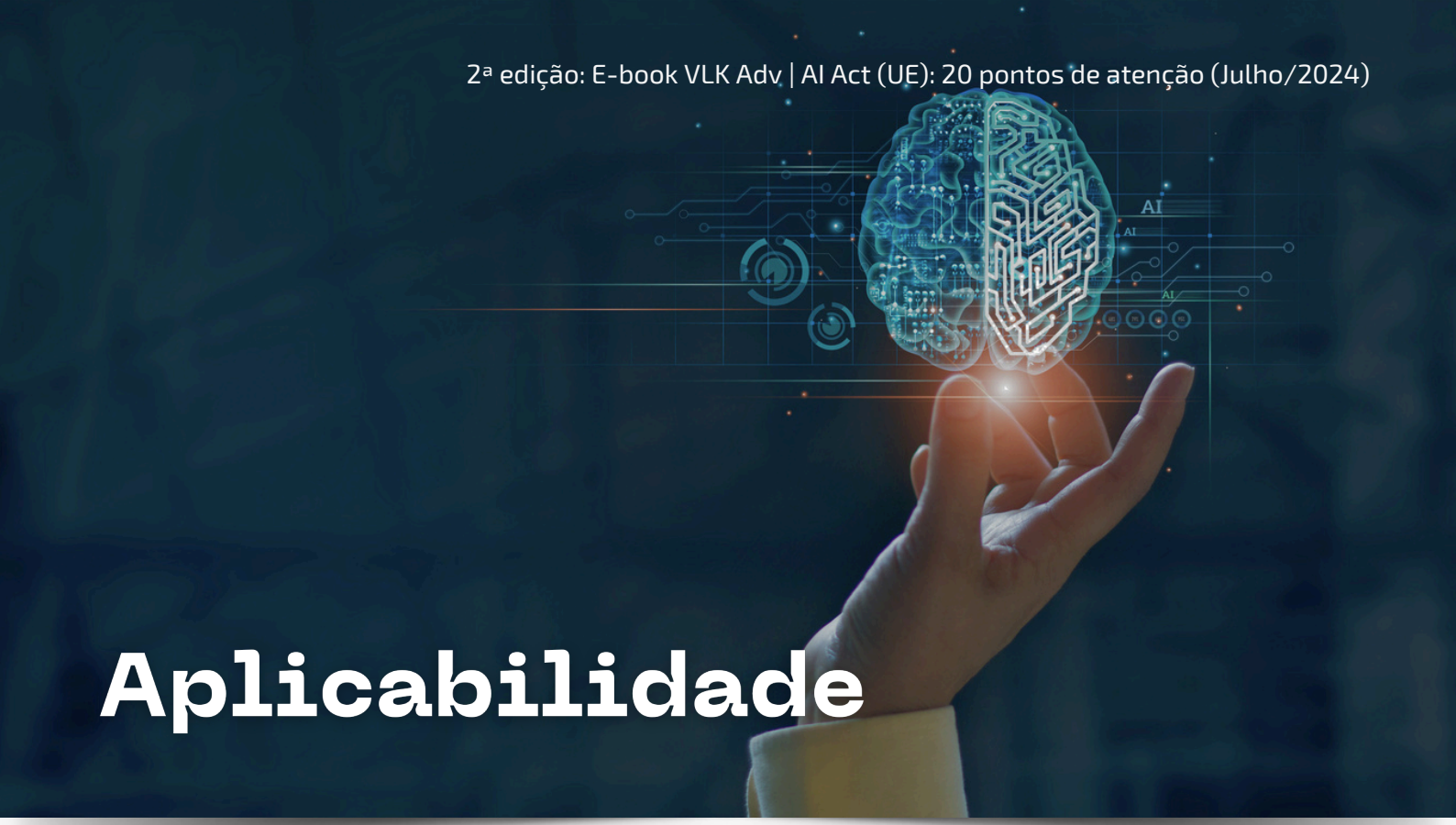
Além disso, existe uma tendência de que o texto da UE sirva de modelo para a elaboração de outras legislações ao redor do mundo. Tal fenômeno de "importação" dos regulamentos europeus – o que chamamos de Efeito Bruxelas – já é de praxe nas áreas do Direito que envolvem tecnologia, e não seria a primeira 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.

Em 2023, foi apresentado, no Senado Federal, texto substitutivo ao referido Projeto, o PL 2338/23, justamente com abordagem correlata ao AI Act, prescrevendo uma ampla gama de normas para o desenvolvimento e uso responsável de sistemas de IA e enfatizando a proteção dos direitos dos indivíduos afetados.

