cd:// conselho digital

NOTA DE TEMA

Inteligência Artificial: Regulação Baseada em Risco e Ciclo de Vida

Como o mundo tem regulamentado sistemas de inteligência artificial

ABRIL / 2026

Sobre o Conselho Digital

O Conselho Digital é uma entidade brasileira, sem fins lucrativos ou afiliações políticas, que coordena, estuda e representa o ecossistema dos aplicativos de internet e toda a diversidade dos seus modelos de negócios.

Nossa organização acredita que a tecnologia, quando bem construída e utilizada, é uma porta para o futuro. Ela nos mantém conectados, potencializa habilidades, desenvolve novas oportunidades e pode mudar a vida das pessoas para melhor.

Partindo dessa premissa, atuamos através de estudos, eventos e atividades de advocacy em favor de políticas públicas e setoriais que fortaleçam uma internet livre, segura e responsável no Brasil e no mundo.

Defendemos políticas que respeitem a neutralidade tecnológica, a inovação e a diversidade de modelos de negócios; e que tenham como consequência:

- Usuários conscientes e com poder de escolha;
- Uma sociedade plural e próspera;
- Ambientes de negócio juridicamente seguros;
- Mercados abertos e dinâmicos; e
- Empresas responsáveis e competitivas.

Por fim, assumimos o compromisso de construir um ambiente harmonioso e produtivo entre nossos associados, assim como uma relação transparente e colaborativa com a sociedade e governo.

Diretor-Executivo
www.conselhodigital.org.br

Takeaways – Posição do Conselho Digital

- **O risco em sistemas de inteligência artificial manifesta-se principalmente na aplicação concreta e no contexto de uso**, embora determinados sistemas possam apresentar riscos sistêmicos já na fase de desenvolvimento. Por isso, a regulação deve distinguir entre deveres aplicáveis ao desenvolvimento do sistema e obrigações associadas ao seu uso específico.
- **A classificação de risco deve ocorrer preferencialmente quando a finalidade e o contexto de uso estiverem suficientemente definidos**, podendo ser revista ao longo do ciclo de vida do sistema conforme novas informações se tornem disponíveis.
- **O desenvolvimento de IA exige deveres gerais de diligência e transparência**, focados em riscos sistêmicos, sem impor restrições desproporcionais à inovação.
- **A lei deve definir o núcleo da regulação**: categorias de risco, critérios de classificação e consequências jurídicas associadas a cada nível.
- **A regulamentação infralegal deve exercer papel complementar**, voltado à concretização técnica e setorial dos critérios definidos em lei, preservando segurança jurídica e previsibilidade regulatória.
- **A adaptação regulatória não pode significar expansão discricionária do escopo legal**: o regulador deve permanecer vinculado às categorias e finalidades estabelecidas pelo legislador.
- **A classificação de risco deve se basear em parâmetros objetivos**, focados na gravidade do dano.
- **Orientações regulatórias e mecanismos de revisão são essenciais** para garantir proporcionalidade, previsibilidade e evitar obsolescência normativa.
- **Responsabilidade acompanha controle**: as obrigações devem recair sobre quem controla o contexto de uso e tem capacidade real de mitigar riscos.

- **Deveres por papel na cadeia**:
  - **Integrador**: responder por customização, configuração, testes e compatibilidade com o contexto específico.
  - **Usuário institucional/deployer**: responder pelo impacto concreto, decisão automatizada no contexto, supervisão humana, avaliação de impacto, transparência aos afetados e mecanismos de contestação.

Qual a posição do Conselho Digital?

- **Como regular a inteligência artificial:** A Inteligência Artificial é uma **tecnologia de propósito geral**, aplicável a múltiplos setores econômicos e sociais, cujos impactos variam significativamente conforme o **contexto de uso**, a finalidade e o grau de autonomia decisória do sistema. Um sistema de inteligência artificial que recomenda músicas ou evita spam não tem o mesmo impacto que um sistema de IA que decide concessão de crédito ou acesso a benefícios públicos. Por isso, **o modelo mais apropriado para regular a inteligência artificial é o modelo de regulação baseado em risco**.

