

À

**Comissão Temporária Interna sobre Inteligência Artificial  
SENADO FERAL**

**Ref.: Contribuição do IBRAC ao Projeto de Lei ° 2.338/2023 – Regulamentação de Sistemas de Inteligência Artificial**

O IBRAC, Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional é uma entidade privada, sem fins lucrativos, criada em dezembro de 1992 com o objetivo de promover a realização de pesquisas, estudos e debates sobre temas relacionados à defesa da concorrência, comércio internacional e consumo. Nesta toada, vem submeter contribuições à CTIA, a fim de auxiliar no processo de discussão empreendido pelo Senado Federal sobre o assunto, especialmente no âmbito do Projeto de Lei 2338/2023.

Este documento está dividido em duas grandes partes. Uma primeira, voltada a uma breve análise comparativa de modelos regulatórios debatidos mundo afora, que é complementada pelo Anexo 1 (planilha em que esta análise é feita de maneira mais pormenorizada). E uma segunda, que traz comentários específicos a artigos do PL 2338/2023, especialmente aqueles que dizem respeito à responsabilidade dos agentes de Inteligência Artificial.

**I. Modelos regulatórios para a Inteligência Artificial**

No Anexo 1 a este documento, foi realizada uma comparação entre as iniciativas regulatórias debatidas ao redor do mundo, a partir de quatro perguntas-guia:

- Qual é o tipo de iniciativa analisada?
- O que a iniciativa diz sobre enforcement?
- Quem são os principais destinatários da proposta? e
- A proposta cria direitos?

A primeira pergunta se justifica porque se notou que embora algumas jurisdições já tenham propostas legislativas para a regulação de IA, outras não possuem iniciativas que nasceram dos poderes legislativo ou executivo, mas sim aquilo que aqui denominamos iniciativas “principiológicas” - que delineiam parâmetros para a criação e uso de IA - advindas de outros órgãos.

No caso da presente pesquisa, somente o AI Act tem natureza legislativa (e, vale notar, ele surge após a adoção de parâmetros de soft-law publicados em 2019 na União Europeia, vide *Ethics Guidelines for Trustworthy AI*). As demais propostas analisadas são todas principiológicas. Nesse sentido, a única proposta que teria competência normativa para criar novos direitos - o AI Act - não o faz. Ao contrário, a proposta busca proteger direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia - como o direito à não-discriminação, liberdade de expressão, dignidade humana, privacidade e proteção de dados pessoais - que podem ser adversamente afetados com sistemas de IA.

Vale ressaltar que essa proteção se dá a partir de uma lógica de categorização de riscos: quanto maior o risco, maior os cuidados e obrigações que recaem sobre os provedores de IA. Aquelas categorias de sistemas de IA que apresentam riscos inaceitáveis são proibidas.

A proposta é direcionada principalmente para (i) provedores de sistemas de IA estabelecidos dentro da UE ou em um terceiro país que colocasse sistemas de IA no mercado da UE ou os implementasse no território da UE; (ii) usuários de sistemas de IA localizados na UE; e, para evitar o *bypass* regulatório, (iii) provedores e usuários de sistemas de IA localizados em um país terceiro onde

o resultado produzido por esses sistemas fosse usado na UE. O projeto, no entanto, não se aplica a sistemas de IA desenvolvidos ou usados exclusivamente para fins militares, a autoridades públicas em um terceiro país, nem a organizações internacionais ou autoridades que utilizam sistemas de IA no âmbito de acordos internacionais de cooperação judicial e policial.

No que tange o mecanismo de *enforcement*, a proposta exige que os Estados-Membros designem uma ou mais autoridades competentes, incluindo uma autoridade de supervisão nacional, encarregada de supervisionar a aplicação e implementação do regulamento, e estabelece um Conselho Europeu de Inteligência Artificial (composto por representantes dos Estados-Membros e da Comissão) a nível da União Europeia. As autoridades nacionais de vigilância de mercado seriam responsáveis por avaliar a conformidade dos operadores com as obrigações e requisitos para sistemas de IA de alto risco, tomando medidas proibitivas e restritivas a sistemas de IA em desconformidade com a lei ou que representem um risco alto. Cabe aos Estados-Membros o estabelecimento de regras sobre penalidades, incluindo multas administrativas, e tomar todas as medidas necessárias para garantir que sejam aplicadas de forma adequada e eficaz. Apesar de a estrutura brasileira ser consideravelmente diferente, visto que é somente um país, há algumas críticas feitas ao sistema de *enforcement* proposto pelo AI-Act que podem ser aproveitadas pela discussão nacional.

Ausência de estruturas de fiscalização eficazes dado que a Comissão propõe deixar a avaliação preliminar de riscos, incluindo a qualificação como de alto risco, a cargo da autoavaliação dos fornecedores.

Necessidade de fortalecimento da supervisão democrática: há preocupação com a delegação excessiva de poder regulatório a organizações privadas de padronização europeias (ESOs), devido à falta de supervisão democrática, à impossibilidade de os interessados (organizações da sociedade civil, associações de consumidores) influenciarem o desenvolvimento de padrões e à falta de meios judiciais para controlá-los uma vez que tenham sido adotados. Há recomendações para que a Lei de IA codifique um conjunto de requisitos legalmente vinculativos para sistemas de IA de alto risco (por exemplo, formas proibidas de discriminação algorítmica), que as ESOs podem especificar por meio de padrões harmonizados.

Ausência de possibilidade para a reivindicação de direitos individuais: os indivíduos afetados por sistemas de IA e as organizações de direitos civis não têm o direito de reclamar às autoridades de vigilância do mercado ou processar um fornecedor ou usuário por não cumprir os requisitos. Assim, embora algumas disposições do projeto de lei visem impor obrigações aos usuários de sistemas de IA, não há mecanismo de reclamação ou recurso judicial disponível para eles. Há recomendações para que a proposta seja emendada para incluir, entre outras coisas, um direito explícito de recurso para os indivíduos e direitos de consulta e participação para os cidadãos da UE em relação à decisão de alterar a lista de sistemas de alto risco no Anexo III.

