Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

4 de Outubro de 2022

Dez recomendações prioritárias do CIPL para a regulação de IA no Brasil

I. Introdução

Os benefícios da inteligência artificial (IA) para abordar uma vasta série de mudanças sociais e melhorar nosso modo de vida são inegáveis. Ao possibilitar um conjunto de tecnologias emergentes (incluindo aprendizado de máquinas, visão computacional e processamento de linguagem natural), a IA capacita organizações dos setores público e privado a oferecerem melhores serviços em uma infinidade de áreas, incluindo assistência de saúde, no setor automotivo, na agricultura, no campo militar, nos serviços financeiros, no cumprimento e implementação de leis, na educação e marketing. Vinte e cinco por cento das grandes empresas no Brasil já estão usando IA[i], e um estudo de 2021 da Embrapii, grupo brasileiro de pesquisa e inovação industrial, revelou que 76% das empresas acreditam que o uso de ferramentas de IA terá um grande impacto em sua competitividade[ii]. De acordo com um relatório da Associação Brasileira das Empresas de Software (ABES) e da International Data Corporation (IDC), espera-se que os gastos com IA no Brasil aumentem em 28% em 2022, em US$ 504 milhões[iii]. Além disso, o uso de tecnologia da IA apresenta muitas oportunidades para pequenas e médias empresas.

Embora o progresso acelerado da tecnologia de IA tenha resultado em inúmeros benefícios para a sociedade e impulsionado o crescimento dos negócios, também criou preocupações com relação a uma variedade de riscos e potenciais desafios legais, éticos e sociais. Um dos desafios potenciais enfrentados pelas organizações é como garantir o uso responsável e a prestação de contas (*accountability*) da tecnologia de IA e equilibrar esse uso com preocupações relacionadas à proteção de dados e ao direito dos indivíduos à privacidade. O Centre for Information Policy Leadership (Centro de Liderança em Políticas de Informação - CIPL)[iv] tem trabalhado na questão de uma IA responsável por muitos anos e tem se engajado com formuladores de leis e de políticas, bem como com departamentos governamentais e autoridades de proteção de dados no desenvolvimento de uma estrutura sensata e pronta para o futuro, de modo a propiciar uma IA pautada pela responsabilidade e prestação de contas (em inglês, accountability). O CIPL saúda o Senado Federal do Brasil pela criação de uma comissão especial de juristas (a "Comissão do Senado") para considerar uma estrutura apropriada para regular a IA no Brasil. Para auxiliar a Comissão do Senado nesse esforço, o CIPL apresenta este documento a fim de indicar as suas principais recomendações para a regulamentação da IA no Brasil. Estas recomendações são baseadas na experiência internacional do CIPL na área de política e regulamentação de IA[v], bem como em seu trabalho anterior sobre questões de IA no Brasil.[vi]

II. Recomendações Principais

1. Regime de IA flexível e adaptável

O regime de IA do Brasil deve ser projetado de forma a permitir que ele evolua e seja flexível às mudanças no ecossistema de IA. A IA está em constante desenvolvimento e um regime excessivamente prescritivo ou inflexível corre o risco de criar uma estrutura que ou se tornará rapidamente desatualizada ou inibirá a inovação. O Brasil pode criar um regime tecnologicamente agnóstico e preparado para o futuro, regulando apenas as questões e riscos principais da IA e possibilitando uma IA responsável através de um conjunto de outras ferramentas, conforme descrito nestas recomendações. De fato, tal abordagem é consistente com a Estratégia Brasileira de Inteligência Artificial (EBIA) de 2021, que recomenda evitar ações regulatórias que possam limitar desnecessariamente a inovação, a adoção e o desenvolvimento da IA.[vii]

2. Regime baseado em estruturas legais existentes

Ao construir um regime de IA, o Brasil deve se basear nas estruturas legais existentes e evitar duplicar ou criar quaisquer exigências conflitantes com essas estruturas. Por exemplo, certos aspectos da IA já são regulados pela Lei Geral de Proteção de Dados (LGPD),[viii], pelo Marco Civil da Internet,[ix] pelo Código de Defesa do Consumidor[x] e pela Lei de Acesso à Informação.[xi] Exigências redundantes ou conflitantes com esses regimes podem resultar em proteções incongruentes para os indivíduos e incertezas no que diz respeito a seus direitos. Também podem criar incerteza regulatória tanto para as entidades reguladas quanto para os reguladores, assim como obrigações de conformidade dispendiosas e desnecessárias para as organizações.

3. Abordagem regulatória baseada em princípios e resultados, e que permita a responsabilização e a prestação de contas por parte das organizações (accountability)

Para garantir o sucesso a longo prazo de seu regime de IA, o Brasil deve adotar uma abordagem regulatória baseada em princípios e resultados que permita a responsabilização e a prestação de contas pelas organizações. Regras baseadas em princípios prescrevem os resultados que as organizações devem alcançar, mas deixam a critério das organizações a forma de se alcançarem tais resultados. A responsabilização e a prestação de contas exigem que as organizações operacionalizem e traduzam essas regras baseadas em princípios através de políticas, procedimentos, controles e governança apropriados e demonstráveis para garantir a sua conformidade. A prestação de contas também permite a adaptação de regras baseadas em princípios a setores específicos, aplicações tecnológicas e diferentes níveis de risco.

O regime brasileiro de IA deve incluir explicitamente uma obrigação de prestação de contas para garantir que as organizações que desenvolvem e implantam tecnologias de IA o façam de forma responsável. A implementação da prestação de contas é uma alternativa mais eficaz do que exigências legais rígidas e prescritivas que englobem todas as aplicações IA, independentemente do risco envolvido. A prestação de contas/responsabilização (*accountability*) já é reconhecida globalmente como um elemento-chave para uma regulamentação eficaz e garantia de conformidade corporativa. Ela tornou-se o foco central de muitos regimes regulatórios, incluindo proteção de dados e privacidade, anticorrupção, lavagem de dinheiro, crimes de colarinho branco e fraude corporativa, controles e sanções de exportação e assistência de saúde. Da mesma forma, no contexto da IA, as obrigações de prestação de contas podem permitir a inovação responsável em matéria de IA, promover a confiança no ecossistema de IA e facilitar a coleta e o uso responsável de dados para treinamento, desenvolvimento e implantação de IA. No Brasil, a prestação de contas é um princípio chave da proteção de dados à luz da LGPD[xii] , e a abordagem da prestação de contas sob esse regime poderia servir como fonte de inspiração, já que o Brasil trabalha na direção de uma estrutura de IA responsável.