- **Regulação baseada em risco:** A regulação baseada em risco é um modelo regulatório em que as obrigações impostas variam conforme o **potencial de dano associado a determinada atividade ou sistema**. Em vez de regular toda tecnologia da mesma forma, o foco recai sobre a **probabilidade e a gravidade de impactos negativos**. Quanto maior o risco, maior a intensidade das exigências. Esse modelo busca proporcionalidade e eficiência regulatória.

- **Um mesmo Sistema de IA pode ter aplicações com diferentes riscos:** Assim como um martelo (ferramenta / tecnologia) pode ser usado para pendurar um quadro na parede ou quebrar uma vitrine de uma loja, um mesmo sistema de IA pode ser utilizado para finalidades completamente distintas. **Um mesmo sistema de inteligência artificial** (ferramenta / tecnologia) **pode gerar níveis de risco distintos conforme a finalidade e o contexto de uso**.

- **Sistemas de IA são contextuais e a regulação também deve ser:** É **o contexto de uso que determina o nível de risco envolvido na aplicação de IA**. Por exemplo: um sistema de IA de biometria facial pode ser usado para desbloquear o celular de um usuário (baixo

risco) ou para vigilância em massa em espaços públicos com impactos sobre direitos fundamentais (alto risco).

- **Regular o risco da Aplicação, não a Tecnologia em Abstrato:** Quando regulamos uma ferramenta, devemos regular o seu uso de alto risco e não a tecnologia em si. A regulação deve priorizar os riscos associados à aplicação concreta dos sistemas de inteligência artificial, sem prejuízo de deveres gerais aplicáveis ao desenvolvimento quando existirem riscos sistêmicos previsíveis. Por exemplo: o uso do martelo para vandalismo é crime; o uso do martelo para reforma doméstica não. Da mesma forma é com a inteligência artificial. Uma boa regulação de IA não exigiria o mesmo grau de proteção para a biometria aplicada ao desbloqueio de celular e a biometria aplicada à vigilância em massa.

I - Gestão Baseada em Risco

- **Como definir o que é arriscado ou não?** Reconhecer que a regulação deve ser baseada em risco - e focada no *alto risco* - é apenas o primeiro passo. A questão central é como cada sistema jurídico identifica esse risco e operacionaliza o risco em obrigações regulatórias concretas.
    - Alguns modelos definem previamente quais aplicações são consideradas de alto risco e impõem obrigações específicas para cada categoria; outros utilizam critérios mais abertos e permitem que a avaliação seja feita caso a caso; outros ainda tratam o risco como um parâmetro contínuo de governança.
    - Assim, a diferença entre os regimes não está em regular ou não o risco, mas na forma como ele é definido, classificado e convertido em exigências regulatórias.
    - Sempre que possível, esses critérios devem ser operacionalizados por parâmetros verificáveis e documentáveis, permitindo consistência regulatória e auditabilidade.
- **Diferentes formas de definir quando há risco:** Diferentes regimes variam quanto:
    - **(i) ao grau de obrigatoriedade das regras** (se são vinculantes ou apenas orientativas),
    - **(ii) à forma como estruturam o modelo regulatório** (com categorias fixas ou princípios gerais),
    - **(iii) ao nível de previsibilidade do risco** (se a lei define previamente quais aplicações são de alto risco, se essa

definição pode ser ampliada caso a caso pela autoridade competente, ou ainda se a avaliação é sempre no caso concreto)

- **(iii) ao critério analisado para definir o risco** (finalidade, setor, impacto sobre direitos, severidade do dano, o grau de supervisão humana, o impacto em populações vulneráveis etc),

- **(iv) ao momento em que a avaliação do risco é exigida** (antes da colocação no mercado, já no desenvolvimento ou de forma contínua de acordo com cada momento)

- **Grau de obrigatoriedade das regras:** As regulações de inteligência artificial variam significativamente quanto à sua força normativa. Na prática, regimes eficazes tendem a combinar instrumentos vinculantes e orientativos, formando estruturas de governança regulatória.

