

CONSIDERAÇÕES DA BRASSCOM SOBRE INTELIGÊNCIA ARTIFICIAL

Junho de 2022

A Brasscom, Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais (TIC), é entidade sem fins lucrativos de representatividade nacional, e que congrega algumas das mais dinâmicas e inovadoras empresas de TIC alinhadas com a Transformação Digital do Brasil.

A digitalização do país inevitavelmente será alavancada com a massificação do uso de soluções baseadas em inteligência artificial (IA). A IA tem o potencial para melhorar o bem-estar social e humano, contribuir para a atividade econômica, aumentar a inovação e a produtividade, além de ajudar a humanidade a solucionar seus maiores desafios e seus problemas. Segundo estudo da PriceWaterhouseCoopers (PWC), as tecnologias baseadas em IA podem aumentar o PIB global em US\$ 15,7 trilhões, um total de 14%, até 2030, sendo US\$ 0,5 trilhão só na região da América Latina¹. Portanto, torna-se cada vez mais necessário o aprofundamento das discussões em torno dessas tecnologias e de alternativas de políticas públicas que estimulem a utilização e inovação responsável em IA que se articulem com as boas práticas empresariais e valorizem a autodeterminação, levando em conta o melhor interesse socioeconômico.

As discussões em torno da IA estão avançando ao redor do mundo. Existem jurisdições que estão discutindo marcos legais robustos, como é o caso da União Europeia. O Brasil tem caminhado neste sentido e, atualmente, o principal desafio é aprofundar as discussões para entender quais são os aspectos que devem ser considerados em uma futura legislação de IA, suportada por ferramentas de governança e *accountability* para contribuir para o desenvolvimento e o uso de IA responsável no país.

Este documento apresenta a visão da Brasscom sobre como implementar uma abordagem baseada em risco para regulação e conformidade de IA. Baseia-se na premissa de que a regulação da IA deve permanecer ágil, assim como os usos da tecnologia que ela busca regular. Portanto, não deve visar uma abordagem única para todos ou a eliminação de todos os potenciais riscos. Deve permitir, sim, a avaliação de riscos e benefícios contextuais, mitigação de riscos e melhorias constantes.

É também de suma importância que a Comissão leve em consideração as diretrizes de melhor regulamentação estabelecidas pela Lei de Liberdade Econômica², para que o futuro marco legal de IA seja baseado nelas. Por isso, nós instamos a Comissão a realizar uma avaliação de impacto completa, incluindo uma avaliação de impacto econômico em relação à regulação de IA, bem como quais falhas de mercados se pretende endereçar e verificar se novas falhas podem ser equivocadamente criadas a partir da própria regulação.

De maneira geral, a nossa visão para uma estrutura de IA eficaz e à prova de futuro beneficia:

- Indivíduos, garantindo que os benefícios da IA sejam continuamente equilibrados com os riscos potenciais;

¹ <https://www.pwc.co.uk/economic-services/assets/macroeconomic-impact-of-ai-technical-report-feb-18.pdf>

² http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm

- Organizações, permitindo-lhes colher benefícios das mais recentes tecnologias e manter-se competitivas na era digital moderna sem prejudicar os indivíduos e a sociedade e, sempre que possível, proporcionar benefícios a esses grupos;
- Reguladores, fornecendo ferramentas modernas que permitem uma regulação flexível e eficaz, sem prejudicar a inovação; e
- A sociedade e a economia, promovendo o desenvolvimento e a adoção mais ampla de IA benéfica e confiável, levando em consideração o custo de oportunidade de não usar a IA.

Nesse sentido, a Brasscom gostaria de agradecer a oportunidade concedida pela Comissão de Juristas responsável por subsidiar o Senado Federal na Elaboração de Substitutivo sobre IA (CJSUBIA) de apresentar suas considerações sobre o tema. Os comentários abaixo refletem diversos tópicos presentes nos eixos temáticos para debate apresentados pela CJSUBIA em seu Plano de Trabalho.

1. Sobre a regulação

A justificativa para as regulações econômicas surge da necessidade de reduzir o poder de mercado potencial, para aumentar a eficiência e, ao mesmo tempo, garantir uma competição saudável entre os produtores em uma economia, bem como a preservação e garantia de direitos individuais. Apesar de o debate geralmente ter como enfoque se (ou como) um mercado deve ser regulado, também é preciso pensar em quando este mercado deve ser regulado, antes ou depois de uma falha de mercado. Neste sentido, destacamos que, com base no tempo de suas obrigações, os regulamentos são categorizados como ex ante ou ex post.

As regulações ex ante visam amplamente identificar problemas de antemão e moldar o comportamento e as respostas das partes interessadas por meio da intervenção regulatória. Isto é, tal regulação é implementada previamente à ocorrência de um comportamento indesejado, de forma a desestimular que os agentes que participam daquele mercado o pratiquem. Em outras palavras, a regulação ex ante ocorre quando o regulador prevê de forma antecipada como o regulado deve se comportar, a partir de um sopesamento de interesses, direitos e riscos afetos àquela temática, sem que haja conhecimento concreto das particularidades que circundarão a situação que se busca regular.

De outro lado, as regulações ex post surgem quando uma falha ou distorção no mercado já emergiu. Ou seja, são desenvolvidas com base nas informações disponíveis, quando já foram apresentadas evidências suficientes para demonstrar as externalidades negativas e os custos daquela falha ou distorção. Sendo assim, as regulações ex post podem ser consideradas como uma reação a determinada situação concreta e suas especificidades.