As demais propostas regulatórias, conforme mencionado, são principiológicas, ou seja, seu cumprimento é voluntário.

O documento estadunidense - *Artificial Intelligence Risk Management Framework* (AI RMF 1.0) - consiste em um *framework* elaborado pelo *National Institute of Standards and Technology* (NITS), a pedido do Congresso estadunidense. Da mesma forma que o AI Act, o documento também objetiva a preservação de direitos existentes. O AI RMF é destinado a ser prático, adaptar-se ao panorama da IA à medida que as tecnologias de IA continuam a se desenvolver, e ser operacionalizado por organizações em vários graus e capacidades para que a sociedade possa se beneficiar da IA ao mesmo tempo em que é protegida de seus possíveis danos. Busca ser abrangente e flexível, isto é, não é específico a nenhum setor e destina-se aos atores de IA ao longo do ciclo de vida da IA e em suas diferentes dimensões. As dimensões da IA consideradas são: Contexto de Aplicação, Dados e Entrada, Modelo de IA e Tarefa e Saída.

Os atores de IA envolvidos nessas dimensões, que realizam ou gerenciam o *design*, desenvolvimento, implementação, avaliação e uso de sistemas de IA e impulsionam os esforços de gerenciamento de riscos de IA, são o público principal do AI RMF. Como a proposta se trata de um framework não-vinculante, não há uma proposta de *enforcement* no sentido de um órgão ou entidade supervisora e fiscalizadora da implementação das recomendações do guia. No entanto, em 30 de março, o NITS lançou o Centro de Recursos de IA Confiável e Responsável para "*facilitar a implementação e o alinhamento internacional com o AI RMF*". Assim, embora o *compliance* com o disposto no *framework* seja voluntário, pode-se dizer que há uma entidade centralizada para auxiliar em sua implementação. A ideia é que o *framework* seja dinâmico e abrangente e, assim, conta com a participação contínua, com mecanismos para *feedbacks* constantes. O *framework* e os recursos de suporte serão atualizados, expandidos e aprimorados com base na evolução da tecnologia, no panorama de padrões ao redor do mundo e na experiência e *feedback* da comunidade de IA. O NIST continuará a alinhar o AI RMF e orientações relacionadas com os padrões internacionais, diretrizes e práticas aplicáveis.

Além disso, de maneira similar à abordagem da União Europeia, a primeira parte do *framework* é construída a partir dos riscos. Especificamente, discute como as organizações podem enquadrar os riscos relacionados à IA e descreve o público-alvo. Em seguida, os riscos e a confiabilidade da IA são analisados, delineando as características de sistemas de IA confiáveis, que incluem serem válidos e confiáveis, seguros, seguros e resilientes, responsáveis e transparentes, explicáveis e interpretáveis, aprimorados em privacidade e justos, com seus vieses prejudiciais gerenciados.

De acordo com o *National Strategy for AI*, a Coreia do Sul pretende alcançar a liderança no ecossistema global de IA até o ano de 2030, adotando uma postura arrojada que propõe inovação regulatória e revisão das leis subjacentes existentes. Neste sentido, a abordagem é pautada pela máxima de "*aprovar primeiro e regular depois*". Ou seja, adota-se uma postura de incentivo da IA no país por meio da criação de uma legislação flexível e de *sandboxes* regulatórios que fomentem seu desenvolvimento e uso em ambiente seguro e protegido de eventuais impeditivos legais existentes, exceto para os casos em que haja algum prejuízo à vida e/ou segurança das pessoas (o documento não esclarece quais seriam esses casos). A ideia é perseguir o desenvolvimento nacional e social, compartilhando os benefícios e oportunidades de crescimento econômico possibilitados pela IA. Ao contrário da proposta de legislação da inteligência artificial mais proeminente hoje no Brasil - PL 2338/2023 ("PL"), a Estratégia Nacional da Inteligência Artificial da Coreia do Sul é mais permissiva e ousada, já que flexibilidade e foco na liderança no ecossistema global de IA que pautam a abordagem sul coreana vai de encontro à orientação de uma postura mais preventiva e conservadora constante do PL, contando com enfoque baseado em um rigoroso processo de avaliação prévia e gestão de riscos, de forma centrada nos direitos humanos.

De forma mais concreta, a Coreia do Sul pretende que uma futura legislação da IA contenha: (i) princípios com foco no desenvolvimento nacional e social, através do compartilhamento de benefícios e oportunidades do crescimento econômico de forma abrangente; (ii) uma base para informatização inteligente, por meio de investimento na indústria, apoio ao desenvolvimento tecnológico e regulamentação de política de dados; (iii) disposições obrigatórias que exijam que o governo estabeleça medidas de resposta aos impactos da IA no ambiente laboral; (iv) normas éticas, de prevenção à violação de informações pessoais e privacidade e; (v) medidas de proteção mínima, para garantir a segurança e confiabilidade de cada nova tecnologia e serviço.

No Reino Unido, a Câmara dos Comuns lançou uma investigação em 20 de outubro de 2022 para examinar o impacto da IA na sociedade e na economia, se e como a IA e seus diferentes usos devem ser regulamentados; e as propostas de governança de IA do governo do Reino Unido. Em 31 de agosto de 2023, a Câmara dos Comuns publicou o relatório, destacando as descobertas iniciais, abordando os recentes desenvolvimentos em IA, seus benefícios e desafios, e como o governo do Reino Unido respondeu, comparando a abordagem com a de outros países e jurisdições. É esse o relatório que a presente pesquisa analisou. O relatório foi lançado no contexto de um *white paper* sobre IA publicado pelo governo no final de março de 2023, que visava orientar o uso de IA no Reino Unido, impulsionar

a inovação de maneira responsável, manter a confiança do público na tecnologia de IA e surgiu do documento de política de julho de 2022 intitulado 'Estabelecendo uma abordagem pró-inovação para regulamentar a IA' e da 'Estratégia Nacional de IA' publicada em setembro de 2021.