  - **Hard Law:** Algumas são juridicamente vinculantes (hard law), como o **AI Act da União Europeia** ou propostas legislativas nacionais, impondo obrigações taxativas, sanções e mecanismos formais de fiscalização.

  - **Soft Law:** Outras assumem a forma de diretrizes, princípios ou frameworks técnicos (soft law), como os **Princípios da OCDE**, que não criam deveres legais imediatos, mas influenciam práticas regulatórias, decisões judiciais e políticas públicas.

  - **Padrões técnicos:** Além disso, padrões técnicos internacionais — como normas **ISO** e **IEEE, o NIST AI Risk Management Framework nos Estados Unidos, e as NBRs publicadas pela ABNT** — desempenham papel crescente na operacionalização dessas regras, servindo como referência para conformidade, auditoria e certificação.

- Na prática, mesmo instrumentos não vinculantes podem moldar fortemente o comportamento de empresas e governos, especialmente quando incorporados a contratos, exigências de mercado ou futuras regulamentações formais.

- **Estrutura do modelo regulatório:** As regulações de IA diferem quanto à forma como organizam juridicamente o risco.

  - **Classificação em categorias graduais:** Tanto o modelo europeu quanto o modelo brasileiro do PL 2.338/2023 aprovado no Senado, os sistemas ou aplicações são pré-enquadrados em categorias de risco — por exemplo, baixo, médio, alto ou excessivo. A adoção de categorias formais de risco permite previsibilidade, embora desconsidere a possibilidade fática de determinada aplicação, ainda que inserida em uma atividade originalmente classificada como de alto risco, no seu contexto concreto de uso, não o ser.

    - Essa classificação não é meramente descritiva: ela organiza o nível de atenção regulatória que cada caso receberá. A lógica é proporcional: quanto maior o risco identificado, maior a intensidade da intervenção. A categorização funciona como um mecanismo de triagem normativa.

  - **Modelo escalonado europeu:** A União Europeia adota um **modelo escalonado com categorias formais** previamente definidas em lei: **risco inaceitável (proibido), alto risco (fortemente regulado), risco limitado (transparência) e risco mínimo (sem obrigações específicas)**.

  - **Modelo escalonado brasileiro:** O Brasil, no texto aprovado no Senado (PL 2.338/2023), também estrutura o regime em categorias formais — **risco excessivo (vedado), alto risco (obrigações reforçadas) e demais riscos (obrigações gerais)** — compondo um modelo escalonado que onera inclusive sistemas de baixo ou nenhum risco.

- **Modelos contextuais:** Em contraste, instrumentos como os da OCDE e o NIST não organizam o regime em categorias jurídicas fixas, mas operam a partir de princípios e diretrizes gerais, sem divisão formal em níveis de risco. Nesses modelos, o **risco é avaliado de forma contextual e contínua**, com foco no uso (e não no desenvolvimento do sistema/modelo de IA) com base em parâmetros como probabilidade e severidade de impactos, exigindo que organizações identifiquem, documentem e mitiguem riscos ao longo do ciclo de vida do sistema, em vez de enquadrá-lo previamente em uma categoria legal específica.

- **Nível de previsibilidade da classificação:** As jurisdições diferem quanto ao grau de segurança jurídica que oferecem na definição do que será considerado alto risco. O ponto central não é apenas quem classifica, mas quão previsível e estável é essa classificação.

  - **União Europeia (AI Act):** O alto risco está definido em listas taxativas na própria lei, o que oferece previsibilidade ex ante. As organizações sabem previamente se sua aplicação se enquadra como alto risco, reduzindo margem de incerteza, porém de forma dissociada do uso efetivo da IA.