Por ser caracterizada como uma regulação prévia, que não dispõe de todas as informações sobre como determinada conjuntura se desenvolverá e quais serão seus efeitos, a regulação ex ante pode apresentar algumas complicações. São exemplos:

- Propensão a vieses e interesses dos reguladores, conforme mencionado anteriormente;
- Tendência à elaboração de uma regulação rígida, haja vista que não há pleno conhecimento sobre pontos que de fato merecem ser objeto de regulação e em qual medida;

- Regulação que não leva em consideração fatos e seus efeitos, mas sim previsões, possibilidades e riscos, de forma que pode haver um descompasso entre a realidade e a regulação; e
- Propensão a um olhar específico para algum setor, ignorando as características dos demais.

Estes possíveis efeitos podem se tornar ainda mais problemáticos quando pensamos em regulações *ex ante* voltadas para o setor de tecnologia. Isso porque, é possível que, além de acabar por gerar uma inocuidade da legislação, tais efeitos imponham limitações insuperáveis ao desenvolvimento de determinada tecnologia, sufocando a inovação. Esse alerta se torna ainda mais significativo quando pensamos especificamente sobre a inteligência artificial, que ainda está em pleno processo de desenvolvimento e implementação.

Via de regra, a regulação de tecnologias é desafiadora em virtude da sua natureza disruptiva e dinâmica. Portanto, a Brasscom gostaria de respeitosamente alertar que a questão da regulação da IA não é binária, mas sim uma questão de escopo e calibração entre instrumentos de *hard law*, *co-regulação* e *soft law*, com o intuito de criar um ambiente habilitador para o desenvolvimento e uso de IA, dispondo de segurança jurídica em prol da inovação, como aspecto fundamental para a existência de investimentos e expansão econômica. Particularmente em uma área de tecnologia que está mudando tão rapidamente quanto a IA, precisamos de uma estrutura regulatória que possa se recalibrar dinamicamente com base nas melhores práticas de IA em evolução, caso contrário, corremos o risco de sufocar desnecessariamente inovações benéficas.

Nós incentivamos a Comissão a examinar métodos mais flexíveis de regulação, tais como a regulação responsiva, conforme exploramos abaixo.

1.1 A regulação responsiva como o caminho

A alternativa sugerida seria que o trabalho desenvolvido por esta Comissão tome como base a teoria da regulação responsiva. Isto porque a teoria em questão tem como fundamento a ideia central de uma pirâmide regulatória, na qual a autorregulação se encontra na base, abarcando a maior parte das situações, enquanto a regulação de comando encontra-se no topo, reservando a atuação mais intrusiva do Estado para os casos estritamente necessários. Isto é, há um escalonamento da intervenção regulatória estatal, de forma a possibilitar a cooperação, o diálogo e a criação de políticas internas pelos entes privados, sem excluir a possibilidade de o Estado atuar por meio de punições, advertências, multas e sanções nos casos que exijam a adoção destas medidas.

A teoria da regulação responsiva foi uma proposta alternativa à perspectiva binária de regulação vs. desregulação, prisma este que atualmente afeta a discussão de novas tecnologias, dentre elas a inteligência artificial. Por meio deste modelo, é possível chegar a um meio termo entre o livre mercado e a regulação estatal, dito de outra forma, há uma maior elasticidade para se atender aos interesses privados das empresas e aos direitos dos cidadãos, bem como ao interesse público. Neste ponto, cabe ressaltar que, justamente por trazer estes benefícios, algumas agências reguladoras brasileiras já vêm adotando este modelo de regulação, dentre elas estão a Agência Nacional de Telecomunicações (Anatel) e a Agência Nacional de Energia Elétrica (ANEEL).

Além dos exemplos acima, é possível observar certos elementos da regulação responsável em legislações que têm temáticas mais próximas à inteligência artificial. No que tange à proteção de dados pessoais, um dos mecanismos utilizados para assegurar essa proteção são os documentos elaborados por entidades privadas que atuam como controladoras ou operadoras. Em outro ponto, o Marco Civil da Internet também adotou alguns princípios que estimulam a atuação conjunta do Estado e dos entes privados, como: estímulo de boas práticas para a preservação da estabilidade, segurança e funcionalidade da rede; natureza participativa da rede; e liberdade de modelos de negócios, desde que não conflitem com os princípios do Marco Civil. É também relevante a abordagem de regulação de IA pretendida pela União Europeia, isto porque, o *Artificial Intelligence Act* traz uma escalada da regulação de acordo com os riscos apresentados pelo sistema de inteligência artificial.

Tendo em vista suas principais características, é possível concluir que a regulação responsável seria capaz de endereçar diversas questões problemáticas que são aventadas quando se fala de um marco legal da inteligência artificial. São exemplos:

- o equilíbrio entre uma futura regulação e a necessidade de continuidade de desenvolvimento tecnológico e estímulo à inovação da inteligência artificial, tendo em vista que, em face do escalonamento de regulação responsável, apenas as situações estritamente necessárias seriam reguladas pelo Estado, evitando a imposição de obrigações legais que desestimulariam o investimento na área e sufocariam o desenvolvimento e uso da inteligência artificial no mercado brasileiro;
- a interação de uma legislação estanque com uma tecnologia que continuará a evoluir e se modificar ao longo do tempo, dado que a maior parte das situações seria abarcada pela autorregulação, ficando na base da pirâmide, se reservando o marco legal da inteligência artificial a abordar apenas os pontos necessários;
- a incapacidade de uma legislação única abordar de forma adequada a ampla gama de sistemas de inteligência artificial aplicados aos mais distintos setores, tendo em vista que os entes privados teriam certa liberdade para dispor sobre a tecnologia em questão; e
- a problemática de uma tecnologia que exige uma perspectiva multidisciplinar ser regulada por meio de uma perspectiva unilateral, novamente considerando que os entes privados teriam certa liberdade para dispor sobre as tecnologias em questão, se reservando a regulação estatal ao estritamente necessário.