O relatório sugere que a abordagem do governo para a governança e regulamentação da IA deve abordar doze desafios mapeados, tanto por meio de políticas domésticas quanto de engajamento internacional. Nesse sentido, a iniciativa é também principiológica, já que, ainda que no âmbito governamental, não consiste (ainda) em uma proposta de legislação. No entanto, o Poder público é o principal destinatário da proposta, tendo em vista que a proposta se concentra em estabelecer princípios para a atividade regulatória.

No que diz respeito ao *enforcement*, a adoção setorial é apontada como ponto de partida tendo em vista o tempo necessário para a criação de novos organismos reguladores. Nesse sentido, o relatório aponta que diversos reguladores já estão empenhados em engajar-se nas implicações da IA para as suas competências. Assim, ainda que se reconheça a necessidade de estabelecer novos órgãos regulatórios e funções de suporte central, o relatório aponta que a estruturação da regulamentação propriamente dita requer maior desenvolvimento e consideração em documentos legislativos e regulatórios subsequentes. Além disso, no *white book*, o governo sinalizou que poderá legislar de modo a estabelecer deveres *de due regard* para as entidades reguladoras existentes, o que sugere que deve haver um projeto de lei sobre IA direcionado na nova sessão do parlamento.

Por fim, muito diferente do caminho seguido pelo projeto de lei sendo desenvolvido no Brasil, ou mesmo o AI Act europeu, existe ainda a proposta regulatória implementada no Japão. A seu respeito, a abordagem do país para enfrentar os desafios de IA segue, com antecipado, uma linha regulatória principiológica, e guiada por recomendações não vinculantes do Ministério de Economia, Comércio e Indústria (“METI”). Especificamente, o METI entende que “*regulações horizontais legalmente vinculantes para sistemas de IA são desnecessárias neste momento*”, observadas as dificuldades dessas normas em acompanhar a velocidade e a complexidade da inovação em IA. Ao ver do Ministério, uma regulamentação prescritiva, estática e detalhada, no contexto atual, poderia sufocar a inovação sem ter a capacidade de endereçar adequadamente seus riscos. Assim, no que diz respeito ao *enforcement*, a posição do governo é a de que, ao menos no cenário atual, orientações não vinculativas, baseadas em um diálogo multilateral e com atualização contínua, devem pautar os esforços de empresas no uso adequado de IA.

Dito isso, o quadro regulatório atual do país é composto basicamente por orientações não mandatórias destinadas aos agentes desenvolvedores e contratantes de IA, pautadas especialmente no uso de princípios para guiar seu uso, publicadas ao longo dos últimos anos. Em 2019, o governo japonês publicou os Princípios Sociais da Inteligência Artificial Centrada no Ser Humano (Princípios Sociais), guiados por três objetivos iniciais que devem nortear a implementação de IA na sociedade: dignidade humana, diversidade e inclusão, e sustentabilidade. Para alcançar esses objetivos, os Princípios Sociais estabelecem sete princípios em torno da IA: (1) centralização no ser humano; (2) educação/alfabetização; (3) proteção da privacidade; (4) garantia de segurança; (5) competição justa; (6) justiça, responsabilidade e transparência; e (7) inovação. A fim de orientar a aplicação desses princípios em projetos de IA, as Diretrizes de Governança do METI para Implementação dos Princípios de IA buscam guiar empresas exemplos de cenários específicos da aplicação dos Princípios, incluindo estratégias para mapeamento de riscos, garantia de informação a indivíduos sobre sistemas de IA e mecanismos para prevenção e repressão de incidentes. Em 2018, o METI também elaborou Diretrizes de Contrato sobre Utilização de IA e Dados, que buscam orientar a elaboração de contratos envolvendo o desenvolvimento e uso de IA, prevendo e explorando cláusulas-modelos a serem utilizadas como referência pelos agentes do mercado.

De maneira mais abrangente, várias diretrizes foram publicadas para a proteção e utilização de dados com relação à IA. O Guia de Governança Corporativa para Privacidade na Transformação Digital e o Guia para Utilização de Imagens de Câmera, ambos desenvolvidos em conjunto pelo METI

e pelo Ministério dos Assuntos Internos e Comunicações (MIC), fornecem orientações em matéria de privacidade e proteção de dados, incluindo sua preocupação sobre a esfera de uso de IA.

Vale ressaltar que, para além de diretrizes não-mandatórias, o Japão tem buscado adaptar sua legislação à implementação de IA em diferentes frentes legais específicas, naquilo que couber. A exemplo, em 2020, a Lei de Tráfego Rodoviário revisada e a Lei de Veículos de Transporte Rodoviário entraram em vigor, permitindo a condução automatizada de Nível 3 (ou seja, automação condicional) em vias públicas. No setor financeiro, a Lei de Vendas a Prazo foi revisada em 2020 para permitir que um "intermediário certificado de compra de crédito abrangente" determinasse os valores de crédito usando dados e IA. Por fim, a Lei de Direitos Autorais também foi alterada em 2017 para promover o uso de dados em aprendizado de máquina: a emenda esclareceu que o download ou processamento de dados pela internet ou outros meios para desenvolver modelos de IA não constitui uma violação de direitos autorais.

Dito isso, é notório que o caminho seguido pelo Japão se mostra mais conservador e cauteloso para fins de regulação de IA. Diferentemente do PL brasileiro, não se buscou, por exemplo, adotar regras fixas que buscam classificar sistemas de IA conforme risco e atribuir responsabilidade por incidentes e violações a direitos de maneira correspondente. Nesse sentido, considerando a dinamicidade e velocidade da evolução de sistemas de AI, a fim de construir um quadro regulatório adequado à sua complexidade, as diferentes orientações publicadas pelo METI podem servir de inspiração para o Brasil a fim de resguardar que alguns temas regulatórios possam ser desenvolvidos de forma não-mandatária, em formatos de guias, reduzindo riscos de que eventual regulação horizontal resultante do PL brasileiro afogue a inovação com regras rígidas sobre o uso de IA.