  - **Brasil (PL 2.338/2023 – texto aprovado no Senado):** Embora existam categorias formais, a definição de alto risco baseia-se em critérios abertos relacionados ao impacto sobre direitos fundamentais. Além disso, autoridades setoriais ou a autoridade coordenadora (ANPD) podem detalhar e complementar essa classificação. Isso amplia a elasticidade regulatória, mas reduz a previsibilidade normativa.

  - **Estados Unidos:** Não há classificação legal geral de risco. A previsibilidade depende de interpretação de normas setoriais existentes e da aplicação de frameworks como o NIST AI RMF. O enquadramento tende a ser mais contextual e dependente de enforcement posterior.

- **Reino Unido:** A ausência de categorias nacionais fixas e a delegação a reguladores setoriais tornam a previsibilidade dependente do setor e da atuação regulatória específica, focada no contexto do uso e existência (ou não) de risco considerável.

- **Singapura e Israel:** Como operam majoritariamente por diretrizes e governança voluntária, a previsibilidade decorre mais de boas práticas e expectativas regulatórias do que de categorias legais rígidas.

- **Deveres e Responsabilização:** A depender do modelo regulatório escolhido, diferentes deveres e responsabilidades são aplicáveis.

  - **Regimes vinculantes (UE e Brasil):** Cada categoria de risco está previamente associada a um conjunto de obrigações jurídicas. Sistemas de baixo risco podem estar sujeitos apenas a deveres gerais de diligência ou transparência, enquanto sistemas de alto risco podem exigir avaliação de impacto, documentação técnica robusta, supervisão humana e monitoramento contínuo. A consequência jurídica não é arbitrária, mas vinculada ao enquadramento realizado.. A desconformidade pode resultar em sanções administrativas, multas e imposição de medidas corretivas pela autoridade competente, mesmo para sistemas de baixo ou nenhum risco.

  - **Modelos predominantemente orientativos ou setoriais (EUA, Reino Unido, Singapura, Israel):** A responsabilização tende a ocorrer de forma indireta e muitas vezes ex post, por meio da aplicação de normas setoriais existentes, enforcement de agências reguladoras ou responsabilidade civil.

- **Critério utilizado para definir o risco:** As jurisdições também divergem quanto ao parâmetro substantivo adotado para identificar o que torna uma aplicação arriscada.

- **União Europeia (AI Act):** O critério central combina finalidade e setor de uso, com foco especial em áreas sensíveis como emprego, crédito, educação, segurança e justiça. O risco é associado ao potencial impacto estrutural dessas aplicações.

- **Brasil (PL 2.338/2023 – texto aprovado no Senado):** O critério é centrado no impacto potencial sobre direitos fundamentais, criando sobreposição com outras previsões legais que versam sobre os mesmos direitos (ex. LGPD, Marco Civil da Internet, entre outras).

- **Estados Unidos:** A análise tende a se basear na probabilidade e severidade de danos, especialmente riscos ao consumidor, concorrência, segurança ou conformidade com normas setoriais existentes.

- **Reino Unido:** O risco é analisado à luz de princípios como segurança, fairness, accountability e transparência, aplicados por reguladores setoriais.

- **Singapura e Israel:** A avaliação é contextual e baseada em governança responsável, com ênfase em confiabilidade, segurança, explicabilidade e mitigação de danos sociais.

II - Ciclo de Vida

- **Por que o ciclo de vida é determinante:** A Inteligência Artificial não é um produto estático; ela evolui ao longo do tempo. Riscos podem surgir na fase de design, intensificar-se no treinamento, manifestar-se na implementação ou emergir após atualizações. Por isso, a gestão baseada em risco pode acompanhar todo o ciclo de vida do sistema — da concepção ao monitoramento pós-implantação. Medir risco apenas em um momento isolado pode produzir conclusões incompletas.