É importante entender quais são os elementos da prestação de contas, pois programas de IA responsável devem ser baseados nesses elementos. Há diferentes abordagens para se fracionar a prestação de contas/responsabilização em suas partes constituintes. Uma abordagem que está ganhando força entre organizações e reguladores é o uso de uma estrutura de responsabilização, tal como a estrutura criada pelo CIPL (veja abaixo). Os elementos dentro da Estrutura de Responsabilização do CIPL são extraídos de elementos de responsabilização similares de outras áreas regulatórias (ver acima), o que a torna agnóstica em termos de lei e, também, aplicável ao contexto de IA. O regime de IA do Brasil pode estabelecer os

elementos específicos e os resultados esperados da prestação de contas, ou a Autoridade Nacional de Proteção de Dados (ANPD) ou outro órgão regulador apropriado pode aperfeiçoar os elementos de prestação de contas na orientação regulatória para guiar as organizações à medida em que estas constroem programas de IA no Brasil baseados na prestação de contas.

Elemento de prestação de contas	Descrição
Liderança e Supervisão	**Estabelecer liderança e supervisão para o uso responsável de IA**, incluindo governança, relatórios, adesão de todos os níveis de administração e nomeação de pessoal apropriado para supervisionar o programa de prestação de contas em IA da organização e relatar à administração e à diretoria.
Avaliação de risco	**Avaliar e mitigar os riscos** que as aplicações de IA podem representar para os indivíduos, incluindo a ponderação do risco do uso de IA em relação a seus benefícios.
Políticas e Procedimentos	**Estabelecer políticas e procedimentos internos escritos de IA** que operacionalizem as exigências legais e criem processos e controles concretos a serem seguidos pela organização, refletindo os riscos identificados, a lei aplicável, regulamentos, padrões do setor, bem como os valores e objetivos da organização.
Transparência	**Proporcionar transparência às partes interessadas interna e externamente** sobre as práticas de IA da organização, os direitos dos indivíduos em relação a seus dados e os benefícios e/ou riscos potenciais das aplicações de IA. Isto também pode incluir a comunicação com as autoridades reguladoras relevantes, parceiros comerciais e terceiros sobre as práticas de IA da organização. É importante ressaltar que proporcionar transparência efetiva no contexto de IA depende da natureza da audiência envolvida, que informará o nível de detalhamento e o tipo de informação a ser fornecida.[xiii]
Treinamento e Conscientização	**Oferecer treinamento aos funcionários** para assegurar o conhecimento das práticas de IA da organização. Isso assegura que a responsabilização pela IA esteja inserida na cultura da organização.
Monitoramento e Verificação	**Monitoramento e verificação (inclusive na fase de testes pré-mobilização de determinadas aplicações de IA) da implementação e eficácia do programa de responsabilização de IA e da conformidade interna** com as práticas e controles de IA da organização através de auditorias internas ou externas regulares e planos de correção.
Resposta e Aplicação da Lei	**Implementar procedimentos de resposta e aplicação** para tratar de inquéritos, reclamações e não conformidade interna e para fazer cumprir ações contra atos de não conformidade relativos ao programa de prestação de contas de IA da organização.

Figura 1 – Estrutura de Responsabilização do CIPL - Elementos Universais de Prestação de Contas

4. Abordagem baseada em risco que considere riscos e benefícios de aplicações de IA de maneira holística

A abordagem baseada em risco para regular a IA é crucial para um regime de IA baseado em princípios e em resultados robustos. O foco de tal abordagem avalia o risco do impacto da tecnologia de IA no contexto de usos e aplicações específicas, em vez do risco da tecnologia de modo abstrato. Compreender o impacto potencial e qualquer risco de danos de uma aplicação específica de IA sobre os indivíduos permite que as organizações tomem decisões baseadas no risco e implementem controles e estratégias de mitigação apropriadas para minimizar os riscos envolvidos em um projeto de IA. Ao concentrar-se nos impactos e riscos, as organizações podem determinar como alocar recursos e garantir que seja dada a devida atenção às aplicações de IA que apresentam maiores riscos. Por exemplo, o uso de IA para recomendar músicas ou filmes muito provavelmente exige menos escrutínio do que aplicações de IA usadas em carros para desviar de pedestres ou outros veículos, ou o uso de tecnologia de reconhecimento facial em aplicações comerciais. Além disso, o regime brasileiro de IA poderia fornecer critérios não exaustivos para ajudar as organizações a determinar se suas aplicações de IA representam um alto risco para os indivíduos. Uma estrutura de IA poderia delinear categorias, tipos e exemplos específicos de danos a indivíduos que deveriam ser considerados como parte de um processo de avaliação de impacto de IA. Além disso, para encorajar avaliações de risco e mitigação de riscos em aplicações de IA como medida de responsabilidade

e prestação de contas, o Brasil poderia considerar a elaboração de uma estrutura que exija requisitos mais rigorosos apenas para as aplicações de IA que possam causar impactos prejudiciais ou negativos sobre os indivíduos.
Qualquer exigência de avaliação de risco no regime de IA do Brasil deve incluir explicitamente a avaliação dos benefícios de uma proposta de aplicação de IA ou os riscos de não prosseguir com o desenvolvimento ou implantação da aplicação de IA em questão (risco de reticência). Isso é tão importante quanto focalizar os danos que podem resultar de se prosseguir com a aplicação de IA. Também ajuda a garantir que o uso de uma aplicação de IA seja proporcional aos resultados desejados. Por exemplo, pode haver altos riscos relacionados a um sistema de IA específico que pode ser anulado por benefícios atraentes para os indivíduos e a sociedade em geral. Por exemplo, a IA oferece enormes benefícios quando usada para monitorar o conteúdo em plataformas on-line a fim de combater a desinformação, o que poderia superar os riscos associados ao processamento de dados pessoais relevantes.

Após conduzir uma avaliação de risco para aplicações específicas de IA, as organizações podem descobrir que o nível de risco residual ainda é muito alto. Em tais casos, as organizações devem ter a possibilidade de consultar a ANPD ou outro órgão regulador setorial relevante em relação à aplicação, revisar o escopo do projeto de IA para reduzir os riscos ou abandonar o projeto e considerar alternativas. O regime brasileiro de IA deve deixar tais avaliações e determinações para as organizações, pois elas estarão melhor posicionadas para avaliar holisticamente os riscos envolvidos. Naturalmente, sob o princípio de responsabilização, as organizações devem ser capazes de demonstrar suas avaliações de risco e processo de tomada de decisão a pedido de um regulador apropriado para fins de fiscalização. Além disso, essa abordagem flexível garantirá que o regime de IA do Brasil possa ser aplicado universalmente a todas as aplicações de IA.