Ou seja, além de ser uma alternativa que se coloca no meio de perspectivas extremas (regulação vs. desregulação) que causam não só implicações negativas, mas impossibilitam que se chegue a consensos, bem como que se consiga abarcar interesses e direitos distintos, a regulação responsável também traz possíveis respostas a diversas questões espinhosas quando se trata da regulação de tecnologias, incluindo da inteligência artificial.

2. Definição de Princípios

O desenvolvimento e elaboração de uma estrutura regulatória eficiente deve ter como base pilares principiológicos bem definidos, que reflitam de maneira apropriada o ecossistema sobre aquilo

que pretende-se regular. Vale lembrar que a OCDE já divulgou os seus Princípios de IA³, que inclusive foram aderidos pelo Brasil e amplamente explorados na Estratégia Brasileira de Inteligência Artificial⁴. E que, apesar de terem um caráter recomendatório para os países e portanto carecem de certa concretude, são uma referência teórica importante para que mantenhamos consistência com as discussões internacionais.

Dito isto, a Brasscom gostaria de respeitosamente fazer referência a sua Carta de Princípios ([link](#)), que traz alguns conceitos importantes sobre a temática, conforme abaixo:

- Inclusão – Sistemas de IA devem beneficiar a sociedade como um todo e auxiliar no desenvolvimento socioeconômico sustentável.
- Valores – Sistemas de IA devem tomar suas decisões visando ao respeito pelas leis e direitos fundamentais do cidadão.
- Transparência – Sistemas de IA devem ser projetados e desenvolvidos de modo a garantir que sua operação seja suficientemente transparente, de acordo com o modelo de negócio em questão, para permitir o entendimento de como o sistema de IA produz seus resultados. O grau de transparência deve levar em conta a finalidade pretendida dos sistemas de IA e os riscos atrelados ao seu funcionamento, conforme o caso, ficando a critério do provedor a adoção das medidas apropriadas.
- Proteção de Dados e Segurança – Sistemas de IA devem prezar pela proteção de dados e segurança da informação, adotando as melhores práticas para garantir a confiabilidade e integridade dos dados.
- Desenvolvimento e Uso Responsável - Sistemas de IA devem ser desenvolvidos com observância destes princípios desde a sua concepção. A indústria tem a responsabilidade de reconhecer os potenciais usos indevidos da tecnologia e a responsabilidade e oportunidade de adotar medidas para evitar condutas razoavelmente previsíveis em desacordo com esses princípios.
- Responsabilização e Prestação de Contas - Demonstração, pelos provedores de sistema de IA, da adoção de medidas eficazes para o bom funcionamento dos sistemas, observadas suas funções, e responsabilização nos limites de suas respectivas participações, contexto e tecnologias disponíveis. O controle dos agentes sobre os sistemas de IA deverá ser proporcional ao risco potencial atrelado ao seu funcionamento e finalidade, bem como às salvaguardas e medidas de mitigação adotadas.
- Boas Práticas Globais - Desenvolvimento de IA integrado a boas práticas globais, de modo a acelerar a adoção de IA e o seu desenvolvimento a custos acessíveis.

3. Definição de IA

Uma definição clara e amplamente compreendida de IA será um elemento fundamental para uma estrutura regulatória de IA eficaz. A Brasscom reconhece o desafio de criar uma definição aceitável que permaneça pertinente ao longo do tempo, principalmente à luz das diversas opiniões e da falta de consenso entre a indústria e as experiências acadêmicas.

³ <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

⁴ https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-diagramacao_4-979_2021.pdf

Gostaríamos de alertar que um conceito equivocadamente amplo colocaria todos os softwares contemporâneos potencialmente no escopo. Uma definição mais restrita é necessária para evitar o excesso de regulação e focar na subcategoria de sistemas de IA onde é mais provável que surjam questões de risco importantes. A este respeito, será importante estabelecer a linha clara entre a última onda de sistemas de IA que aprendem com dados e experiência, e software tradicional e sistemas de controle baseados em IA que operam de acordo com regras codificadas, ou até mesmo a automação.

Os sistemas tradicionais são previsíveis porque funcionam da mesma maneira quando apresentados nas mesmas circunstâncias, de acordo com as regras que lhes foram dadas – mesmo que a experiência passada tenha demonstrado que isso não é o ideal. Em contraste, os sistemas modernos de IA aprendem com a experiência, seja com dados de treinamento fornecidos ou com dados coletados em uso, e, portanto, a maneira como eles se comportam em qualquer circunstância é mais difícil de prever.

Portanto, a definição de sistemas de IA deve ser cautelosamente concebida, inclusive para excluir de seu escopo a automação, na medida em que a IA não se restringe a responder a comandos e possui a capacidade de aprender a perceber, interpretar e interagir com o ambiente externo com as ações e as informações recebidas. Para que seu conceito não seja genérico, e acabe por equivocadamente abarcar outras tecnologias que não são em sua essência baseadas em IA, sugerimos a adoção da definição apresentada pela OCDE⁵:

“sistema de inteligência artificial (sistema de IA): é um sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos por humanos, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Os sistemas de IA são projetados para operar com vários níveis de autonomia.”