## **II. Responsabilização dos agentes de Inteligência Artificial**

### **1. Análise do risco para verificação do sistema de responsabilidade aplicável (artigo 27)**

- **Art. 27, caput:**

O texto proposto ampara-se no arranjo normativo da tutela dos direitos difusos e coletivos do ordenamento jurídico brasileiro. Ao buscar solucionar o modelo da reparação de danos causados por sistemas de inteligência artificial, o legislador recorreu, notadamente, ao direito consumerista, em que impera o princípio da reparação integral pelo dano causado.

Referido princípio objetiva, justamente, colocar o lesado, na medida do possível, em situação equivalente à anterior ao fato danoso, e parece ir ao encontro da defesa legislativa de direitos difusos e coletivos, os quais também se encontram protegidos pelo Projeto de Lei em questão.

- **Art. 27, § 1º:**

Ao estabelecer uma gradação de riscos associados a determinado sistema de inteligência artificial, o texto proposto se inspira nas discussões havidas na Europa, cuja proposta normativa elenca quatro graus distintos: (i) risco inaceitável; (ii) risco alto; (iii) risco limitado; e (iv) risco mínimo. No entanto, a proposta legislativa europeia não abordou em detalhes o regime jurídico aplicável à reparação de danos, focando os esforços iniciais em normas de natureza preventiva.

O Projeto de Lei em questão, por outro lado, também se propõe a resguardar os direitos de possíveis lesados por sistemas de inteligência artificial por meio da adoção do regime de responsabilidade objetiva. Além disso, a responsabilização do fornecedor e do operador também vai ao

---

<sup>1</sup> Art. 27. O fornecedor ou operador de sistema de inteligência artificial que cause dano patrimonial, moral, individual ou coletivo é obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema.



encontro de outras disposições do Código de Defesa do Consumidor que preveem a responsabilização solidária entre a cadeia de fornecimento.

- **Art. 27, § 2º:**

A Proposta de Regulação da União Europeia estabelece que os riscos limitados são aqueles que ensejam obrigações de transparência e acesso à informação (tal como a interação com *chatbots*), ao passo que os riscos mínimos seriam aqueles utilizados em aplicações cotidianas, tais como videogames e filtros tecnológicos.

Diante da natureza dos sistemas de inteligência artificial de risco limitado ou mínimo, a sistemática da tutela de direitos difusos e coletivos, notadamente sob a égide do Direito do Consumidor, que prevê a figura do consumidor como hipossuficiente e o fornecedor/operador como sendo aquele com melhores condições de defender seus interesses e, eventualmente, arcar com suas ações lesivas. (teoria do risco do negócio).

De todo modo, recomenda-se que haja uma delimitação e uma maior clareza sobre os direitos processuais das partes (em especial, referentes à produção probatória) de modo a assegurar que haja paridade de armas e o contraditório efetivo, respeitando também o princípio constitucional da presunção de inocência.

## **2. Discussões terminológicas**

Uma das principais novidades trazidas no anteprojeto é a criação dos conceitos de alto risco e risco excessivo. O risco excessivo se refere àqueles riscos proibidos, em que não se pode aplicar o uso do sistema de IA, e cujas hipóteses estão elencadas no artigo 14 do anteprojeto.<sup>3</sup> Já o alto risco se refere àqueles riscos elevados no uso de IA, cujas hipóteses estão dispostas no artigo 18 do anteprojeto.

Ambas as expressões têm inspiração europeia, mais especificamente na Proposta de Regulamento de Inteligência Artificial da União Europeia – em que pese a expressão “alto risco”, tratando-se de sistemas de IA, já estivesse presente em outras normativas e documentos europeus, como no Livro Branco sobre a Inteligência Artificial e na Proposta de Resolução do Parlamento Europeu 2020/2014.

Em um primeiro momento, para fins de responsabilização civil, indaga-se se seria relevante a importação dos termos alto risco e risco excessivo, visto que se trata de expressões novas no direito civil brasileiro, e que, portanto, não se comunicam com disposições normativas civilistas. Por exemplo, no próprio anteprojeto do Código Civil de 2002, o parágrafo único do artigo 963 – atual parágrafo único do artigo 927 – previa a expressão “grande risco”<sup>4</sup>, mas a expressão “grande” foi após suprimida. Sobre esse ponto, Sílvio Rodrigues afirma que caberia ao arbítrio do juiz atribuir o que seria um grande risco.<sup>5</sup>

Por fim, questiona-se a pertinência dos termos “operador” e “fornecedor” para fins de responsabilização civil, visto que estes conceitos podem acabar se confundindo com o de operador

<sup>2</sup> Art. 27. § 2º Quando não se tratar de sistema de inteligência artificial de alto risco, a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima.

<sup>3</sup> Art. 14. São vedadas a implementação e uso de sistemas de inteligência artificial:

I – que empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos desta lei;

II – que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como associadas à sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial à sua saúde ou segurança ou contra os fundamentos desta lei;

III – pelo poder público, para avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional.

<sup>4</sup> Art. 963. Aquele que, por ato ilícito (arts.184 e 185), causar dano a outrem, é obrigado a repará-lo.

Parágrafo único. Todavia, haverá a obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, grande risco para os direitos de outrem, salvo se comprovado o emprego de medidas preventivas e tecnicamente adequadas. Disponível em: BRASIL. Câmara dos Deputados. Projeto de Lei nº 634/1975. Disponível em: [http://imagem.camara.gov.br/Imagem/d/pdf/DCD13JUN1975SUP\\_B.pdf#page=1](http://imagem.camara.gov.br/Imagem/d/pdf/DCD13JUN1975SUP_B.pdf#page=1). Acesso em: 21 fev. 2023.