É possível observar uma tendência em algumas regiões, particularmente na UE, de proibir aplicações específicas de IA. Por exemplo, o uso do reconhecimento facial para aplicação da lei e vigilância ou o uso de IA para inferir emoções de uma pessoa física. Embora existam preocupações legítimas associadas ao uso de tais aplicações de IA, tais preocupações devem ser tratadas através do uso de avaliações de risco e caso a caso. Há circunstâncias em que uma proibição direta do uso de IA para inferir emoções impediria, por exemplo, o uso de IA para detectar se um indivíduo é suicida e para permitir uma resposta e intervenção apropriada de modo a evitar que o indivíduo prejudique a si mesmo ou outros. Os benefícios desse uso de IA podem superar os riscos e devem ser potencialmente permitidos, embora sob condições e salvaguardas rigorosas. Ao mesmo tempo, o uso de IA para inferir emoções de indivíduos para manipulá-los ou coagir comportamentos específicos, que de outra forma eles não assumiriam, poderia ser completamente inapropriado e acarretar riscos muito altos e não deveria ser permitido. Cada uma dessas aplicações deve ser submetida a uma avaliação de risco e, dependendo dos resultados, pode ser conduzida uma determinação quanto a se proceder ou não com a aplicação de IA proposta. Sendo assim, com exceção das aplicações de IA categoricamente prejudiciais e nefastas que potencialmente justifiquem a proibição, o Brasil no geral deve evitar a proibição de qualquer aplicação específica de IA sob seu regime de IA. Naturalmente, sempre pode haver alguns maus atores que prosseguirão com usos deletérios de IA, mas uma proibição legislativa direta não irá deter esses maus atores. Entretanto, isso certamente impediria usos potencialmente benéficos de IA.

5. Regime que incentive o desenvolvimento e implementação de práticas responsáveis de IA, incluindo soluções tecnológicas e Tecnologias de Melhoria/Incremento da Privacidade

Como mencionado acima, a prestação de contas permite a flexibilidade necessária para que as organizações alcancem a conformidade através de controles e práticas baseados em riscos, verificáveis e aplicáveis. A prestação de contas em IA pode ser alcançada através de uma variedade de mecanismos, o que é particularmente importante já que muitas organizações diferentes estão inovando no campo de IA, desde grandes empresas multinacionais até PMEs e start-ups, passando por instituições públicas de pesquisa e acadêmicas, entidades governamentais e outros órgãos do setor público. Tais mecanismos incluem políticas, programas e controles internos feitos sob medida para o tamanho, estrutura e atividades de processamento de dados da empresa. Eles também poderiam incluir esquemas formais de responsabilização e garantia, tais como códigos de conduta, certificações e normas aplicáveis (veja abaixo para mais informações sobre tais esquemas formais de responsabilização). Finalmente, as empresas líderes que desenvolvem tecnologias de IA também estão investindo cada vez mais em tecnologias de melhoria/incremento da privacidade (ou PETs no acrônimo em inglês para privacy-enhancing technologies), incluindo aprendizagem federada, privacidade diferencial, uso de dados sintéticos ou criptografados para treinamento algorítmico etc.

Qualquer regime que regulamente a IA no Brasil deve incentivar o desenvolvimento e implementação de práticas de IA responsáveis e soluções tecnológicas para tratar de privacidade e outras preocupações no desenvolvimento e implementação de sistemas de IA. As organizações devem ser encorajadas a adotar tais práticas para permitir a inovação responsável em IA, ao mesmo tempo em que asseguram a conformidade com eventual regime de IA e proteções apropriadas para os indivíduos. Nos últimos anos, o CIPL tem coletado exemplos de tais práticas responsáveis de IA em linha com os elementos da Estrutura de Responsabilização do CIPL. O CIPL fornece uma tabela dessas práticas no final deste documento (ver Anexo 1). O CIPL não recomenda, porém, que nenhuma dessas práticas em particular seja tornada obrigatória diretamente por uma lei de IA, pois as organizações precisarão fazer determinações baseadas em risco sobre quais medidas de responsabilização seriam apropriadas em um determinado contexto de IA. Naturalmente, a ANPD e outros reguladores apropriados podem exemplificar em orientações regulatórias os exemplos dessas melhores práticas, incluindo práticas adicionais que se desenvolvem ao longo do tempo no Brasil e globalmente, para ajudar as organizações a fazer as escolhas apropriadas. Finalmente, o CIPL embarcará em um projeto para mapear e analisar as PETs mais prevalentes e promissoras e se engajará em discussões globais com reguladores e setores econômicos para assegurar uma adoção e compreensão mais ampla do potencial de tais tecnologias.

6. Cooperação regulatória e interpretação consistente das regras de IA

Estão ocorrendo globalmente muitas discussões sobre qual órgão ou órgãos reguladores deveriam ser responsáveis pela IA. No Brasil, a ANPD terá um grande papel a desempenhar, já que muitas aplicações de IA envolvem o uso de dados pessoais. Além disso, o uso de IA é predominante em muitos setores da indústria, tais como saúde e serviços financeiros, e os reguladores setoriais também terão interesse em supervisionar a regulamentação de IA no Brasil. Algumas nações consideraram o estabelecimento de um órgão regulador dedicado à IA. O CIPL é de opinião que a supervisão e aplicação de IA no Brasil deve ser realizada pelos reguladores existentes, incluindo a ANPD, e tais reguladores devem trabalhar em conjunto através de um centro coordenador ou outro fórum de cooperação (semelhante ao Fórum de Cooperação em Regulamentação Digital do Reino Unido[xiv]) para assegurar uma interpretação consistente das regras,

supervisão e aplicação da IA. Alavancar a experiência e as competências das agências reguladoras existentes e evitar uma abordagem regulatória fragmentada através da coordenação regulatória é fundamental para o sucesso de qualquer regime de IA no Brasil.

7. Mecanismos de co-regulação que permitam a inovação responsável em IA

Os reguladores são encarregados de executar uma infinidade de tarefas sob condições de recursos limitados. Mecanismos de co-regulação, tais como estruturas de garantia de IA, certificações, códigos de conduta e normas poderiam ajudar a aliviar algumas das pressões que os reguladores podem enfrentar na execução de suas tarefas existentes adicionadas a um novo regime de IA no Brasil. Tais mecanismos de co-regulação estão começando a proliferar nos mercados globais de IA. Estes incluem o UK Centre for Data Ethics and Innovation (CDEI) AI Assurance Framework[xv], o New South Wales AI Assurance Framework[xvi], o NIST AI Risk Management Framework do Departamento de Comércio dos EUA[xvii], o código de conduta para sistemas de inteligência artificial do Serviço Nacional de Saúde do Reino Unido (NHS) [xviii] e as normas ISO e IEEE para inteligência artificial[xix].