- **Ciclo de vida e Gestão de Riscos:** A gestão baseada em risco responde à pergunta: "***quão rigorosa deve ser a regulação?***" O ciclo de vida responde à pergunta: **"*quando e por quem ela deve ser aplicada?*"** Quando os dois elementos trabalham juntos, o resultado tende a ser:

    - regulação proporcional,
    - foco em prevenção,
    - possibilidade de revisão,
    - e mais segurança jurídica.

- **Momento do ciclo de vida da IA em que a avaliação do risco é exigida:** A regulação pode incidir em diferentes fases do ciclo de vida de um sistema de IA, que normalmente incluem: **(i) concepção e design**, **(ii) desenvolvimento e treinamento**, **(iii) testes e validação**, **(iv) colocação no mercado ou disponibilização**, e **(v) uso, monitoramento e atualização**. As jurisdições diferem quanto ao ponto em que exigem a avaliação formal do risco.

    - **União Europeia e colocação no mercado :** A avaliação ocorre predominantemente **antes da colocação no mercado** ou **entrada em operação (conformidade ex ante)**, isto é, quando a finalidade e o contexto de uso já estão suficientemente delimitados, com **deveres de monitoramento posterior**.

    - **Brasil e riscos no desenvolvimento no PL 2338/23 aprovado no Senado:** A avaliação pode ser exigida já na fase de desenvolvimento e deve se estender ao longo do ciclo de vida do sistema. Isso significa que o **escrutínio regulatório pode incidir em estágio anterior à definição completa do uso concreto**, antecipando obrigações mesmo quando a aplicação final ainda não está plenamente consolidada.

    - **Estados Unidos e abordagem contínua e distribuída:** A abordagem é contínua e distribuída, sem um momento formal

único de certificação prévia. O risco pode ser **gerido internamente desde o design até a operação**, com **responsabilização frequentemente ocorrendo após a introdução no mercado** ou diante de danos concretos.

- **Reino Unido e escolhas setoriais:** A avaliação ocorre conforme exigido por reguladores setoriais e tende a estar vinculada ao **contexto específico de aplicação dentro de cada setor**.

- **Singapura e Israel:** A lógica é de **gestão contínua de riscos** ao longo do desenvolvimento, implementação e uso, sem **marco formal único de aprovação prévia**, privilegiando **governança progressiva** conforme o contexto se define.

- **Ciclo de vida e pluralidade de atores na cadeia de IA:** O ciclo de vida de um sistema de IA envolve diferentes agentes que atuam em momentos distintos e exercem graus variados de controle sobre o risco:

  - **desenvolvedores** (concebem e treinam o modelo),
  - **fornecedores** (colocam o sistema no mercado sob sua marca),
  - **integradores ou implementadores** (adaptam e incorporam o sistema a produtos ou serviços específicos),
  - **distribuidores** (comercializam ou disponibilizam o sistema) e
  - **usuários ou operadores finais** (utilizam a aplicação no contexto concreto).

- **Dever regulatório por ator:** Como a IA é tecnologia de propósito geral, uma aplicação pode ser dada ao sistema independentemente da intenção original do desenvolvedor. Assim, os deveres regulatórios devem ser distribuídos conforme o papel e o grau de controle de cada ator sobre o risco.

  - Quem projeta e treina o modelo deve mitigar riscos previsíveis de arquitetura e dados; quem integra e define o contexto de

uso deve avaliar impactos concretos da aplicação; quem opera o sistema deve garantir uso conforme a finalidade declarada.

- Da mesma forma, a responsabilização deve considerar quem causa o dano, evitando tanto lacunas de responsabilidade quanto imputações desproporcionais.

- **Como as regulações se distribuem ao longo da cadeia de atores:** As diferentes legislações e diretrizes alocam deveres conforme o papel exercido por cada agente no ciclo de vida do sistema.