<sup>5</sup> RODRIGUES, Sílvio. Direito Civil: responsabilidade civil. Volume IV, 7ª edição revista e atualizada. São Paulo: Saraiva, 1963, p. 175.

trazido na LGPD e o de fornecedor trazido no CDC. Considerando que podem ser agentes diferentes (por exemplo, o operador do sistema de IA pode ser distinto do operador que tratou os dados deste sistema), o uso deste mesmo termo pode, na prática, implicar confusão no momento da responsabilização.

### **3. Excludentes de responsabilidade (artigo 28)**

Sem comentários.

### **4. Interface com CDC (artigo 29), sob o âmbito da responsabilidade civil**

No que diz respeito à responsabilidade civil por danos decorrentes de sistemas de IA, deve-se dedicar especial atenção à intersecção entre as disposições do Projeto de Lei nº 2338/2023 (“PL 2338/23”) e o Código de Defesa do Consumidor (“CDC”). O art. 29 do PL 2338/23 deixa claro que as hipóteses de responsabilização civil decorrentes de danos causados por sistemas de IA no âmbito das relações de consumo permanecem sujeitas às regras do CDC.

Assim, nas relações de consumo, a responsabilidade dos fornecedores e operadores de sistemas de IA (independentemente do risco) continuará condicionada à existência de um defeito daquele produto ou serviço. Essa compreensão está em consonância com as discussões da União Europeia. Em sua proposta para a regulamentação da responsabilidade civil não contratual dos produtores de sistemas de IA (AI Liability Directive<sup>6</sup>, que propõe adaptações ao regime de responsabilidade dos produtores por produtos defeituosos) a UE manteve como requisito o nexo de imputação consistente em se verificar que determinada conduta danosa do sistema de IA foi decorrente de uma falha do dever de cuidado do produtor (Art. 4º). Tratando-se ou não de uma IA de alto risco, a falha do produtor continua sendo requisito de sua responsabilização (ainda que o dever de cuidado seja mais restritivo no caso de IAs de alto risco).

No Brasil, para avaliar se o comportamento da IA pode ser considerado defeituoso, os próprios parâmetros do CDC devem ser levados em conta, especialmente: **(i)** os riscos que razoavelmente se esperam (art. 12, § 1º, II e art. 14, § 1º, II); **(ii)** e a época em que o produto foi colocado no mercado ou que o serviço foi fornecido (art. 12, § 1º, II e art. 14, § 1º, II).

Com relação aos riscos razoavelmente esperados, é certo que existem legítimas expectativas sobre a forma como a IA deve se comportar em determinados casos. Entretanto, não é possível antecipar todos os infinitos cenários em que a IA deverá tomar uma decisão, tampouco o que seria uma decisão acertada naquela circunstância específica. Em casos de danos provocados dentro de cenários imprevisíveis, o operador do direito deve levar em consideração o previsto nos arts. 12, § 1º, II e 14, § 1º, II do CDC. Ou seja, dever-se-á ponderar se realmente pode se falar em defeito do produto/serviço quando aquele determinado dano se deu fora do âmbito das razoáveis expectativas de risco.

Por esse motivo, a previsão do art. 12, § 1º, II e art. 14, § 1º, II do CDC também é de especial relevância. A época em que a IA foi colocada no mercado deve ser considerada pelos operadores do direito, na medida em que não há como se falar em legítima expectativa sobre a segurança e os riscos de uma IA fora do âmbito do conhecimento técnico do momento em que esta foi inserida no mercado.

### **5. Interface com LGPD sob o âmbito da responsabilidade civil**

- **Art. 27, caput:**

---

<sup>6</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496>

Ao definir o ressarcimento de danos, a LGPD (Art. 42) especifica que a reparação é decorrente da “*violação à legislação de proteção de dados pessoais*”. Sugerimos a introdução do mesmo recorte epistemológico aqui.

Embora o Art. 42 da LGPD utilize a conjunção alternativa “ou” para se referir ao controlador e ao operador, em seu §1º, há a discriminação das hipóteses em que o controlador e o operador possuem responsabilidade solidária – deixando claro a diferença de responsabilidade de cada posição. Aqui, por outro lado, usa-se o “ou” sem apresentar qualquer distinção de responsabilidade, deixando evidente lacuna.

No *Liability for Artificial Intelligence*<sup>7</sup> (“Relatório”), elaborado pela *European Commission*, há a diferenciação entre responsabilidade do operador e fornecedor. Entendemos que esse também era o objetivo aqui, visto que houve preferência por mencionar as duas figuras em vez de usar a definição de “*agentes de inteligência artificial*”, que faz, justamente, referência conjunta a ambas.

A diferenciação também é relevante, pois, como levantado pelo Relatório, a responsabilização indiscriminada do fornecedor pode gerar impacto no desenvolvimento de novas tecnologias.

As definições de “operador” e “fornecedor” incluem tanto pessoa física como jurídica, mas não deixa clara a questão da “*vicarious liability*”.

- **Art. 27. § 1º:**

Diferentemente da seção de “Risco Alto”, que possui previsão clara sobre a sua definição, o mesmo não ocorre com o “Risco Excessivo”. Embora o artigo 16 preveja que “caberá à autoridade competente regulamentar os sistemas de inteligência artificial de risco excessivo”, o artigo 14 (artigo introdutório da seção de Risco Excessivo) é confuso, pois apresenta hipóteses em que a implementação de sistemas de IA são vedadas – gerando a interpretação de que sistemas de IA de risco excessivo são os que se enquadram nas hipóteses elencadas no artigo, sendo, consequentemente, vedados.

Dessa forma, soa estranho atribuir responsabilidade, nesta seção, por algo que parece vedado.