Os esquemas de certificação e códigos de conduta envolvem o uso de certificadores ou órgãos de monitoramento de terceiras partes, bem como provedores de resolução de disputas que estão associados a tais esquemas. Essas entidades podem desempenhar importantes funções de fiscalização e supervisão na linha de frente e corrigir muitas questões antes que um regulador precise intervir. Essas entidades revisam os programas de conformidade e responsabilização de organizações e asseguram que elas cumpram com o padrão relevante no qual foram certificadas. Quando necessário, elas podem suspender certificações e tomar outras medidas corretivas contra organizações não conformes. As funções de resolução de disputas desses esquemas aliviam os reguladores do fardo de lidar com um grande número de casos "fáceis", permitindo que eles concentrem sua atenção de fiscalização em assuntos mais importantes e estratégicos.

Os padrões de IA podem ajudar a estabelecer requisitos básicos para certos usos de IA que podem ser modificados e melhorados ao longo do tempo, à medida que o ecossistema de IA avança. Os padrões são frequentemente desenvolvidos em processos multissetoriais e podem ser melhor projetados através do envolvimento de uma ampla série de atores, em vez de deixar seu desenvolvimento apenas para os formuladores de políticas e legisladores. Assim como as certificações, os órgãos de normatização podem ajudar a garantir a adesão adequada às normas adotadas, o que pode resultar em um impulso em direção à uniformidade em inúmeros aspectos do ecossistema de IA. Além disso, mecanismos de co-regulação podem ajudar a aumentar a confiança ao demonstrar que uma aplicação de IA atende a certos critérios que foram estabelecidos por uma iniciativa transversal de especialistas relevantes do setor e/ou avaliados por um órgão independente.

8. Abordagem moderna de supervisão regulatória

Reguladores terão um papel importante a desempenhar para garantir a aplicação adequada de regras baseadas em princípios e estruturas de co-regulação. Eles também precisam manter-se atualizados sobre os desenvolvimentos da tecnologia de IA e suas mais recentes aplicações. Isso requer uma nova abordagem de supervisão regulatória, que difere de abordagens e comportamentos regulatórios tradicionais.

A fim de permitir a inovação e experimentação responsável em IA, o regime de IA do Brasil deve incentivar abordagens novas e ágeis na supervisão regulatória. Os reguladores precisam estar prontos e equipados com recursos e qualificações apropriados para engajarem-se construtivamente no tópico de IA com o setor e os órgãos governamentais que desenvolvem e utilizam a tecnologia.

Além disso, eles precisarão de ferramentas modernas e ágeis de supervisão regulatória, tais como sandboxes regulatórios, projetos de prototipagem de políticas e conselhos de revisão de dados, todos os quais desempenham um papel importante na caixa de ferramentas regulatórias de IA.

(a) Os sandboxes regulatórias de IA fornecem "espaços seguros" supervisionados para que as organizações testem produtos, serviços, projetos ou modelos comerciais inovadores de IA no mundo real com consumidores reais. Eles podem ser usados para ajudar a tratar e resolver alguns dos aspectos mais desafiadores da implantação de aplicações de IA contra o pano de fundo das exigências legais existentes, particularmente aquelas que parecem inconsistentes ou em tensão com novas tecnologias e práticas comerciais. Os sandboxes regulatórios oferecem uma oportunidade para organizações responsáveis e reguladores inovadores trabalharem e aprenderem juntos em um ambiente colaborativo para possibilitar os benefícios da IA e, ao mesmo tempo, garantir a proteção dos indivíduos. O Brasil já adotou os sandboxes nos setores de seguros[xx], bancos[xxi] e fintech[xxii]. O regime brasileiro de IA deve encorajar a ANPD ou outros reguladores apropriados a criar sandboxes regulatórios com o propósito de encorajar a inovação em IA e aprendizagem de máquinas. Tal abordagem foi proposta pela Índia em seu projeto de Lei de Proteção de Dados[xxiii] .Também temos visto esforços de autoridades de proteção de dados por lançar sandboxes para a IA. Por exemplo, em 2021, a Autoridade Norueguesa de Proteção de Dados (Datatilsynet) lançou um sandbox regulatório especial para aplicações de IA.[xxiv] Além disso, o governo colombiano desenvolveu um sandbox regulatório para promover o princípio da privacidade por desenho e por padrão (Privacy by Design and Default) em projetos de IA[xxv]. Finalmente, em Cingapura, a Infocomm Media Development Authority (Autoridade de Desenvolvimento Midiático Infocomm, IMDA) e a Personal Data Protection Commission (Comissão de Proteção de Dados Pessoais, PDPC) lançaram um sandbox para PETs a fim de apoiar empresas em projetos piloto de PET que abordam desafios comerciais comuns[xxvi].

(b) *Os programas de prototipagem de políticas* são projetos-piloto colaborativos que mobilizam uma coalizão de atores públicos e privados. Esses programas são também laboratórios de inovação regulatória destinados a permitir o desenvolvimento e teste de uma ideia de política/norma no campo das tecnologias novas e emergentes, incluindo a IA. Ao contrário dos sandboxes regulatórios que são projetados para testar inovações em relação às exigências regulamentares existentes, os programas de prototipagem de políticas permitem o teste de políticas que ainda não foram adotada. A ideia de política a ser testada pode ser inspirada por uma lei que está sendo discutida, um instrumento de autorregulamentação, um código de conduta, um conjunto de diretrizes do setor etc. Os programas de prototipagem de políticas também são programas empíricos que fornecem informações sobre políticas baseadas em evidências aos formuladores de políticas, seja para melhorar as estruturas de governança existentes ou para informar novas estruturas. Um exemplo de um projeto de prototipagem de políticas bem-sucedido no espaço de IA é o Projeto Open Loop[xxvii]. Os projetos de Open Loop foram implantados na Europa no contexto de avaliações de risco de IA e da abordagem política prevista na proposta de Lei de IA da UE e, em Cingapura e no México, sobre transparência e explicabilidade.

O processo de prototipagem de políticas normalmente envolve a seleção de um grupo de participantes (por exemplo, empresas de IA iniciantes) e a solicitação de que eles apliquem protótipos de políticas (estruturas normativas co-desenvolvidas sobre certos tópicos de IA, como explicabilidade, ou avaliação de risco) em aplicações específicas de IA que tais participantes construíram e estão implantando. Com base nessa aplicação, a organização que conduz o processo de prototipagem de políticas pode coletar informações sobre a experiência dos participantes e testar e avaliar os protótipos de política sob condições do mundo real. Essas estruturas podem ser melhoradas com base nas lições aprendidas e, em última instância, informar o debate regulatório de IA através de recomendações baseadas em evidências. O governo brasileiro pode considerar envolver-se em projetos de prototipagem de políticas para testar qualquer proposta de regras de IA no mercado antes de adotá-las em um regime de IA para o Brasil.