Atualmente, uma Comissão Temporária no Senado discute esses e vários outros Projetos de Lei que foram apresentados nos últimos anos nas duas casas legislativas. Contudo, a abordagem regulatória que será adotada no Brasil segue em aberto, sendo objeto de amplo debate entre entes legislativos, autoridades regulatórias e representantes de todas as esferas da sociedade brasileira.



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 sejam capazes de agir ou pensar de forma racional, ou próxima à humana , podendo aprender com experiências, entender e responder a linguagem, reconhecer imagens e tomar decisões complexas; **algoritmos** são um conjunto de instruções para se executar uma tarefa, inclusive as 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", um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais;" (Art. 3, 1)*
> 2ª edição: E-book VLK Adv | AI Act (UE): 20 pontos de atenção (Maio/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 algum grau 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. É importante destacar que existem alguns sistemas de inteligência artificial que **não são regulados pelo AI ACT,** destacando-se sistemas:

É importante destacar que existem alguns sistemas de inteligência artificial que **não são regulados pelo AI ACT,** destacando-se sistemas:

- Utilizados exclusivamente para **fins militares, de defesa ou de segurança nacional** (Art. 2, 3);

- Destinados ao **uso por países terceiros e organismos internacionais** para fins de cooperação internacional ou de acordos internacionais para efeitos de **cooperação policial e judiciária** (Art. 2, 4);

- Utilizados exclusivamente para fins de **investigação e desenvolvimento científicos** (Art. 2,6);

- Que **estejam em etapa de investigação, testagem ou desenvolvimento,** desde que não sejam colocados em mercado ou serviço, e a **testagem não seja feita em condições reais** (Art. 2, 8);

- Empregados para **fins exclusivamente pessoais,** quando utilizados por pessoa física, **no que diz respeito às obrigações dos Implantadores** (Art. 2, 10);

- Sistemas de IA de **licença gratuita e de código aberto,** ressalvados os sistemas caracterizados como proibidos, de risco elevado, ou de risco limitado (Art. 2,12).

6) O que são os modelos de IA de Propósito 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 finais de IA– aí sim, sistemas de IA - podem ser construídas. Por esse motivo, eles são conhecidos como **modelos de base** ou **modelos de fundação** (*foundational models*). Os modelos de IA podem ser alterados ou aperfeiçoados em novos modelos, mas, para se tornarem sistemas de IA, é necessário adicionar outros componentes, como uma interface de usuário, por exemplo. Além disso, podem ser integrados em sistemas de IA por meio de APIs, bibliotecas, download direto e cópias físicas (Considerando 97).

A nível de modelos, o AI Act optou por regular apenas aqueles que possuem apresentam *generalidade significativa* e que têm competência para *executar uma vasta gama de tarefas variadas:* os **modelos de IA de propósito geral** (*General AI – GPAI*) (art. 3°, 63), o que inclui os **grandes modelos de IA generativa** (Considerando 99).Sem prejuízo de outros critérios, serão considerados modelos de IA de propósito geral aqueles que, cumulativamente: *(i)* tenha, pelo menos, um bilhão de parâmetros; *(ii)* tenha sido treinado com grande volume de dados utilizando a auto supervisão em escala; e *(iii)* executam com competência uma vasta

gama de tarefas (Considerando 98).

Esses modelos precisam ser treinados com grandes quantidades de dados para aprender uma ampla gama de habilidades. Então, podem ser adaptados ou "refinados" 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* e o *Copilot* da Microsoft, entre tantos outros sistemas.

Dentre essa categoria, o AI Act escolheu dar atenção especial a modelos de IA de Propósito 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 (Art. 51, 1) – 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 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 está 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. De acordo com o Art. 3º:

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

Implantadores referem-se às pessoas físicas ou jurídicas que utilizam sistemas de IA sob sua autoridade, excluídos os usos não profissionais e pessoais, garantindo que a utilização de tais sistemas esteja em conformidade com o regulamento.