Uma uniformidade terminológica facilitará a interoperabilidade e compatibilidade das soluções de inteligência artificial em aderência às legislações dos diversos países onde tais sistemas sejam utilizados, além de permitir uma melhor integração nas cadeias globais de desenvolvimento e produção, beneficiando-se, ademais, de padrões e estruturas de certificação que venham a ser globalmente adotadas.

Por fim, ressalte-se que seria importante que a definição a ser incorporada no texto legal deverá qualificar a natureza jurídica da inteligência artificial como de software, para permitir a integração desse conceito ao arcabouço jurídico brasileiro existente.

3.1 Determinando quais sistemas de IA serão cobertos pela estrutura regulatória

Acreditamos que uma legislação de IA deve se concentrar apenas em sistemas de IA de alto risco e ser proporcional e coerente em relação às leis existentes no Brasil que se aplicam de maneira neutra em termos de tecnologia. Portanto, é preciso haver uma maneira de as organizações determinarem se seus sistemas de IA atendem aos critérios de alto risco para se enquadrarem no escopo da lei. Tendo em

⁵ <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

vista a relevância da contextualização do uso de certo sistema para a aferição do grau de risco a ele inerente, que deverá considerar a grau de risco, sua escala e a probabilidade de que o risco venha a se concretizar, acreditamos que não deverá a legislação definir, a priori, quais atividades devam ou não ser consideradas de alto risco, cabendo as próprias organizações realizar este enquadramento, a depender da sua análise de risco no caso concreto.

A Brasscom propõe que a futura legislação adote a seguinte abordagem para determinar se a IA está dentro ou fora do escopo do regulamento:

- a) Adotar uma estrutura fácil de usar para identificar sistemas de IA de alto risco cobertos.

A abordagem para identificar sistemas de IA de “alto risco” cobertos deve funcionar para organizações de todos os tamanhos. Não deve ser muito complexo ou prescritivo, a exemplo do modelo de avaliação de risco discutido no âmbito da União Europeia, que seria desproporcional para a maioria das organizações, difícil de aplicar na prática e pode dificultar o desenvolvimento e implantação de tecnologias inovadoras baseadas em IA no Brasil.

Por outro lado, deve esclarecer como os riscos diferem para sistemas de IA voltados para humanos e não humanos, bem como critérios de avaliação de risco apropriados. Enquanto alguns aplicativos de IA são voltados para humanos (por exemplo, sistemas de reconhecimento facial, sistemas de recomendação ou sistemas de contratação), muitos aplicativos de IA não são (por exemplo, análise de informações meteorológicas, defeitos no chão de fábrica, gargalos nas redes ou estado das estradas).

Os sistemas de IA que não são voltados para humanos normalmente não compreendem dados pessoais nos conjuntos de dados e frequentemente alimentam análises para outras máquinas, não para usuários finais humanos. Como resultado, os sistemas de IA voltados para humanos e não humanos têm tipos distintos de riscos associados a eles. Por exemplo, considerar os riscos de privacidade é essencial para sistemas voltados para humanos. Mas os riscos de privacidade não estão presentes, via de regra, na análise de dados do sensor climático alimentada a outro sistema que usa a análise para avaliar os padrões climáticos por um longo período de tempo.

A aplicação dos mesmos requisitos de gerenciamento de risco a ambos os tipos de sistemas de IA não permitiria que tecnólogos e avaliadores avaliassem os riscos para os sistemas de IA de maneira acionável e também seria oneroso para as organizações – dificultando desproporcionalmente a inovação.

- b) Deixar explícito que os usos de IA com nenhum ou baixo risco estão fora do escopo do regulamento de IA.

Naturalmente, uma legislação com foco em sistemas de IA de alto risco não afetaria os usos benéficos da IA que impliquem um uso de risco muito baixo ou inexistente. Corroborando com o disposto no item acima, citamos outros exemplos de usos de baixo ou inexistente risco incluem IA usada para os seguintes propósitos:

- Para fins industriais ou técnicos, incluindo a racionalização e otimização de processos operacionais ou produtivos existentes, fora das configurações de alto risco;
- Garantir a segurança da rede e prevenir ataques cibernéticos;
- Para prevenir e detectar transações financeiras ou comerciais fraudulentas;
- Prevenir ou detectar lavagem de dinheiro;
- Antecipar a probabilidade e a natureza de reclamações dos clientes para direcionar o atendimento proativo adequado ao cliente;
- Para fins de medição de audiência de sites e dispositivos para garantir a conformidade com os padrões de publicidade, de acordo com as legislações vigentes.

Nesse ponto, há que se notar que o artigo 5º, inciso II, da Constituição Federal estabelece que “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”. A partir do dispositivo em questão, é possível extrair que a lógica do sistema brasileiro é a de que tudo é permitido, exceto aquilo que for expressamente proibido por lei. Transportando essa lógica para o futuro marco legal da inteligência artificial, todos os usos de sistemas de inteligência artificial devem ser permitidos, exceto aqueles que sejam expressamente proibidos pela lei. Sendo assim, mesmo nos casos em que o sistema de inteligência artificial apresentar um alto risco, ou mesmo um risco inaceitável, ele somente deverá ser vetado caso, após uma análise concreta de impacto, se entender que os riscos envolvidos não são compensados ou mitigados pelos benefícios esperados.

4. Abordagem baseada em riscos

Como qualquer sistema, incluindo processos baseados em humanos, os sistemas de IA não são perfeitos. Eles, no entanto, oferecem a oportunidade de melhorar drasticamente a atual tomada de decisão baseada em seres humanos. Assim, a referência operacional para sistemas de IA não deve ser a perfeição, mas sim o desempenho de processos atuais comparáveis (se existentes) ou uma alternativa disponível movida por seres humanos.