- **Art. 27. § 2º:**

No Relatório, por exemplo, há a diferenciação entre responsabilidade objetiva do operador e fornecedor. A responsabilidade objetiva do fornecedor é apresentada da seguinte forma:

“[13] Strict liability of the producer should play a key role in indemnifying damage caused by defective products and their components, irrespective of whether they take a tangible or a digital form. [14] The producer should be strictly liable for defects in emerging digital technologies even if said defects appear after the product was put into circulation, as long as the producer was still in control of updates to, or upgrades on, the technology. A development risk defence should not apply” (p.42)

No Relatório, também há a distinção de operador de *frontend* e *backend*, distinção que interfere no grau de responsabilidade:

“If there are two or more operators, in particular: (a) the person primarily deciding on and benefitting from the use of the relevant technology (frontend operator) and (b) the person continuously defining the features of the relevant technology and providing essential and ongoing backend support (backend operator), strict liability should lie

---

<sup>7</sup> Disponível em: [https://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report\\_EN.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf). Acesso em: 17.10.2023.



with the one who has more control over the risks of the operation. strict liability should lie with the one who has more control over the risks of the operation.” (p. 39)

Com relação ao ônus da prova, a LGPD determina que a inversão somente poderá ocorrer quando o juiz entender que a alegação do titular de dados for verossímil, quando houver hipossuficiência para fins de produção de prova ou quando a produção de provas for excessivamente onerosa para o titular. Entendemos que a hipossuficiência não se aplicaria aqui, em razão da dificuldade técnica da produção da prova, mas a verossimilhança seria um critério adequado.

- **Art. 28<sup>8</sup>**

No mesmo sentido do item anterior, considerando a sugestão de mudança de redação do caput, nossa sugestão é a seguinte:

“Art. 28. Não haverá responsabilização quando: II – os agentes de inteligência artificial comprovarem que o dano é decorrente de fato exclusivo da vítima ou de terceiro, assim como de caso fortuito externo;”

Não há atribuição de deveres de cuidado, diferentemente do que ocorre, por exemplo, na LGPD (Art. 43 e 44), que inclui, entre outras responsabilidades, a adoção de medidas de segurança. Para referência, a sugestão do Relatório da *European Commission*:

“[16] Operators of emerging digital technologies should have to comply with an adapted range of duties of care, including with regard to (a) choosing the right system for the right task and skills; (b) monitoring the system; and (c) maintaining the system. [17] Producers, whether or not they incidentally also act as operators within the meaning of [10], should have to: (a) design, describe and market products in a way effectively enabling operators to comply with the duties under [16]; and (b) adequately monitor the product after putting it into circulation.” (p. 44)

---

<sup>8</sup> Art. 28. Os agentes de inteligência artificial não serão responsabilizados quando: (...) ou II – comprovarem que o dano é decorrente de fato exclusivo da vítima ou de terceiro, assim como de caso fortuito externo.

## ANEXO 1 – COMPARATIVO DOS MODELOS REGULATÓRIOS EM OUTROS PAÍSES

	PROPOSTA ANALISADA	TIPO DE INICIATIVA	ENFORCEMENT	PRINCIPAIS DESTINATÁRIOS DA PROPOSTA	CRIAÇÃO DE DIREITOS
UE	AI ACT	Legislativa  "While the European Commission initially adopted a soft-law approach, with the publication of its non-binding 2019 Ethics Guidelines for Trustworthy AI and Policy and investment recommendations, it has since shifted towards a legislative approach, calling for the adoption of harmonised rules for the development, placing on the market and use of AI systems." (briefing, p. 2)	<p>The proposal requires Member States to designate one or more competent authorities, including a <b>national supervisory authority</b>, which would be tasked with supervising the application and implementation of the regulation, and establishes a <b>European Artificial Intelligence Board</b> (composed of representatives from the Member States and the Commission) at EU level. 6National market surveillance authorities would be responsible for assessing operators' compliance with the obligations and requirements for high-risk AI systems. They would have access to confidential information (including the source code of the AI systems) and subject to binding confidentiality obligations. Furthermore, they would be required to take any <b>corrective measures</b> to prohibit, restrict, withdraw or recall AI systems that do not comply with the AI act, or that, although compliant, present a risk to health or safety of persons or to fundamental rights or other public interest protection.</p> <p>Administrative <b>fin</b>es of varying scales (up to €30 million or 6 % of the total worldwide annual turnover), depending on the severity of the infringement, are set as sanctions for non-compliance with the AI act. Member States would need to lay down rules on penalties, including administrative fines and take all measures necessary to ensure that they are properly and effectively enforced. (briefing, p. 6, grifos no original)</p> <p>Ebers and others stress that the AI act <b>lacks effective enforcement structures</b>, as the Commission proposes to leave the preliminary risk assessment, including the qualification as high-risk, to the providers' self-assessment. They also raise concerns about the excessive delegation of regulatory power to private European standardisation organisations (ESOs), due to the lack of democratic oversight, the impossibility for stakeholders (civil society organisations, consumer associations) to influence the development of standards, and the lack of judicial means to control them once they have been adopted. Instead, they recommend that the AI act codifies a set of legally binding requirements for high-risk AI systems (e.g. prohibited forms of algorithmic discrimination), which ESOs may specify through harmonised standards. Furthermore, they advocate that European policymakers should <b>strengthen democratic oversight of the standardisation process</b>.</p> <p><i>Commentators deplore a crucial gap in the AI act, which does not provide for individual enforcement rights. Ebers and others stress that individuals affected by AI systems and civil rights organisations have no right to complain to market surveillance authorities</i></p>	<p>"The new rules would apply primarily to <b>providers of AI systems established within the EU or in a third country</b> placing AI systems on the EU market or putting them into service in the EU, as well as <b>to users of AI systems located in the EU</b>. To prevent circumvention of the regulation, the new rules would also apply to providers and users of AI systems located in a third country where the output produced by those systems is used in the EU. However, the draft regulation does not apply to AI systems developed or used exclusively for military purposes, to public authorities in a third country, nor to international organisations, or authorities using AI systems in the framework of international agreements for law enforcement and judicial cooperation.</p> <p>" (briefing, p. 3, grifos no original)</p>	Não há criação de novos direitos. O AI Act prevê apenas a proteção dos direitos fundamentais e de outros direitos já existentes na UE.