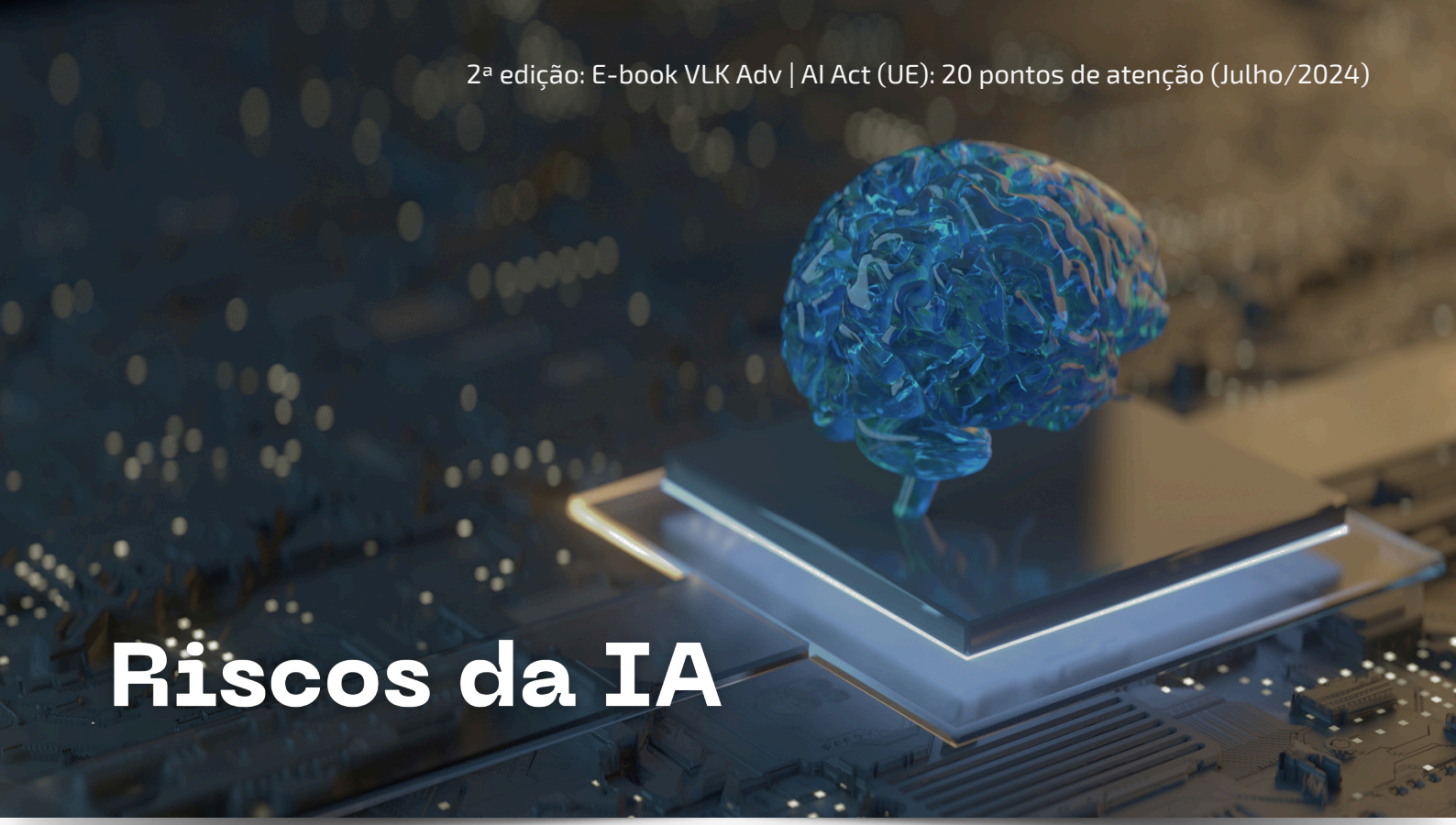
Mandatários são entidades na UE designadas por fornecedores fora da UE para assumir responsabilidades regulamentares em seu nome, bem como certas obrigações próprias, facilitando a conformidade transfronteiriça.

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, mas não se enquadram como fornecedores ou importadores.

Operadores englobam todas as categorias acima, além dos **fabricantes de produtos** que integrem sistemas de IA, 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 (Art. 3º, 2), e estabelece critérios objetivos para abordá-los de maneira sistemática. Abaixo apresentaremos alguns riscos aos direitos e liberdades fundamentais comumente presentes na literatura especializada, cuja adoção medidas mitigatórias entendemos recomendável:

- ***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 assumir o controle do 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 (art. 13), como a elaboração de guias ou a inclusão, no próprio desenho do

sistema (isto é, na jornada do usuário), 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, ressaltando a aplicação do Regulamento Geral de Proteção de Dados ao tratamento de dados pessoais no contexto de sistemas de inteligência artificial (Art. 2, 7).

- **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 (Art. 15, 4). Essas medidas podem incluir a formação de equipes diversas e multidisciplinares de colaboradores (considerando 165 e Art. 95, 2, d), até, como sugere o AI Act, a seleção e análise crítica dos dados e suas respectivas fontes, garantindo que estes sejam acurados, pertinentes e representativos (Art. 10). 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:** Há 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 (Art. 15, 5). 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 Propósito 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.