Existe um risco real de que os usos inovadores da IA possam ser impedidos ao exigir que os sistemas de IA atendam a um padrão que excede em muito o exigido por abordagens que não são de IA. Às vezes, isso pode ser deliberado devido a restrições protecionistas artificiais, mas com mais frequência é provável que seja devido à falta de compreensão sobre falhas ocultas nas decisões existentes que não são de IA e à tendência natural das pessoas de perdoar mais os erros cometidos por um humano vs. por uma máquina.

Na medida em que os sistemas de IA são tão abrangentes, em termos de complexidade e contextos de uso, quando se discute inteligência artificial, é fundamental que se traga um olhar a respeito de possíveis impactos, tendo como premissa a gestão de risco. Portanto, não pode haver uma abordagem de “tamanho único” para regular a IA porque não há um caso único de uso para a IA. A IA refere-se a sistemas ou máquinas que imitam a inteligência humana para executar tarefas e podem se aprimorar iterativamente com base nas informações que coletam, e que assumem muitas formas e atendem a muitos propósitos, abrangendo uma ampla gama de perfis de risco.

É importante, portanto, adotar uma abordagem holística para permitir que a IA floresça e se desenvolva sob alguns parâmetros principiologicos para refletir o papel desempenhado pela IA em um determinado contexto operacional e setorial, bem como a natureza e a probabilidade de possíveis danos. Embora seja óbvio que alguns usos da IA exigirão escrutínio e salvaguardas extras, paralelamente, deve haver um reconhecimento claro dos custos de oportunidade de não desenvolver e usar a IA.

A IA, quando desenvolvida e usada com responsabilidade, pode ajudar a reduzir uma vasta gama de riscos inerentes à vida cotidiana. Conceitualmente, a Brasscom apoia uma abordagem baseada em risco para qualquer nova estrutura regulatória, mas é vital garantir que ela seja direcionada aos casos de uso corretos, levando em consideração a probabilidade de dano e não apenas a gravidade do dano, bem como consideração do custo de não usar a IA em termos de benefícios perdidos.

É necessária uma abordagem proporcional, equilibrando possíveis riscos com os muitos benefícios sociais e econômicos prometidos pela IA e reconhecendo claramente os custos de oportunidade de não usar a IA em uma situação específica ou desenvolver IA com capacidades específicas. É importante reconhecer que existem falhas nas abordagens existentes (sem IA) e, se um sistema de IA imperfeito tiver um desempenho melhor do que o status quo em uma tarefa crucial para salvar vidas, seria desejável o uso do sistema de IA. Nos casos em que a alternativa de não usar a IA representa um risco maior do que o risco representado pela implantação de um sistema de IA, a estrutura regulatória não deve desencorajar o uso benéfico líquido da IA.

Também é importante refletir o contexto operacional mais amplo ao avaliar o nível de risco. As organizações que usam IA terão mais incentivo para investir em mitigações e salvaguardas adicionais para reduzir os riscos se isso reduzir a carga regulatória.

4.1 Sistemas de IA voltados para humanos e não humanos

A Brasscom entende que não se deve regular a IA porque é IA, mas porque a IA, quando usada em determinados e específicos contextos sensíveis, pode gerar riscos únicos para as pessoas. O foco principal de qualquer definição do escopo da legislação não deve, portanto, se concentrar nas tecnologias em si, mas em como elas são usadas e em quais contextos. Portanto, ao considerar os riscos, deve-se esclarecer como os riscos diferem para sistemas de IA voltados para humanos e não humanos, bem como critérios de avaliação de risco apropriados. Enquanto alguns sistemas de IA são voltados para humanos (por exemplo, sistemas de reconhecimento facial, sistemas de recomendação ou sistemas de contratação), muitos sistemas de IA não o são (por exemplo, análise de informações meteorológicas, defeitos no chão de fábrica, gargalos nas redes ou condições das estradas).

Os sistemas de IA que não são voltados para humanos normalmente não têm dados pessoais nos conjuntos de dados e frequentemente alimentam análises para outras máquinas, não para usuários finais humanos. Como resultado, os sistemas de IA voltados para humanos e não humanos têm gradações distintas de riscos associados a eles. Por exemplo, considerar os riscos à proteção de dados pessoais é essencial para sistemas voltados para humanos. Mas os riscos à proteção de dados pessoais não estão presentes na análise de dados do sensor climático alimentada a outro sistema que usa a análise para avaliar os padrões climáticos por um longo período de tempo. A aplicação dos mesmos requisitos de gerenciamento de risco a ambos os tipos de sistemas de IA não permitiria que tecnólogos e avaliadores

avaliassem os riscos para os sistemas de IA de maneira acionável e também seria oneroso para as organizações – dificultando desproporcionalmente a inovação.

Em outras palavras, podemos concluir que os sistemas de IA voltados para não humanos apresentam riscos menores, até mesmo em muitos casos inexistentes, e que, portanto, não deveriam estar sujeitos a cargas regulatórias tão rígidas.

4.2 Valorização das boas práticas e da governança empresarial

A confiança no ambiente digital é uma premissa estruturante desse ecossistema havendo inúmeras iniciativas para que as organizações dediquem recursos financeiros e humanos ao desenvolvimento e adoção de controles para garantir que os princípios basilares e a confiança sejam honrados. Importante destacar que as empresas de tecnologia possuem um grande comprometimento em desenvolver soluções baseadas em IA que sejam responsáveis e atendam às expectativas de seus clientes e da sociedade em geral. A Brasscom entende que projetar a IA para ser confiável exige a criação de soluções que reflitam princípios éticos profundamente enraizados na sociedade. Esses princípios são críticos para lidar com os impactos sociais da IA e criar confiança, à medida que a tecnologia se torna cada vez mais parte dos produtos e serviços que as pessoas usam no trabalho e em casa todos os dias.