(c) *As comissões de análise de dados* (com acrônimo em inglês DRBs, para "Data review boards") são úteis tanto para organizações do setor público quanto privado. No contexto da IA, elas podem ser usadas para considerar os impactos de um determinado uso de dados em uma aplicação de IA antes de seu desenvolvimento, implantação ou uso. DRBs são comitês permanentes (cujas características podem ser definidas pelos reguladores) convocados de acordo com certos indicadores de risco. Eles se destinam a promover um diálogo ponderado entre uma organização e as principais partes interessadas que compõem o conselho de revisão de dados e a consideração dos riscos e benefícios em relação a projetos de IA de alto risco. As comissões de análise de dados podem incluir especialistas em proteção de dados, advogados, engenheiros, defensores de consumidores, acadêmicos e outras partes interessadas. As organizações podem estruturar seus DRBs de diferentes maneiras, dependendo dos objetivos para a própria DRB. Por exemplo, as DRBs internas podem ajudar as organizações a tomar decisões para minimizar os riscos envolvidos em determinados projetos de IA. As DRBs que recorrem à experiência de partes interessadas externas podem ser úteis para criar confiança e confiança de que o projeto de IA passou por um processo de revisão minucioso antes de ser implantado[xxviii]. O Brasil deve considerar incentivar o desenvolvimento e o uso de tais conselhos em qualquer regime de IA que desenvolva.

9. Responsabilidade

A responsabilidade por danos causados por sistemas e aplicações de IA é um tema complexo e que está sendo debatido atualmente no Brasil. Há uma série de diferentes atores envolvidos no desenvolvimento e implantação de IA, incluindo desenvolvedores, fornecedores e usuários. É importante lembrar que a maioria dos sistemas de IA não são desenvolvidos como um produto ou serviço independente que é lançado no mercado por uma única entidade. Muitas aplicações de IA são resultado de numerosas entidades que se baseiam em esforços mútuos. Por exemplo, um aplicativo de IA que emerge da comunidade de código aberto poderia ter sido o resultado dos esforços de centenas ou milhares de contribuintes.

A forma como a responsabilidade é repartida em razão de danos causados pelos sistemas e aplicações de IA é uma área ainda incipiente da lei. Tentativas anteriores no regime de IA proposto pela UE para repartir maior responsabilidade aos desenvolvedores de IA do que os usuários foram alvo de muitas críticas e agora foram minimizadas. Os desenvolvedores têm uma função importante a desempenhar para garantir o funcionamento adequado dos sistemas e algoritmos de IA. Entretanto, também cabe aos usuários

assegurar o uso adequado e apropriado do sistema para fins legais e de forma que não crie riscos e danos às pessoas e à sociedade. A responsabilidade é, portanto, distinta e compartilhada e ambas as partes precisam assegurar sua respectiva conformidade com quaisquer leis no desenvolvimento e uso de sistemas de IA. Ao mesmo tempo, a aplicação de responsabilidade objetiva a cada participante da cadeia de valor da IA frustraria os objetivos do Brasil de apoiar um ecossistema saudável de inovadores, experimentadores, contribuintes e empreendedores. Tal regime ensejaria responsabilidade de forma indiscriminada, sem levar em conta o nível de contribuição e os danos reais causados por cada ator ou sua capacidade de controlar e internalizar os riscos envolvidos em uma determinada aplicação de IA. Além disso, em muitos casos, os usuários de sistemas de IA determinam como esse sistema será implementado em um contexto específico de IA e caberá ao usuário assegurar que haja empreendido uma avaliação de risco e um exercício de mitigação específicos para minimizar qualquer falha no sistema e na aplicação de IA. Em outras palavras, os riscos específicos não podem em todos os casos ser mitigados pelas decisões dos desenvolvedores de um sistema de IA e, como tal, eles não devem ser considerados responsáveis em todos os casos do uso desse sistema.

Considerando que a responsabilidade por danos causados pela IA é território não testado e que não há experiência setorial e regulatória suficiente nessa área até o momento, o CIPL recomenda que o Brasil tenha cautela ao formular quaisquer regras sobre responsabilidade, incluindo como tal responsabilidade é repartida, por danos causados por sistemas e aplicações de IA nessa fase prematura. Além disso, deve haver um esforço concertado para monitorar os desenvolvimentos do mercado e para que os reguladores trabalhem com especialistas legais, profissionais e representantes de desenvolvedores de IA, fornecedores e usuários para se envolverem em discussões ponderadas sobre esse tópico, já que o uso de IA continua a proliferar no Brasil.

10. Processo de múltiplas partes interessadas na elaboração do regime de IA

Ao elaborar um regime de AI, o Brasil deve engajar-se em um processo multissetorial e consultar uma ampla variedade de partes interessadas sobre qualquer estrutura proposta para regulamentar a IA. Tal processo provou ter sucesso no desenvolvimento de outras estruturas legais no Brasil, incluindo o Marco Civil da Internet e a LGPD. Um processo de múltiplas partes interessadas deve incluir consulta a especialistas em ética, advogados e estudiosos de direito, cientistas de dados, engenheiros, especialistas em privacidade e segurança, cientistas de computação, epistemólogos, estatísticos, pesquisadores de IA, acadêmicos, sociedade civil, líderes empresariais e representantes públicos. A Comissão do Senado deve garantir que isso ocorra e interaja com todas as partes interessadas para se pensar sobre questões-chave. De fato, o CIPL saúda a Comissão do Senado por realizar uma série de audiências nacionais e um seminário internacional entre abril e junho de 2022. Ainda assim, o CIPL incentiva a Comissão do Senado a continuar a ter discussões semelhantes durante o restante de 2022 e em 2023, à medida em que avança em sua agenda.

III. CONCLUSÃO

O CIPL é grato pela oportunidade de oferecer contribuições à Comissão do Senado enquanto esta considera o desenvolvimento de uma estrutura apropriada para regular a IA no Brasil. Ao considerar e adotar as recomendações do CIPL apresentadas neste documento, o Brasil garantirá que criará uma estrutura em camadas para a IA que (1) permita um regime ágil, tecnologicamente agnóstico e preparado

para o futuro, baseado em normas e estruturas legais existentes; (2) estará baseada no risco e fundamentada na avaliação holística do impacto das aplicações de IA; (3) fomentará a inovação pautada por responsabilidade e prestação de contas; e (4) permitirá abordagens consistentes e modernas para a supervisão regulatória.

Se você quiser discutir este artigo ou solicitar mais informações, contacte Bojana Bellamy, bbellamy@HuntonAK.com ou Sam Grogan, sgrogan@HuntonAK.com.