Nesse sentido o AI ACT, prevê, dentre

outros: *(i)* obrigações específicas de transparência para sistemas que geram conteúdos sintéticos, como a marcação desses conteúdos como tais em formato legível por máquina e detectável (Art. 50, 2); *(ii)* obrigação de adoção de uma política de conformidade com normas de direitos autorais (Art. 53,1, c); e *(iii)* o dever de publicar relatórios suficientemente pormenorizados sobre os conteúdos utilizados para treinamento dos sistemas (Art. 53, 1, d).

Enfatiza-se, por fim, 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 – na União Europeia essas práticas serão reguladas, sobretudo, pelo Art. 4, da Diretiva 2019/790, que trata da mineração de dados para "qualquer propósito".

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

O **AI Act identifica o risco a partir da função e finalidade do sistema,** com duas listas anexas ao regulamento detalhando aplicações de alto risco. A maioria dos sistemas de IA está isenta 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. A esses sistemas isentos de obrigações legais específicas, a literatura especializada usualmente nomeia de "baixo risco" ou de "risco mínimo" – embora o termo não tenha sido incluído na versão final do texto.

Os riscos apresentados na última versão do AI Act são:

- **Risco limitado (Art. 50):** Sistemas classificados como de **risco limitado** são aqueles que estão sujeitos a obrigações específicas de transparência, como sistemas destinados a interagir com o usuário, sistemas que geram conteúdos sintéticos, sistemas que gere *deep fakes* ou que reconheçam emoções. As obrigações específicas de transparência variam de acordo com a categoria de sistema, no entanto, doutrinariamente são comumente enquadrados na categoria de risco limitado.

- **Alto risco (Art. 6º):** Já os sistemas de IA que têm um potencial impacto significativo na segurança e nos direitos fundamentais das pessoas são considerados de **alto risco.** Para esses sistemas, o AI Act exige uma série de medidas de governança rigorosas, incluindo avaliações de conformidade antes da entrada no mercado e o registro desses sistemas em uma base de dados europeia, 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.

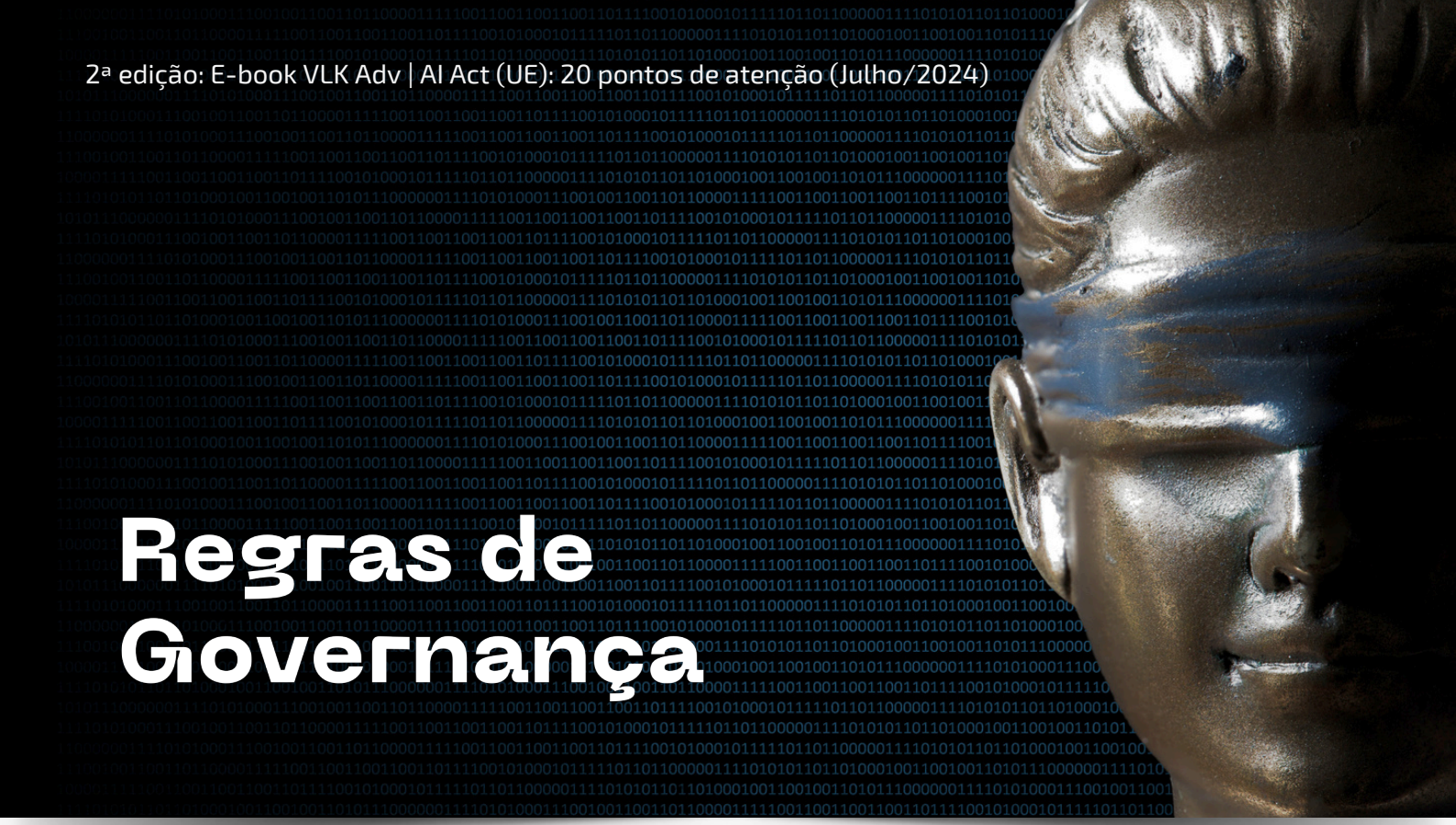
- **Risco inaceitável (Art. 5º):** Existem ainda usos de IA estritamente que são proibidos por violarem diretamente direitos fundamentais e valores da