Considerando a natureza global da economia digital de maneira geral, e do próprio ecossistema de Inteligência Artificial, é fundamental que seja incentivado o desenvolvimento e a adoção de soluções de IA de empresas que se comprometem a adotar medidas, técnicas e administrativas, voltadas para o desenvolvimento e uso responsável de Inteligência Artificial, de acordo com padrões de boas práticas e de governança reconhecidos internacionalmente, que inclusive poderiam ser comprovadas a partir de certificação independente, conforme destacamos abaixo. Incentivar a adoção dessas medidas, por meio da contratação pública, irá auxiliar, em última instância, os agentes de IA no país a estarem em consonância com as melhores práticas internacionais e alavancar a confiança nas novas tecnologias.

Inúmeras empresas que dedicam esforços para o desenvolvimento responsável de IA tem implementado estruturas robustas de governança interna, adotando departamentos inteiros cuja função seja monitorar todo o desenvolvimento de IA garantindo que as avaliações de risco apropriadas sejam adotadas, e que o desenvolvimento seja orientado pelos princípios éticos mínimos para o uso responsável da tecnologia.

4.3 Abordagem interoperável com padrões de governança de IA

Dada a natureza transfronteiriça da economia digital, as estruturas regulatórias e os padrões técnicos de IA devem operar idealmente em todas as nações e regiões. O aumento do alinhamento global na regulação da IA, inclusive no contexto do comércio, ajudará a facilitar a adoção, o uso e a interoperabilidade de tecnologias de IA em diferentes jurisdições.

Para que na prática todo este arcabouço de gestão de risco possa ser implementado de maneira eficiente para garantir a responsabilidade e prestação de contas, deve-se levar em conta os mecanismos de soft law existentes, nomeadamente:

Mecanismos de *Soft Law*

No âmbito das medidas de autorregulação que poderão ser adotadas para garantir um uso responsável de IA, podemos citar:

a) Padrões globais

Padrões de consenso voluntários reconhecidos internacionalmente podem servir como base para regimes autorregulatórios robustos, como guias para reguladores e até mesmo como os próprios padrões regulatórios, se incorporados por referência. Como esses padrões são baseados em uma base ampla e profunda de conhecimento de uma ampla variedade de perspectivas da indústria e da sociedade civil, eles podem ser flexíveis e ágeis de uma maneira que a regulação estática não pode, evoluindo ao longo do tempo à medida que as tecnologias inovam e mudam.

Como referência, gostaríamos de citar que as empresas de tecnologia estão, em escala global, desenvolvendo e discutindo continuamente novas formas de endereçar as preocupações e desafios em torno dos sistemas de IA. Várias dessas iniciativas de definição de padrões já estão em andamento, ou estão finalizados, em nível internacional por meio do comitê de "Inteligência Artificial" da ISO / IEC JTC1 SC42⁶, por exemplo, além das ISO/IEC DIS 23894 (Tecnologia da Informação/Inteligência Artificial/Gestão de Risco)⁷, e ISO/IEC CD 5338 (Tecnologia da Informação/Inteligência Artificial/Processos no ciclo de vida do sistema de IA)⁸.

Destaque-se também a iniciativa do National Institute of Standards and Technology (NIST) que submeteu recentemente à consulta pública o documento "*AI Risk Management Framework*"⁹. O objetivo deste documento é criar, em parceria com todas as partes interessadas, uma estrutura voluntária composta por um processo flexível, estruturado e mensurável para abordar os riscos da IA em todo o ciclo de vida da IA, oferecendo orientação para o desenvolvimento e uso de IA confiável e responsável. O intuito é justamente melhorar a compreensão e ajudar as organizações a gerenciar os riscos corporativos e sociais relacionados ao desenvolvimento, implantação e uso de sistemas de IA. Adotar essa estrutura pode ajudar organizações, indústrias e sociedade a entender e determinar seus níveis de risco, bem como auxiliar na adoção de medidas e mecanismos necessários para evitar riscos e mitigá-los, caso se concretizem.

b) Certificação independente

Uma alternativa interessante para incentivar a autodeclaração de conformidade é permitir que os agentes de IA comprovem sua conformidade com os preceitos da lei, baseados nas melhores práticas e padrões internacionais conforme mencionado no item acima, através de processo de certificação por terceiro independente. Esse mecanismo é particularmente eficiente em termos de dar celeridade e segurança no processo de avaliação de conformidade, permitindo que uma entidade terceira independente possa verificar rapidamente se todas as medidas necessárias para garantir o desenvolvimento e/ou uso responsável da IA foram incorporadas pelos agentes de IA em seus processos, e fornecer um certificado que reconheça todas essas questões. Os próprios agentes de IA se

⁶ <https://www.iso.org/committee/6794475.html>

⁷ <https://www.iso.org/standard/77304.html>

⁸ <https://www.iso.org/standard/81118.html>

⁹ <https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf>

sentirão motivados a receber essa certificação, justamente para comprovar perante as autoridades ou até mesmo outras empresas de que eles estão proativamente se preocupando com questões éticas em IA, como forma de se destacar no mercado.