  - **União Europeia (AI Act):** Estrutura clara por papéis. O *fornecedor* (quem coloca no mercado sob sua marca) concentra os deveres principais de conformidade, documentação e avaliação ex ante; o *integrador/deployer* (quem implementa no contexto concreto) deve garantir uso adequado, supervisão humana e monitoramento; distribuidores têm deveres de verificação formal; e o desenvolvedor pode ser enquadrado como fornecedor quando controla o produto final. O modelo é funcional e vincula obrigações ao papel exercido.

  - **Brasil (PL 2.338/2023 – texto aprovado no Senado):** Também distribui deveres conforme a posição na cadeia, mas com maior abertura conceitual. Desenvolvedores e fornecedores assumem obrigações de governança e avaliação de impacto; implementadores e operadores devem avaliar o contexto concreto de uso. A amplitude dos critérios pode ampliar a responsabilidade de múltiplos agentes, dependendo da interpretação administrativa.

  - **Estados Unidos:** Não há estrutura única por papéis em uma lei geral de IA. A responsabilização decorre de normas setoriais e de proteção ao consumidor. Desenvolvedores e fornecedores podem ser responsabilizados por práticas enganosas ou riscos não mitigados (ex.: FTC), enquanto

operadores podem responder por violações regulatórias no setor específico (ex.: saúde, crédito). O enquadramento depende do tipo de atividade e do dano.

- **Reino Unido:** Como o modelo é setorial, a distribuição de deveres depende do regulador competente. Normalmente, quem controla a aplicação no setor específico assume as principais obrigações, independentemente de ser desenvolvedor ou operador.

- **Singapura e Israel:** As diretrizes enfatizam governança organizacional. A responsabilidade recai sobretudo sobre a entidade que decide implementar ou oferecer o sistema, exigindo que estabeleça processos internos de gestão de risco, independentemente da posição formal na cadeia.

III - Qual o melhor modelo para o Conselho Digital?

- **Regulação centrada na aplicação de alto risco da IA:** O risco não está na tecnologia em si, mas na forma como ela é utilizada. Um mesmo modelo pode recomendar músicas (baixo impacto) ou decidir automaticamente a concessão de crédito (alto impacto). Regular a ferramenta como um todo gera sobrecarga desnecessária; regular o uso concreto permite calibrar intervenção conforme o efeito real.

- **Classificação orientada por usos e não por setores ou tecnologias:** Setores como saúde, crédito ou educação não são, por si, intrinsecamente de alto risco. Um software que organiza prontuários médicos não apresenta o mesmo risco que um sistema que decide automaticamente o acesso a tratamento. Classificar usos específicos evita impor obrigações máximas a aplicações auxiliares ou administrativas de baixo impacto.

- **Modelo setorial com competência técnica vinculada a parâmetros legais:** Reguladores setoriais estão mais próximos da realidade operacional de seus mercados e, por isso, conseguem distinguir com maior precisão diferentes usos da tecnologia — por exemplo, entre um sistema de detecção de fraude (que mitiga risco) e uma decisão automatizada de crédito sem revisão humana (que pode ampliar risco). Contudo, essa contextualização deve ocorrer dentro de critérios previamente definidos em lei. O regulador setorial aplica e interpreta parâmetros legais objetivos ao caso concreto, mas não pode ampliar categorias de risco, redefinir conceitos legais ou criar novas obrigações estruturais por via infralegal. Assim, preserva-se a especialização técnica sem abrir espaço para expansão discricionária do regime.

- **Lei clara e restritiva quanto à classificação de risco:** Caso exista modelo escalonado, aos moldes europeu, as categorias devem estar definidas em lei, com hipóteses delimitadas. A ampliação pelo

regulador infralegal gera incerteza e aumenta custo de capital, pois empresas passam a operar sob risco permanente de reclassificação futura.

- **Equilíbrio entre incentivos preventivos e accountability ex post:** Obrigações excessivas antes da entrada no mercado podem sufocar inovação; ausência de responsabilização posterior gera risco social. O modelo eficiente combina liberdade inicial proporcional ao risco com enforcement firme quando há dano ou negligência. Modelos excessivamente prescritivos tendem a favorecer grandes incumbentes, criar barreiras à entrada e deslocar recursos de inovação para cumprimento burocrático. Em vez disso, o foco deve estar na efetividade da governança.