União: 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.

- **Modelos de IA de Propósito Geral (Art. 3, 63):** são os modelos descritos no item 6 deste documento. Sobre eles recaem uma série de obrigações de governança, como o dever de elaborar e manter documentação técnica do modelo, incluindo o seu processo de treino e testagem nos termos do anexo XI, elaborar e manter documentação que suporte a integração do modelo de IA a outros sistemas de IA, adotar a política de conformidade com a legislação europeia de direitos autorais e fornecer ao público relatório com o conteúdo utilizado para o treinamento dos sistemas.

- **Modelos de IA de Propósito Geral com risco sistêmico (Art. 51):** São modelos de propósito geral 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. Pressupõem-se como enquadrados nessa categoria aqueles modelos de propósito geral potência computacional total superior a 10^25 FLOPS. São aplicáveis a esses modelos, além das obrigações aplicáveis aos modelos de IA de Propósito Geral, uma série de obrigações de governança específicas, como a necessidade de proceder uma avaliação de conformidade, adotar medidas de gestão de eventuais riscos sistêmicos, comunicar ao Serviço para IA e demais Autoridades Competentes incidentes graves, e ter níveis apropriados de cibersegurança.

É importante destacar que as categorias de riscos não são necessariamente excludentes, isto é, é possível que um sistema se enquadre em mais de uma das categorias de risco apresentadas acima – por exemplo, um sistema de IA que realiza entrevistas e toma decisões em um processo seletivo será, a um só tempo, um sistema de alto risco e risco limitado, devendo atender às obrigações aplicáveis a ambas as categorias de risco.



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 propósito 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 alto risco, 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 (Propósito 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 alto risco?

O AI Act estabelece um **conjunto rigoroso de obrigações para os diferentes sujeitos** envolvidos nos sistemas de IA classificados como de alto risco, 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 alto risco e, além disso, sejam organismos de direito público ou operadores privados que prestam serviços públicos, ou operadores que implementam 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 contexto brasileiro, algumas propostas legislativas têm incluído previsões para avaliações de impacto que são semelhantes em objetivo, embora possam variar nos detalhes específicos. Por exemplo, após uma avaliação preliminar que determinaria o grau de risco do sistema, os sistemas considerados de alto risco procederiam a uma Avaliação de Impacto Algorítmico (AIA). Realizada por

profissionais qualificados e independentes, a AIA seguiria etapas rigorosas de análise e mitigação de riscos, e seria concebida como um procedimento contínuo que acompanha o ciclo de vida completo dos sistemas, com atualizações periódicas e parâmetros delimitados pelas autoridades competentes.

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

No AI Act, fornecedores de modelos de IA de propósito 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 Propósito Geral de Risco Sistêmico?

As IAs de Propósito Geral de Risco Sistêmico, categoria das IAs de Propósito 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 as propostas legislativas têm abordado essas questões de classificação e obrigações?

As propostas legislativas no Brasil têm abordado as questões de classificação e obrigações para sistemas de inteligência artificial com diversas abordagens. Embora não haja um texto definitivo aprovado e muitos pontos sigam em aberto, as discussões recentes têm refletido uma tendência para uma governança mais rigorosa comparativamente ao AI Act europeu.