Considerando a natureza global da economia digital de maneira geral, e do próprio ecossistema de Inteligência Artificial, é fundamental que seja permitida a emissão de certificação por qualquer entidade independente reconhecida internacionalmente, por exemplo daquelas reconhecidas pela *International Accreditation Forum* (IAF).

c) Avaliações de Impacto - Ferramenta de gestão de risco e de *accountability*

Vale ressaltar que uma abordagem prévia de avaliação de conformidade com requisitos pode acarretar em custos exacerbados às organizações e desincentivar a inovação. Conforme afirmamos no item acima, uma alternativa interessante é estabelecer programas de inteligência artificial responsáveis, que incentivem as organizações a realizarem autoavaliações flexíveis de sistemas de IA para refletir de maneira apropriada os riscos associados ao desenvolvimento e uso de determinados sistemas baseados em IA.

Semelhante ao que temos no contexto da Lei Geral de Proteção de Dados e os relatórios de impacto à proteção de dados pessoais, exigir Avaliações de Impacto de Tomada de Decisão Automatizadas (AITDA) – seria uma alternativa mais equilibrada para exigir revisões prévias gerais, ao invés de criar uma lista taxativa de aplicações de IA de consideradas de alto risco. Essa abordagem também se alinharia ao princípio de responsabilidade e prestação de contas, onde as organizações que desenvolvem e utilizam sistemas de IA estão na melhor posição para avaliar, determinar e documentar o nível de risco gerado por suas próprias atividades e mitigar esses riscos adequadamente.

A futura lei de IA poderia exigir que os sistemas de IA que possam atender critérios de alto risco sejam submetidos a um AITDA – um processo de autoavaliação passo a passo para identificar e quantificar riscos e benefícios e identificar e documentar as mitigações desses riscos. Por exemplo, a tomada de medidas concretas para garantir a qualidade e amplitude adequadas dos dados de treinamento funcionariam como mitigações que reduzem o risco geral. Os componentes básicos do processo das AITDAs poderiam ser formalizados em alto nível na regulação, deixando espaço para que as organizações adotem processos internos de acordo com as melhores práticas internacionais de avaliação de risco, conforme mencionamos anteriormente.

Abaixo, citamos algumas características que entendemos serem fundamentais para compor a estrutura das Avaliações de Impacto de Tomada de Decisão Automatizadas:

- A estrutura para identificar sistemas de IA de alto risco cobertos deve envolver o uso de avaliações de impacto, realizadas pelas organizações com base nas melhores práticas internacionais, projetadas para avaliar a probabilidade, gravidade e escala do impacto do uso de IA. Essas avaliações de impacto incluiriam as seguintes considerações:
 - Gravidade e probabilidade de danos a indivíduos, grupos ou sociedade em geral (dependendo de conclusões que podem ser alcançadas com razoável certeza);
 - Nível e significado do envolvimento humano e revisão e adequação ao contexto;

- Magnitude e probabilidade de benefício do uso da IA para indivíduos, grupos ou sociedade em geral;
 - Risco de reticência e/ou custos de oportunidade de não usar a IA para indivíduos, grupos de indivíduos ou sociedade em geral. Isso incluiria a ponderação dos benefícios do uso da IA versus deixar o processo sob o status quo atual (ou seja, medir se o resultado é aprimorado pelo uso da IA em vez de deixá-lo como feito atualmente); e
 - Medidas de mitigação para lidar com os riscos.
-
- Pré-Avaliação. As organizações realizariam uma simples pré-avaliação para determinar se uma avaliação de impacto em grande escala é necessária à luz dos critérios gerais previstos na lei. Isso permitiria que as organizações alocassem melhor seus recursos para a avaliação de sistemas de IA que podem apresentar um alto risco e impediriam as organizações de realizar avaliações do uso de IA em contextos em que é óbvio que há muito pouco risco envolvido.

 - Ponderando os benefícios da IA, não apenas os danos - Idealmente, esse processo de avaliação de risco de IA poderia se concentrar não apenas nos danos, mas também nos benefícios do sistema de IA em questão. Ao focar também nos efeitos positivos da IA, também levaria em conta os riscos de não usar a IA em um contexto específico, juntamente com os usos e aplicações benéficos da IA, como seu potencial para reduzir ou mitigar a discriminação, aumentar a autonomia humana, possibilitam descobertas científicas ou contribuem para padrões de vida mais elevados. Isso permitiria um procedimento de avaliação de risco mais holístico e abrangente, baseado em um cálculo de benefícios e custos. Em alguns casos, os benefícios de um uso de IA para indivíduos ou um grupo de indivíduos podem ser significativos, independentemente de seus riscos. Embora o benefício do uso de IA não deva afetar diretamente a classificação de risco de uma aplicação de IA, a consideração do benefício reduziria o risco de reticência de não avançar com a aplicação de IA benéfica pretendida meramente devido à possibilidade de alto risco. Essa interpretação é, em última análise, corroborada na norma sobre gestão de risco da International Organization for Standardization em parceria com a International Electrotechnical Commission: IEC/ISO 31010¹⁰. Nesta norma, a ISO e IEC exploram também como o risco é uma medida da extensão em que uma entidade é influenciada negativamente por uma potencial circunstância ou evento. Normalmente, o risco é uma função de 1) os impactos adversos que podem surgir se a circunstância ou evento ocorrer; e 2) a probabilidade de ocorrência. As entidades podem ser indivíduos, grupos ou comunidades, bem como sistemas, processos ou organizações. O impacto dos sistemas de IA pode ser positivo, negativo ou ambos e pode abordar, criar ou resultar em oportunidades ou ameaças. O documento afirma também que, em alguns casos, os riscos podem ser positivos. O papel da gestão de risco é justamente minimizar os impactos negativos previstos dos sistemas de IA - adotando as medidas necessárias para a mitigação de potenciais riscos - e identificar oportunidades para maximizar os impactos positivos.