- **Responsabilização orientada por governança efetiva e resultados concretos:** Em caso de dano ou negligência, a análise de responsabilidade deve considerar se o agente adotou medidas razoáveis de mitigação, monitoramento e correção compatíveis com o risco da aplicação. A presença de estruturas internas adequadas deve funcionar como elemento atenuante; sua ausência, como fator de agravamento. Esse modelo incentiva investimento real em governança e prevenção, em vez de simples cumprimento procedimental, alinhando incentivos econômicos com redução concreta de riscos.

- **Imputação baseada na falha concreta e não na mera existência da tecnologia:** A responsabilização deve estar ligada a dano efetivo, violação legal ou falha relevante de mitigação. Presumir risco elevado apenas pela adoção de IA cria incentivos para evitar tecnologia mesmo quando ela reduz riscos.

- **Acoplamento a padrões técnicos como solução de dinamicidade:** Em vez de detalhar tecnicamente obrigações na lei, o modelo pode reconhecer padrões técnicos de gestão de risco como referência. Isso permite atualização constante conforme a tecnologia evolui, sem necessidade de ampliar discricionariamente o escopo regulatório.

- **Equilíbrio entre inovação e proteção de direitos:** a regulação baseada em risco busca equilibrar dois objetivos complementares, promovendo a inovação tecnológica e assegurando a proteção adequada de direitos individuais e coletivos. Um modelo eficaz deve garantir proporcionalidade regulatória sem comprometer a confiança pública nos sistemas de inteligência artificial. Neste contexto, é importante evitar sobreposições com normas vigentes que possam gerar insegurança jurídica. Aqui, uma reflexão premente que deve nortear os dispositivos relativos à proteção de direitos é: qual é a lacuna de proteção constatada na legislação atual (ex. LGPD) que necessita de enfrentamento complementar por uma nova Lei?

- **Papel das autoridades reguladoras:** as autoridades reguladoras desempenham papel essencial na implementação da regulação baseada em risco, especialmente na emissão de orientações técnicas, coordenação entre setores e monitoramento da evolução tecnológica. Esse papel deve ser exercido com transparência e previsibilidade, respeitando os limites estabelecidos na legislação.

🇪🇺 União Europeia – AI Act (Reg. 2024/1689)

Grau de juridicidade:

- Hard law.

Estrutura institucional:

- Escalonado (níveis graduais de risco)
- Transversal (se aplica de forma geral a múltiplos setores da economia).

Critério central de identificação do risco:

- Finalidade
- Setor de uso.

Listas de risco taxativas:

- Os sistemas de alto risco estão definidos em listas taxativas nos anexos (modelo tipológico fechado).

Momento e forma de avaliação:

- Predominantemente antes da colocação no mercado ou entrada em operação (conformidade ex ante), com monitoramento posterior

Categorias formais de risco:

- risco inaceitável (proibido)
- alto risco (fortemente regulado)
- risco limitado (transparência)
- risco mínimo (sem obrigações específicas).

Comentários e Observações Relevantes

A primeira grande regulação de inteligência artificial: A União Europeia foi a primeira jurisdição a aprovar um marco regulatório abrangente e vinculante para sistemas de IA, o AI Act (Regulamento 2024/1689).

Aplicação faseada: O AI Act foi aprovado em 2024 e sua implementação começou a ser faseada — embora as principais obrigações para os sistemas de alto risco ainda estejam em processo de entrada em vigor.

Peso da conformidade: Alguns setores apontam que o peso da conformidade ex ante pode criar barreiras de inovação para pequenas e médias empresas; há ainda preocupações sobre interpretação e aplicação descoordenada entre Estados-membros.

🇧🇷 Brasil – PL 2.338/2023

texto aprovado no Senado

Grau de juridicidade:

- Hard law (em processo legislativo).