			<p>or to sue a provider or user for failure to comply with the requirements. Similarly, Veale and Zuiderveen Borgesius warn that, while some provisions of the draft legislation aim to impose obligations on AI systems users, there is <b>no mechanism for complaint or judicial redress</b> available to them. Smuha and others <b>recommend amending the proposal to include, inter alia, an explicit right of redress for individuals and rights of consultation and participation for EU citizens</b> regarding the decision to amend the list of high-risk systems in Annex III.</p> <p>It has also been stressed that the text as it stands <b>lacks proper coordination mechanisms</b> between authorities, in particular <b>concerning cross-border infringement</b>. Consequently, the competence of the relevant authorities at national level should be clarified.</p> <p>Furthermore, guidance would be desirable on how to ensure compliance with transparency and information requirements, while simultaneously <b>protecting intellectual property rights and trade secrets</b> (e.g. to what extent the source code must be disclosed), not least to avoid diverging practices in the Member States. (p. 9)</p>		
EUA	<p><a href="#">Artificial Intelligence Risk Management Framework (AI RMF 1.0)</a></p>	<p>Framework de parâmetros sugestivos.</p> <p>É destinado a uso voluntário e busca melhorar a capacidade de incorporar considerações de confiabilidade no design, desenvolvimento, uso e avaliação de produtos, serviços e sistemas de IA, para que os atores que projetam, desenvolvem, implementam ou utilizam sistemas de IA possam gerenciar os riscos e promover um uso confiável da tecnologia.</p>	<p>Como a proposta se trata de um framework não-vinculante, não há uma proposta de enforcement no sentido de um órgão ou entidade supervisora e fiscalizadora da implementação das recomendações do guia. No entanto, em 30 de março, o NITS lançou o Centro de Recursos de IA Confiável e Responsável para "facilitar a implementação e o alinhamento internacional com o AI RMF". Assim, embora o compliance com o disposto no framework seja voluntário, pode-se dizer que há uma entidade centralizada para auxiliar em sua implementação.</p>	<p>Reconhecendo que há uma variedade de atores com uma diversidade de expertise e origens, compostos por equipes demograficamente e disciplinarmente diversas, o AI RMF destina-se a ser utilizado por atores de IA ao longo do ciclo de vida da IA e em suas diferentes dimensões. (p. 9)</p> <p>As dimensões da IA consideradas são: Contexto de Aplicação, Dados e Entrada, Modelo de IA e Tarefa e Saída. Os atores de IA envolvidos nessas dimensões, que realizam ou gerenciam o design, desenvolvimento, implementação, avaliação e uso de sistemas de IA e impulsionam os esforços de gerenciamento de riscos de IA, são o público principal do AI RMF.</p> <p>Há também uma quinta dimensão intitulada "Pessoas e Planeta", que representa os direitos humanos e o bem-estar mais amplo da sociedade e do planeta. Os atores de IA nessa dimensão compõem um público separado do AI RMF que informa o público principal. Esses atores de IA podem incluir associações comerciais, organizações de desenvolvimento de padrões, pesquisadores, grupos de defesa, grupos ambientais, organizações da sociedade civil,</p>	<p>Não há criação de direitos, mas objetiva a preservação de direitos existentes.</p> <p>"O Framework é destinado a ser voluntário, <b>preservador de direitos</b>, não específico do setor e agnóstico quanto ao caso de uso, proporcionando flexibilidade para organizações de todos os tamanhos e em todos os setores e ao longo de toda a sociedade para implementar as abordagens no Framework." (p. 2)</p>

				usuários finais e indivíduos e comunidades potencialmente impactados.	
<b>Reino Unido</b>	The governance of artificial intelligence: interim report – Report Summary	Principiológica	<p>A proposta inicial do governo do Reino Unido assume a forma de um white paper que se propõe como uma abordagem pró-inovação à regulamentação da IA. Através dessa proposta, busca-se garantir que as medidas regulatórias sejam proporcionais ao contexto e aos resultados, concentrando-se no uso do IA e não na tecnologia em si. Dessa forma, são estabelecidos princípios que devem ser interpretados e traduzidos em ações pelos reguladores setoriais de forma individual, ainda que com a assistência de funções centrais, que seriam asseguradas inicialmente pelo governo. Tendo em vista o tempo necessário para a criação de novos organismos reguladores, a adoção setorial é apontada como ponto de partida. Nesse sentido, o relatório aponta que diversos reguladores já estão empenhados em engajar-se nas implicações da IA para as suas competências. Assim, ainda que se reconheça a necessidade de estabelecer novos órgãos regulatórios e funções de suporte central, o relatório aponta que a estruturação da regulamentação propriamente dita requer maior desenvolvimento e consideração em documentos legislativos e regulatórios subsequentes.</p> <p>Além disso, no white book, o governo sinalizou que poderá legislar de modo a estabelecer deveres de due regard para as entidades reguladoras existentes, o que sugere que deve haver um projeto de lei sobre IA direcionado na nova sessão do parlamento.</p>	Poder público, tendo em vista que a proposta se concentra em estabelecer princípios para a atividade regulatória.	A proposta não parece criar novos direitos, mas sim estabelecer uma estrutura regulatória e de governança para a inteligência artificial que incentive a inovação a partir de princípios. Qualquer impacto nos direitos das partes interessadas provavelmente seria abordado em documentos legislativos e regulatórios subsequentes.
<b>Japão</b>	Social Principles of Human-Centric AI (Social Principles); METI's Governance Guidelines for Implementation of AI Principles; METI's Contract Guidelines on Utilization of AI and Data; METI's AI Governance in Japan Ver. 1.1	Principiológica	<p>De acordo com o relatório AI Governance in Japan Ver. 1.1 publicado pelo Ministério da Economia, Comércio e Indústria (METI) em julho de 2021, que descreve a política regulatória de IA do Japão, "requisitos horizontais legalmente vinculativos para sistemas de IA são considerados desnecessários no momento". Essa constatação decorre do entendimento de que regulamentações enfrentam dificuldades para acompanhar a velocidade e complexidade da inovação em IA, de forma que uma regulamentação prescritiva, estática e detalhada neste contexto poderia sufocar a inovação. Portanto, o relatório do METI conclui que, nesse momento, o governo deve respeitar os esforços voluntários das empresas para a governança de IA, fornecendo orientações não vinculativas para apoiar ou orientar esses esforços.</p> <p>Neste contexto, a abordagem regulatória de IA no Japão baseia-se principalmente em guidelines para a aplicação de princípios para ajudar as empresas a implementarem voluntariamente medidas apropriadas de governança de IA.</p> <p>Em 2019, o governo japonês publicou os Princípios Sociais da Inteligência Artificial Centrada no Ser Humano (Princípios Sociais), guiados por três objetivos iniciais que devem nortear a implementação de IA na sociedade: dignidade humana, diversidade e inclusão, e sustentabilidade. Para alcançar esses objetivos, os Princípios Sociais estabelecem sete princípios em torno da IA: (1) centralização no ser humano; (2) educação/alfabetização; (3) proteção da privacidade; (4) garantia de segurança; (5)</p>	Setor privado - na medida que estabelece princípios norteadores no desenvolvimento de projetos de inteligência artificial	A proposta não cria direito, mas tão somente orienta princípios que devem nortear - ainda que de maneira voluntária - a implementação de IA por empresas