Anexo 1 - Exemplos de Melhores Práticas de IA Responsável

A tabela a seguir apresenta exemplos de atividades de IA responsável realizadas por organizações selecionadas de diferentes setores, geografias e tamanhos com base na Estrutura de Responsabilização do CIPL, considerando a cada elemento de responsabilidade e prestação de contas. As práticas não representam padrões setoriais compulsórios, mas servem como exemplos específicos que são calibrados com base em riscos, contexto setorial, modelo de negócios, tamanho e nível de maturidade das organizações.

Elemento de responsabilidade e prestação de contas	**Práticas relacionadas**
Liderança e Supervisão	• Compromisso público desde a cúpula para respeitar ética, valores e princípios específicos no desenvolvimento de IA • Processos institucionalizados de IA e tomada de decisões • Regras do Código Interno de Ética • Conselhos e Comitês de Ética e Supervisão internos e externos para analisar casos de risco no uso de IA e melhorar continuamente práticas de IA • Nomeação de membro do Conselho de Administração para supervisão de IA • Nomeação de líder/oficial de IA responsável • Engenheiros e defensores de privacidade e de IA • Estabelecimento de um conselho interdisciplinar interno/grupo de trabalho sênior (envolvendo, por exemplo, jurídico, equipes técnicas, pesquisa, unidades de negócios, auditoria interna, licitações, time de assuntos públicos, liderança). • Nomeação de "líderes da privacidade" para coordenar o trabalho dos demais • Garantia de inclusão e diversidade no desenvolvimento de modelos de IA e na configuração de equipes de produtos de IA
Avaliação de Risco	• **Compreensão** do propósito e os casos de uso de IA em negócios/processos para a tomada de decisão, ou contribuição em decisões, ou outros • Compreensão do impacto (benefícios e riscos) sobre os indivíduos e a sociedade • Avaliação de Impacto Algorítmico / Ferramentas de viés algorítmico para identificar, monitorar e testar continuamente, incluindo dados sensíveis em conjuntos de dados para evitar enviesamento humano • Ferramentas de avaliação de imparcialidade para garantir que os vieses sejam testados, identificados e quaisquer anomalias sejam mitigadas para evitar o desvio de conceitos em algoritmos • Avaliação de Impacto Ético • Avaliação mais ampla de impacto em Direitos Humanos • Avaliação de impacto de proteção de dados para processamento de alto risco • Qualquer avaliação precisa considerar os benefícios comparados aos riscos da autonomia da IA de modo a definir se tal autonomia é necessária • Considerar técnicas de anonimização • Documentar alternativas e compensações possíveis (por exemplo, precisão x minimização de dados, segurança x transparência, impacto em poucas pessoas

	x benefícios para a sociedade) para processamento de alto risco como parte da DPIA • Avaliação da qualidade de dados via KPIs • Estrutura para preparação de dados e avaliação de modelos (avaliados e utilizados por cientistas de dados) incluindo engenharia de características, validação cruzada, testes de retroalimentação, KPIs validados por empresa etc. • Estabelecer controles e implementação de salvaguardas para mitigar riscos, considerando alternativas e compensações; • Trabalhar de modo ágil em estreita colaboração entre empresas e especialistas em dados para avaliar regularmente necessidades e precisão de resultados - a equipe também inclui analistas de dados, engenheiros de dados, engenheiros de TI e de software para garantir que o modelo possa ser usado corretamente. • Desenvolver metodologias padronizadas de avaliação de risco, que levem em conta a probabilidade e a gravidade dos fatores de risco sobre os indivíduos e/ou a sociedade, o nível de supervisão humana envolvido em decisões automatizadas individualmente com efeitos legais, assim como sua explicabilidade (de acordo com fatores contextuais da decisão sobre a IA) e auditabilidade etc.
Políticas e Procedimentos	• Princípios de alto nível para a IA - como projetar, usar, vender • Adoção de políticas e procedimentos específicos de IA sobre como projetar, usar ou vender IA; • Perguntas e procedimentos de avaliação • Medidas de responsabilização para 2 etapas - treinamento e tomada de decisão • Listas de permissão e bloqueio de usos de IA, bem como listas de casos que merecem atenção redobrada • Avaliação de dados em relação ao propósito: qualidade, proveniência, pessoal ou não, fontes sintéticas, internas ou externas • Objetivo e outros fatores contextuais da IA determinam o quanto a intervenção humana é necessária • Nível de verificação de entrada e saída de dados; • Verificação de preconceito zero ou discriminação injusta na operação ou no resultado durante todo o ciclo de vida da IA • Testagem piloto de modelo de IA antes do lançamento • Uso de dados protegidos (por exemplo, criptografados, pseudônimos ou onde for útil dados sintéticos) em alguns modelos IA/ML • Uso de conjuntos de dados de alta qualidade, mas em menor escala • Onde aplicável, modelos de aprendizagem de IA federada (os dados não deixam o dispositivo), considerando a compensação com a segurança dos dados e as responsabilidades do usuário • Atenção especial para organizações que criam e vendem modelos de IA, software, aplicações • Listas de verificação de due diligence para parceiros comerciais que utilizam tecnologia e ferramentas de IA • Uso ferramentas externas, diretrizes, listas de verificação de autoavaliação • Processos e procedimentos para receber e tratar de feedbacks e reclamações

	• Definição de etapas de escalonamento no que diz respeito a relatórios, governança, análise e manuseio de riscos etc. • Confiabilidade - processo para teste e verificação da confiabilidade do sistema de IA documentado e operacionalizado. • Exploração de formas de anonimizar, desidentificar ou tokenizar dados, ou usar dados sintéticos para treinar modelos de IA; • Modelo de linha de base (se possível explicável) para avaliar a justificativa de emprego de modelos avançados (modelos avançados devem ser usados somente se necessário, a decisão do modelo/KPI deve considerar a complexidade do modelo a ser evitada - sob o princípio da Navalha de Occam) • Fase de ideação entre todas as partes interessadas (cientistas de dados, empresas, usuário final, funções de controle, etc.) onde são discutidas necessidades, resultados, regras de validação, manutenção, necessidade de explicabilidade, orçamento etc. • Documentação do uso de tecnologias de IA, categorias de dados usados em conexão com tecnologias, processo de tomada de decisão, e riscos e mitigações identificados • Aplicação de privacidade e segurança por desenho (privacy and security by-design) no ciclo de vida da IA
Transparência	• Diferentes necessidades de transparência para indivíduos, reguladores, parceiros de negócios / dados e internamente para engenheiros, lideranças nos diferentes estágios do ciclo de vida da IA • Divulgações adequadas comunicadas de maneira simples e fácil de se entender • A IA deve ser inclusiva e, portanto, também acessível e utilizável por pessoas com deficiências/necessidades especiais • A explicabilidade é parte da transparência e da imparcialidade • Trilha de transparência: explicabilidade de decisões e do funcionamento do algoritmo de maneira geral; mais sobre o processo do que sobre a tecnologia; que fatores e que testes são usados para se garantir imparcialidade; responsabilidade pelo impacto das decisões na vida de uma pessoa; qual a extensão da supervisão humana • Explicação de que se trata de uma decisão IA/ML, se houver possibilidade de confusão (Teste de Turing) • Fornecimento de informações contrafactuais • Transparência diferenciada e flexível (vinculada ao contexto, audiência/usuários, propósito de explicabilidade e risco, gravidade de danos), listas prescritivas de elementos de transparência que não são úteis • Compreender as expectativas dos clientes e implementar soluções com base em sua capacidade para compreender a transparência ligada à IA • Da caixa preta até a caixa de vidro: atenção aos dados bem como ao algoritmo/modelo; aspiração à explicabilidade ajuda a entender a caixa preta e constrói confiança • Definição de critérios de implantação de tecnologias de IA dentro da própria organização (por exemplo, cenários de uso) e comunicação aos usuários • Trilha de rastreabilidade para tornar o sistema de IA auditável, particularmente em situações críticas