Estrutura institucional:

- Escalonado (níveis graduais de risco)
- Transversal (se aplica de forma geral a múltiplos setores da economia).

Critério central de identificação do risco:

- Impacto potencial sobre direitos fundamentais

Listas de risco taxativas:

- Não há listas taxativas fechadas de alto risco (modelo criteriológico aberto).
- Autoridade administrativa poderá ampliar a lista.

Momento e forma de avaliação:

- Pode ocorrer já na fase de desenvolvimento e se estende ao longo do ciclo de vida do sistema.

Categorias formais de risco:

- risco excessivo (vedado)
- alto risco (obrigações reforçadas, como avaliação de impacto algorítmico)
- demais riscos (obrigações gerais de governança e transparência)

Comentários e Observações Relevantes

Gestão baseada em risco com lista aberta aumenta flexibilidade, mas reduz previsibilidade e pode gerar distorções em relação ao risco: A regulação deve incidir apenas sobre sistemas comprovadamente de alto risco. A forma como o escalonamento de risco aparece no PL pode ocasionar uma expansão interpretativa do escopo legal sem alteração legislativa, o que pode afetar previsibilidade e estabilidade regulatória.A melhor saída envolve a revisão periódica por via legislativa ou o acoplamento com normas técnicas.

IA e é uma tecnologia de propósito geral e deve ser avaliada de acordo com sua aplicação contextual: Como a avaliação de risco pode ser exigida já na fase de desenvolvimento, antes da definição completa da aplicação concreta, há risco de enquadramentos prematuros, superestimação de riscos ainda hipotéticos e imposição de obrigações desproporcionais a modelos de propósito geral. Além disso, como sistemas de IA podem mudar de finalidade ao longo do ciclo de vida, uma avaliação muito precoce pode não refletir o risco real da aplicação final.

🇺🇸 Estados Unidos – Abordagem Federal Fragmentada (NIST AI RMF, e regulação setorial)

contraponto ao modelo europeu tipificado

Grau de juridicidade:

- Modelo híbrido.
- Soft law (NIST AI Risk Management Framework).
- Hard law setorial (FTC, FDA, CFPB, SEC, entre outros), dentro de suas competências legais já existentes.

Estrutura institucional:

- Não escalonado formalmente.
- Fragmentado e setorial (cada agência regula atividades sob sua competência, não a tecnologia em si).
- Transversal apenas no nível de princípios e diretrizes federais.).

Critério central de identificação do risco:

- Probabilidade e severidade de danos no âmbito da competência da agência (ex.: proteção ao consumidor, segurança de produtos médicos, crédito, valores mobiliários).
- O foco é a atividade regulada, não a IA como categoria autônoma.

Listas de risco taxativas:

- Não há listas nacionais de "alto risco" definidas em lei federal geral.
- A identificação do risco ocorre caso a caso, conforme o setor regulado.

Momento e forma de avaliação:

- Gestão contínua de riscos ao longo do ciclo de vida.
- Sem certificação ex ante obrigatória geral para IA.
- Responsabilização frequentemente ocorre por meio de enforcement posterior, quando há violação de normas setoriais.

Categorias formais de risco:

- Não há categorias jurídicas formais de risco em nível federal geral.

Comentários e Observações Relevantes

Regulação por atividade, não por tecnologia: As agências federais não regulam "inteligência artificial" enquanto tecnologia abstrata, mas sim condutas e produtos dentro de suas competências legais (ex.: práticas enganosas, discriminação em crédito, segurança de dispositivos médicos).

Centralidade do NIST AI RMF: O framework funciona como orientação técnica voluntária, influenciando boas práticas e contratações públicas, mas não cria obrigações jurídicas diretas.

Ênfase em enforcement setorial: A intervenção estatal ocorre quando o uso da IA viola normas existentes — e não porque a tecnologia foi previamente classificada como de alto risco em uma lei geral.