Dentre os aspectos comuns nas propostas

em maior evidência, como o PL 2338/23 e seu substitutivo apresentado em abril, uma característica distintiva 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 mais simples, que não se enquadre no rol exemplificativo dos sistemas de alto risco, deveria passar por essa avaliação, diferentemente do que ocorre na lei europeia.

Além disso, enquanto os sistemas de risco mínimo do AI Act não enfrentam obrigações significativas de governança, as propostas brasileiras tendem a impor uma carga de obrigações gerais bastante onerosas para os sistemas considerados de baixo risco. Notadamente, a categorização de risco no contexto brasileiro engloba o que no AI Act é considerado como risco limitado até alto risco, sem categorias intermediárias restritas apenas a obrigações de transparência.

Por fim, um ponto que aparece com força é a **exigência de 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.

Essa discussão legislativa está em aberto e sujeita a mudanças conforme novos projetos sejam apresentados e o debate público evolua. As propostas finais que serão adotadas ainda estão por ser definidas, indicando um cenário dinâmico e em constante adaptação às novas realidades tecnológicas e suas implicações sociais.

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 propósito 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, envolve uma ampla gama de stakeholders e promove 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 Comitê Europeu de Inteligência Artificial, ajudando na implementação eficaz da regulamentação a partir de uma

representação diversificada de interesses comerciais e não comerciais.

No Brasil, a autoridade competente para a regulação e governança da inteligência artificial ainda está sendo definida. Houve propostas como a do PL 2338, que sugeria que uma única autoridade fosse designada pelo poder executivo para tratar exercer a função de órgão regulador central. A Autoridade Nacional de Proteção de Dados (ANPD) demonstra interesse em assumir esse papel, devido à sua experiência em proteção de dados e práticas relacionadas. Em contraste, sugestões mais recentes favorecem a criação de um órgão especializado dentro da administração pública federal, com o objetivo de coordenar e articular esforços entre várias autoridades de diferentes setores.

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

As empresas que violarem o AI Act enfrentarão multas significativas (Art. 99), 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 endereçar a compensação de indivíduos afetados. O texto faz referência a aplicabilidade de Diretivas já existentes na União Europeia sobre o tema, a exemplo da Diretiva sobre Responsabilidade por Produtos. (85/374/EEC). Adicionalmente, a proposta de diretiva sobre a adaptação das regras de responsabilidade civil extracontratual à inteligência artificial publicada pela Comissão Europeia 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 alto risco 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 (Art. 57), que consistem em testagens regulatórias 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, tem aparecido com força a proposta de implementar *sandboxes*, tendo a ANPD aberto uma consulta pública sobre o estudo a respeito da criação de *sandboxes* de IA e proteção de dados no país. 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) 1.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) 1.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 geram impacto empresarial transformador, independem de legislação específica.

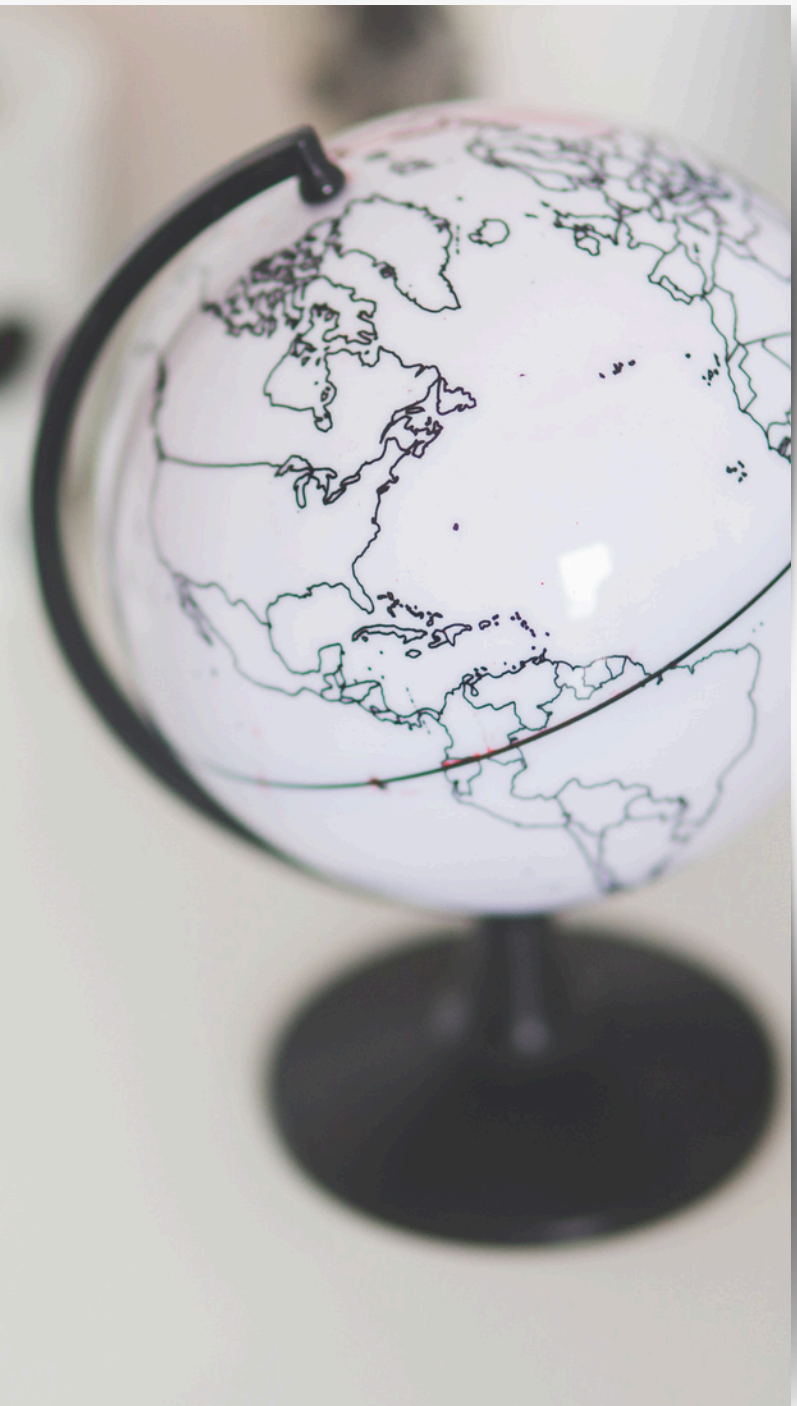
É essencial focar em programas de governança para a conformidade com as regras existentes e ponderar as futuras. Isso envolve avaliar os modelos já desenvolvidos de governança em Proteção de Dados e Cibersegurança, e práticas de IA responsável, incluindo mapeamento dos usos de IA e finalidades, protocolos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