	• Modelos de cartões (pequenos documentos que acompanham os modelos de IA para descrever o contexto em que o modelo deve ser usado, qual é o procedimento de avaliação) • Centro de dados para transparência sobre governança de dados, acessibilidade de dados, linhagem de dados, modificação de dados, qualidade de dados, definição etc. • Utilização de LIME, SHAP etc. para interpretação
Treinamento e Conscientização	• Treinamento de cientistas de dados, incluindo como evitar e lidar com viés • Treinamento funcional cruzado - profissionais e engenheiros de privacidade • Treinamento ad hoc e funcional • Treinamento de equidade para equipes de tecnologia • Treinamento ético para equipes de tecnologia • Utilizar casos em que a implantação problemática de IA foi interrompida • Papel dos "tradutores" nas organizações, explicando o impacto e o funcionamento da IA
Monitoramento e Verificação	• Capacidade de humano no loop - no projeto, na supervisão, na reparação • Capacidade de compreensão humana de negócios e processos que utilizam IA • Capacidade de desenvolvimento humano de software e processos • Capacidade de auditoria humana de inputs e outputs • Capacidade de revisão humana de decisões individuais com efeitos legais • Monitoramento, validação e verificações contínuas • Comitês de supervisão, mesmo em fase de projeto • Reparação pensada para um humano, não para um bot • Monitoramento do ecossistema a partir do fluxo de dados de entrada, processo de dados e saída de dados • Emprego de diferentes técnicas de auditoria • Técnicas de teste contrafactual • Controle de versão e desdobramento de modelos, rastreamento de caixa preta e algoritmos por engenheiros • Modelos RACI para interação humana e IA • Predefinição dos controles de auditoria de IA • Equipe de auditoria interna especializada em IA e outras tecnologias emergentes • Processos devem permitir controle humano ou intervenção no sistema de IA onde seja tecnicamente possível e razoavelmente necessário • Ver a *Assertion-based Framework for the Audit of Algorithms*, de Otto Koppius e Iuliana Sandu • Monitoramento de modelo (incluindo verificações a posteriori e loop de feedback) e processo de manutenção
Resposta e Aplicação da Lei	• Tratamento de reclamações • Mecanismos de reparação e pessoal apropriado para que indivíduos possam corrigir a decisão de IA • Canal de Feedback • Supervisão interna da instalação de IA

Referências

[i] Mercado Brasileiro de Software – Panorama e Tendências 2021, Associação Brasileira das Empresas de Software, disponível em https://abessoftware.com.br/wp-content/uploads/2021/08/ABES-EstudoMercadoBrasileirodeSoftware2021v02.pdf na página 29.

[ii] Brazil excels in the use of artificial intelligence (Brasil se destaca no uso da inteligência artificial), Câmara de Comércio Brasil-Canadá, 26 de abril de 2022, disponível em: https://ccbc.org.br/en/publicacoes/news-ccbc/brazil-excels-in-the-use-of-artificial-intelligence/#:~:text=A%20survey%20conducted%20last%20year,major%20impact%20on%20their%20competitiveness.

[iii] ABES apresenta tendências para o mercado brasileiro de software em 2022, disponível em https://abessoftware.com.br/en/abes-apresenta-tendencias-para-o-mercado-brasileiro-de-software-em-2022/.

[iv] O CIPL é um grupo de reflexão global sobre políticas de privacidade e dados do escritório de advocacia Hunton Andrews Kurth LLP e é apoiado financeiramente por esse escritório de advocacia e por mais de 90 empresas associadas que são líderes em setores-chave da economia global. A missão do CIPL é engajar-se na liderança do pensamento e desenvolver melhores práticas que garantam tanto a proteção efetiva da privacidade quanto o uso responsável de informações pessoais na era moderna da informação. O trabalho do CIPL facilita o engajamento construtivo entre líderes empresariais, profissionais de privacidade e segurança, reguladores e formuladores de políticas em todo o mundo. Para mais informações, consulte o site do CIPL em http://www.informationpolicycentre.com/. Nada neste documento deve ser interpretado como representação de opinião de qualquer empresa membro do CIPL ou do escritório de advocacia Hunton Andrews Kurth.

[v] Para informações sobre o projeto do CIPL sobre Fornecimento Sustentável de Responsabilização em IA na prática, veja: https://www.informationpolicycentre.com/ai-project.html.

[vi] Veja, por exemplo, a resposta do CIPL ao MCTIC do Brasil e sua Consulta Pública - Estratégia Brasileira de Inteligência Artificial, de janeiro de 2020, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/_english__cipl_response_to_mctic_consultation_on_ai_strategy__24_january_2020_.pdf (em inglês) e https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/_portuguese__cipl_response_to_mctic_consultation_ai_strategy__24_january_2020_.pdf (em português); Best Practices in the Use of AI in Brazil, CIPL contribution (Melhores Práticas no Uso de IA no Brasil - Uma Contribuição do CIPL, em: Inteligência Artificial - Sociedade, Economia e Estado, disponível em https://www.livrariart.com.br/inteligencia-artificial-9786556149226/p.

[vii] Ministério da Ciência, Tecnologia e Inovação do Brasil, Resumo da Estratégia Brasileira de Inteligência Artificial (EBIA), 2021, disponível em https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf.