			<p>competição justa; (6) justiça, responsabilidade e transparência; e (7) inovação.</p> <p>A fim de orientar a aplicação desses princípios em projetos de IA, as Diretrizes de Governança do METI para Implementação dos Princípios de IA buscam guiar o uso dos Princípios com exemplos específicos. Ainda, para promover contratos justos para o desenvolvimento de IA e transferência de dados, o METI também as Diretrizes de Contrato sobre Utilização de IA e Dados. Essas diretrizes explicam questões legais chave ao entrar em contratos para transferência de dados ou desenvolvimento de IA incluindo cláusulas-modelo para referência.</p> <p>Por fim, de maneira mais abrangente, várias diretrizes foram publicadas para a proteção e utilização de dados com relação à IA. O Guia de Governança Corporativa para Privacidade na Transformação Digital e o Guia para Utilização de Imagens de Câmera, ambos desenvolvidos em conjunto pelo METI e pelo Ministério dos Assuntos Internos e Comunicações (MIC), fornecem orientações sobre como lidar com dados de privacidade, não apenas em conformidade com a APPI (lei de proteção de dados do Japão), mas também tomando medidas apropriadas com base na comunicação com as partes interessadas.</p> <p>Para além de diretrizes não-mandatórias, o Japão tem buscado adaptar sua legislação à implementação de IA em diferentes frentes legais. A exemplo, em 2020, a Lei de Tráfego Rodoviário revisada e a Lei de Veículos de Transporte Rodoviário entraram em vigor, permitindo a condução automatizada de Nível 3 (ou seja, automação condicional) em vias públicas. No setor financeiro, a Lei de Vendas a Prazo foi revisada em 2020 para permitir que um "intermediário certificado de compra de crédito abrangente" determinasse os valores de crédito usando dados e IA. Por fim, a Lei de Direitos Autorais também foi alterada em 2017 para promover o uso de dados em aprendizado de máquina: a emenda esclareceu que o download ou processamento de dados pela internet ou outros meios para desenvolver modelos de IA não constitui uma violação de direitos autorais.</p>		
Coréia do Sul	AI	National Strategy for	<p>Até 2030 a Coreia do Sul pretende: (i) aprimorar a infraestrutura de IA; (ii) garantir a competitividade em IA; (iii) promover uma inovação regulatória drástica; (iv) revisar leis e (v) nutrir startups, visando alcançar a liderança no ecossistema global de IA.</p> <p>O país também visa o melhor uso de IA e, para isso quer: (i) nutrir e formar os melhores talentos de IA do mundo; (ii) difundir a IA em todas as áreas da indústria e; (iii) construir um governo digital.</p> <p>Por fim, no aspecto social, a Coreia busca a harmonia e coexistência com a IA e, para isso deve: (i) estabelecer uma rede inclusiva de segurança no trabalho e; (ii) prevenir disfunções, estabelecendo o uso ético de IA.</p> <p>Do ponto de vista regulatório, a mentalidade sul coreana é a de “aprovar primeiro e regular depois”. Assim, a proposta é: (i) uma legislação flexível e (ii) sandbox</p>	Poder público	<p>A estratégia nacional não pretende criar novos direitos. Mas, sim estabelecer o desenvolvimento e implementação de IA através de uma legislação flexível e do sandbox regulatório; baseados no princípio de</p>



			<p>regulatório, um sistema que viabilize o desenvolvimento e uso de IA no mercado, apesar da existência leis e regulamentos potencialmente impeditivos, nos casos em que as novas tecnologias não prejudiquem a vida e segurança das pessoas.</p> <p>Além disso, o documento aponta quais seriam os principais conteúdos de uma legislação para IA:</p> <p>(i) princípios - foco no desenvolvimento nacional e social, através do compartilhamento de benefícios e oportunidades do crescimento econômico de forma abrangente;</p> <p>(ii) estabelecer uma base para informatização inteligente – através no investimento em indústrias deste setor e apoio no desenvolvimento tecnológico, apoio para industrialização e comercialização e regulamentação de políticas de dados;</p> <p>(iii) Combate a medidas contra a mudança laboral – disposições obrigatórias que exigem que o governo estabeleça contramedidas de combate a mudanças no ambiente de trabalho e emprego;</p> <p>(iv) Padrões éticos – novas normas éticas, prevenção à violação de informações pessoais e privacidade;</p> <p>(v) Medidas de proteção mínima – Estabelecimento de medidas mínimas de proteção (kill switches) para garantir a segurança e confiabilidade para cada nova tecnologia e serviço.</p>		"aprovar primeiro e regular depois".
China	<a href="#">Regulation for Generative Artificial Intelligence Services proposta legislativa</a>	Legislativa			