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 melhor e mais eficiente desenvolvimento 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.



Panorama Internacional UE AI Act

Neste anexo, apresentamos um breve resumo das abordagens adotadas para a IA nos 5 países que lideram o ranking de adoção da IA da Tortoise – Global AI Index, de 28/06/20231 (em ordem): Estados Unidos da América, China, Singapura, Reino Unido e Canadá. Para referência, o Brasil se encontra na 35ª posição deste ranking, atrás de países como República Tcheca e Malta, porém à frente de toda a América Latina.

Nos EUA, a estratégia de IA inicialmente focava em iniciativas principiológicas, como a Ordem Executiva de 2019 para manter a liderança americana em IA e a estratégia de IA do Departamento de Defesa. Avanços significativos foram feitos com a publicação do Blueprint for an AI Bill of Rights pelo OSTP em 2022, que trouxe cinco princípios não vinculantes para o uso ético da IA. Além disso, o NIST publicou em 2023 um

framework que é referência para a governança de IA e a avaliação de riscos.

Há uma crescente resistência ao uso de tecnologia de reconhecimento facial, exemplificada pela proibição de São Francisco em 2019. Além disso, o advento de grandes modelos de linguagem como o ChatGPT, bem como a preocupação crescente com temas como privacidade ou *deepfakes* no contexto eleitoral, impulsionaram diversas iniciativas regulatórias em âmbito federal, estadual e municipal ao longo de 2023.

Dado o contexto do cenário jurídico-regulatório fragmentado no país, a principal iniciativa para estabelecer padrões para o uso federal de IA foi promulgada: a Ordem Executiva para o Desenvolvimento e Uso (*executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*) do presidente Biden, de outubro de 2023. Ela visa promover a equidade, proteger consumidores e trabalhadores, e reforçar a posição de liderança global dos EUA em inovação em IA, colaborando com outras nações para assegurar o uso seguro e confiável da IA, com base em padrões internacionais e na promoção do desenvolvimento responsável de IA para enfrentar desafios globais.

Na China, a Administração do Ciberespaço divulgou em 11/04/2023 um projeto de regulamentação para os Serviços de IA Generativa, com o objetivo de assegurar que o conteúdo gerado por IA esteja alinhado com os valores sociais e morais, além de prevenir discriminação, garantir precisão e respeitar os direitos de propriedade intelectual.

Além disso, o plano nacional da China para a Inteligência Artificial tem como objetivo tornar o país líder global nesse campo até 2025. Para alcançar essa meta, o país está focado em resolver desafios existentes, como a escassez de chips, equipamentos avançados, software e pessoal capacitado. A estratégia também envolve fortalecer as colaborações entre empresas privadas, instituições de pesquisa e militares, promovendo o desenvolvimento conjunto da IA. Além disso, o governo chinês pretende orientar o desenvolvimento da IA por meio de políticas, regulamentações e avaliações de segurança, bem como fortalecer as capacidades de controle dessa tecnologia.