[viii] LGPD, Lei nº 13.709 de 14 de agosto de 2018, disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[ix] Marco Civil da Internet no Brasil, Lei nº 12.965 de 23 de abril de 2014, disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[x] Código de Defesa do Consumidor do Brasil, Lei nº 8.078 de 11 de setembro de 1990, disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

[xi] Lei de Acesso à Informação do Brasil, Lei nº 12.527 de 18 de novembro de 2011, disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2011/Lei/L12527.htm.

[xii] Artigo 6(X), LGPD.

[xiii] Para fornecer transparência efetiva no contexto de IA, as organizações precisarão considerar o público específico envolvido. Por exemplo, informações sobre o funcionamento interno dos algoritmos pode ser algo inapropriado e inútil aos indivíduos que contestam os resultados de uma decisão automatizada. Em contraste, no contexto de uma investigação regulatória, pode ser necessário fornecer a um regulador informações mais detalhadas sobre como um sistema de IA funciona. Além disso, as organizações precisarão equilibrar o fornecimento de informações transparentes com a necessidade de garantir que a propriedade intelectual e as informações proprietárias

permaneçam adequadamente protegidas. Como tal, pode ser útil considerar os diferentes objetivos de transparência no contexto da IA (ou seja, fornecimento de informações a públicos específicos para alcançar a compreensibilidade, rastreabilidade, explicabilidade, articulação de benefícios ou direitos individuais e vias de reparação). Ao considerar esses fatores e objetivos, as organizações podem tomar decisões contextuais para garantir que o nível correto de informação seja fornecido ao público específico envolvido.

[xiv] UK Digital Regulation Cooperation Forum (Fórum de Cooperação em Regulamentação Digital do Reino Unido), disponível em https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.

[xv] "The roadmap to an effective AI assurance ecosystem" (Estrutura de Referência para um ecossistema eficaz de garantia em IA), do Centre for Data Ethics and Innovation (CDEI), dezembro de 2021, disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1039146/The_roadmap_to_an_effective_AI_assurance_ecosystem.pdf.

[xvi] New South Wales AI Assurance Framework, disponível em https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-ai-assurance-framework.

[xvii] National Institute of Standards and Technology (Instituto Nacional de Normas e Tecnologia), Departamento de Comércio dos EUA, AI Risk Management Framework, disponível em https://www.nist.gov/itl/ai-risk-management-framework.

[xviii] Código de conduta para sistemas de inteligência artificial usado pelo NHS, disponível em https://www.gov.uk/government/news/new-code-of-conduct-for-artificial-intelligence-ai-systems-used-by-the-nhs.

[xix] Veja, por exemplo, ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence (Tecnologia da Informação — Inteligência Artificial — Panorama da credibilidade em inteligência artificial, disponível em https://www.iso.org/standard/77608.html; IEEE P7007 Ontological Standard for Ethically Driven Robotics and Automation Systems (Padrão Ontológico para Sistemas de Robótica e Automação Conduzidos com Ética), disponível em https://site.ieee.org/sagroups-7007/; IEEE Standard Model Process for Addressing Ethical Concerns during System Design (Modelo de Processo Padrão IEEE para Abordar Preocupações Éticas durante Projetos de Sistema), disponível em https://standards.ieee.org/ieee/7000/6781/.

[xx] Em 2020, a Superintendência de Seguros Privados (SUSEP) lançou um sandbox regulatório para o setor de seguros brasileiro. Veja "SUSEP implementa um modelo de sandbox regulatório no Brasil", Julho de 2020, disponível em https://a2ii.org/en/news/a2ii-newsflash-susep-implements-a-regulatory-sandbox-model-in-brazil.

[xxi] Em 2021 o Banco Central do Brasil estabeleceu um programa "sandbox" regulatório buscando estimular a inovação no mercado de finanças e pagamentos. Veja Sciaudone, C., "Inovadores brasileiros vão treinar em 'sandbox' regulatório", 15 de março de 2022, disponível em https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/brazilian-innovators-get-to-play-in-regulatory-sandbox-69251435.

[xxii] Em 2020, a Comissão de Valores Imobiliários do Brasil (CVM) lançou um programa de sandbox regulatório para oportunizar que organizações testassem projetos inovadores no setor financeiro. Veja "Comissão de Valores Imobiliários brasileira começa processo de admissão de participantes de sandbox regulatório", Latin America Business Stories, Novembro 2020, disponível em https://labsnews.com/en/news/economy/brazilian-securities-and-exchange-comission-begins-admission-process-of-regulatory-sandbox-participants/.

[xxiii] Veja o Relatório Provisório do Joint Committee on the Personal Data Protection Bill (Comitê Misto sobre a Lei de Proteção de Dados Pessoais), 2019, publicado em Novembro de 2021, disponível em https://acrobat.adobe.com/link/review?uri=urn%3Aaaid%3Ascds%3AUS%3Af030ad33-879d-4127-870a-9f055fbe2644#pageNum=1 na Seção 40.

[xxiv] Datatilsynet AI Regulatory Sandbox (Caixa de Areia Regulatória de IA da Datatilsynet), disponível em https://www.datatilsynet.no/en/news/2021/sandbox-open-for-new-applicants/.

[xxv] Sandbox regulatório em privacidade por desenho e por padrão em projetos de Inteligência Artificial, Superintendência da Indústria e Comércio da Colômbia, disponível em https://globalprivacyassembly.org/wp-content/uploads/2021/07/B6.-SIC-Colombia-Sandbox-on-privacy-by-design-and-by-default-in-AI-projects.pdf.

[xxvi] Sandbox regulatório de Tecnologias de Melhoria da Privacidade de IMDA e PDPC, Cingapura, disponível em https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/IMDA-and-PDPC-launch-

Singapore-first-Privacy-Enhancing-Technologies-Sandbox-as-they-mark-decade-long-effort-of-strengthening-public-trust.

[xxvii] Veja "Introducing Open Loop, a global program bridging tech and policy innovation" (Apresentando o Open Loop, um programa global interligando tecnologia e inovação em políticas), disponível em https://ai.facebook.com/blog/introducing-open-loop-a-global-program-bridging-tech-and-policy-innovation/; e AI Impact Assessment: A Policy Prototyping Experiment (Avaliação de Impacto de IA: Um Experimento de Prototipagem de Política), disponível em https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3772500_code715910.pdf?abstractid=3772500&mirid=1.

[xxviii] Para mais informações sobre as Comissões de Revisão de Dados, consulte Cate, F., Dockery, R., e Crosley, S., "Why data review boards are a promising tool for improving institutional decision-making" (Por que conselhos de revisão de dados são uma ferramenta promissora para melhorar a tomada de decisão institucional), IAPP Privacy Perspectives, 28 de fevereiro de 2020, disponível em https://iapp.org/news/a/why-data-review-boards-are-a-promising-tool-for-improving-institutional-decision-making/.