A criação de um marco regulatório para a IA não está nos planos de **Singapura**, que prefere fortalecer a sua Estratégia Nacional de IA, iniciada em 2019 e atualizada ao final de 2023. Em vez de uma abordagem regulatória rígida, o país promove a autorregulação no setor privado por meio de recursos como o Modelo de *Framework* de Governança de IA voluntário de 2020 e o *Framework* específico para IA Generativa de 2023, além de um guia de implementação para organizações, uma ferramenta de verificação e uma coletânea de casos de uso para orientar a governança corporativa.

Em 04/03/2024, Singapura publicou diretrizes sobre o uso de dados pessoais em sistemas de IA para fornecer certeza às organizações e proteger os consumidores. Elas também abordam obrigações e melhores práticas sob a Lei de Proteção de Dados Pessoais (PDPA).

Com a aspiração de ser um líder global em áreas de IA que sejam economicamente impactantes e sirvam ao bem público, o país quer promover uma IA que atenda às necessidades e desafios do nosso tempo, ser um grande equalizador e capacitar as

pessoas e os negócios. Para tanto, Singapura realizará 15 ações estratégicas, com um investimento superior a USD 740 M nos próximos 5 anos.

O Reino Unido está adotando uma abordagem equilibrada e inovadora, delineada em março de 2023 em um documento de estratégia apresentado a Secretária de Estado Britânica para Ciência, Inovação e Tecnologia, Michelle Donelan, com a intenção de transformar o Reino Unido em uma liderança global no campo da IA.

Em vez de estatutos específicos, o Reino Unido adota uma abordagem principiológica, visando à aplicação flexível e adaptável dos regulamentos existentes para garantir que a IA seja desenvolvida e utilizada de maneira segura e ética. Os cinco princípios orientadores fundamentais são a segurança, robustez, transparência, justiça e governança.

A implementação dessa abordagem foi confiada aos reguladores setoriais existentes de acordo com os seus respectivos domínios.

Embora atualmente não existam planos para transformar esses princípios em lei, o governo reconhece a possibilidade de futuras legislações serem necessárias, especialmente no caso dos modelos de IA de Propósito Geral (GPAI).

O Canadá possui um projeto de lei para a IA em tramitação avançada, o *Artificial Intelligence and Data Act* (AIDA), que é uma seção do projeto de lei Bill C-27, prosseguiu para a segunda leitura na Câmara dos Comuns em abril de 2023.

O AIDA possui uma abordagem baseada em riscos e visa regular o comércio internacional e interprovincial com sistemas de IA a partir de requisitos comuns para a projeção, o desenvolvimento e o uso desses sistemas; além da proibição de determinadas condutas relacionadas a sistemas de IA que possam resultar em danos graves a indivíduos ou a seus interesses.

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.

Diversos países como Reino Unido, Japão,

Singapura 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. E em março de 2024, publicou uma resolução global liderada pelos Estados Unidos, para a promoção do desenvolvimento seguro e confiável da IA, com o consenso de mais de 120 países. Destaca-se a importância da proteção dos direitos humanos em todas as fases da IA e sua integração com os Objetivos de Desenvolvimento Sustentável. A resolução também apela à criação de estruturas regulatórias para garantir a segurança da IA e promove esforços para reduzir a divisão digital e garantir acesso inclusivo e equitativo às tecnologias de IA.

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 brasileiros 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.

Recentemente, em reunião do Conselho Nacional de Ciência e Tecnologia, o presidente Lula solicitou a formulação de um plano nacional para a utilização da inteligência artificial até junho, visando apresentá-lo na próxima Assembleia Geral das Nações Unidas, em setembro de 2024.

Por fim, reiteramos nosso entendimento sobre qual deve ser a prioridade do Brasil, a de um plano de nação para qualificar mão de obra, com recursos e infraestrutura para criar ecossistemas em torno da literacia em IA, ou seja, a capacidade humana das pessoas entenderem, avaliarem criticamente e utilizarem de forma eficaz e ética a IA, 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 Krastins
Advogada

Jean Santana
Advogado

Mateus Lamonica
Estagiário

Nuria Baxauli
Advogada

Onde o Direito
impulsiona a inovação

FICHA TÉCNICA:

E-book AI Act (UE): 20 pontos de atenção para o Brasil, Edição 2 de 12 de julho 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

Direito,
Inovação
& Tecnologia