¹⁰ <https://www.iso.org/standard/72140.html>

- A avaliação de impacto poderá ser utilizada para analisar e monitorar riscos residuais. As organizações poderiam aproveitar os processos de avaliação de impacto para identificar possíveis riscos e, a partir desta documentação, avaliar as medidas e salvaguardas necessárias para evitá-los e mitigá-los. Após a adoção desse conjunto de mecanismos, a avaliação de impacto serviria para identificar os riscos residuais e avaliar se enquadrariam ainda como de alto risco. Caso seja identificado que os riscos residuais são baixos, os sistemas de IA poderiam ser considerados pelas organizações como não enquadrando nos critérios gerais estabelecidos em lei.
- Aproveitando mecanismos de *Soft Law* para manter a adaptabilidade - As AITDAs devem ser baseadas nas melhores práticas do setor, códigos de conduta, códigos de boas práticas, padrões e mecanismos de certificação liderados pela indústria.

Ao adiar os detalhes dos requisitos específicos de avaliação e documentação para esses instrumentos de soft law, como faz a própria Lei Geral de Proteção de Dados (LGPD), a CJSUBIA pode garantir que o regulamento seja capaz de se adaptar à medida que a tecnologia e as expectativas em torno delas continuem a evoluir. Ao fazê-lo, poderia apoiar e aproveitar os diálogos contínuos sobre o que significa desenvolver e implantar a IA com responsabilidade, como aqueles que ocorrem por meio do Observatório de Políticas de IA da OCDE, apoiado pela rede multissetorial da OCDE de especialistas em IA (ONE AI).

Oferecemos a estrutura acima para um possível regime regulatório centrado na AITDA como exemplo para demonstrar que existem várias maneiras de a Comissão se basear nos requisitos regulatórios existentes e encontrar um equilíbrio mais sustentável entre a necessidade de governança e a necessidade de preservar a inovação em IA e o crescimento econômico do Brasil, apoiando também a evolução contínua das melhores práticas nesta área.

Em contraste, uma abordagem regulatória mais prescritiva, articulando em detalhes um conjunto de requisitos obrigatórios para o projeto, desenvolvimento e implantação de sistemas de IA, nos moldes de uma legislação engessada, prejudicaria a criação desses instrumentos ágeis de *soft law* e poderia restringir o desenvolvimento e o uso de IA no país. Isso resultaria em uma regulação estática e inflexível, povoada por um conjunto de requisitos que seriam desatualizados rapidamente, não acompanhando o ritmo da evolução tecnológica e, como tal, deixando de fornecer orientações úteis e significativas aos desenvolvedores de IA.

d) Outras ferramentas de accountability

A confiança é premissa fundamental para a consolidação e massificação da IA. Portanto, é do próprio interesse dos desenvolvedores criarem sistemas de IA cada vez mais confiáveis e responsáveis, justamente para potencializar os benefícios do uso de novas soluções inovadoras e garantir que todas as partes interessadas possam usufruí-las. Por isso, muitas organizações estão começando a usar de forma proativa estruturas de responsabilidade para lidar com as oportunidades, riscos, desafios e

tensões apresentados pelo uso da IA, bem como para cumprir as leis relevantes, incluindo leis de proteção de dados e antidiscriminação, e considerar proativamente as expectativas sociais e garantir a confiança do cliente.

Essas melhores práticas emergentes estão começando a estabelecer robustez na forma de estruturas de IA coerentes e abrangentes e ferramentas técnicas, e provavelmente catalisarão o desenvolvimento e a implementação das melhores práticas por todas as partes interessadas no ecossistema de IA, desencadeando uma "corrida ao topo". Essas práticas também permitirão que as organizações promovam a responsabilidade organizacional baseada em riscos como uma ponte para o desenvolvimento de diretrizes globalmente harmonizadas e interoperáveis sobre sistemas e usos de IA.

No contexto de IA, o futuro marco legal poderia incentivar os desenvolvedores e os usuários de sistemas de IA a adotar mecanismos alternativos de *accountability* como selos, certificados e códigos de conduta como uma forma de alavancar a adoção de medidas internas para conferir maior robustez aos sistemas que desenvolvem, transmitir confiança àqueles que os utilizam e, em última análise, demonstrar conformidade com os princípios estabelecidos em lei.

5. A questão do potencial viés e discriminação

O crescente uso da inteligência artificial nas mais diversas áreas sensíveis, incluindo em processos de contratação, no âmbito da justiça criminal e na assistência médica, provocou um debate sobre viés e justiça. Reconhecemos que essa é uma questão delicada e que merece esforços de todos os agentes do ecossistema no seu entendimento e enfrentamento. No entanto, tal fragilidade decorre da própria limitação da tomada de decisão humana nesses e em outros domínios, que também pode ser falha, moldada por preconceitos individuais e sociais que geralmente são inconscientes.

Ou seja, a precisão e eficiência das decisões tomadas por sistemas de IA refletem a qualidade dos dados que colocamos neles. Dados incorretos ou imprecisos podem conter preconceitos raciais ou de gênero implícitos. Muitos sistemas de IA poderão continuar sendo treinados usando dados incorretos, tornando esse um problema contínuo. Mas acreditamos que o viés pode ser tratado e transformado e que os sistemas de IA que incorporarem mecanismos para combater viés serão os mais bem-sucedidos.

Um princípio crucial, tanto para humanos quanto para máquinas, é evitar preconceitos e, portanto, evitar discriminação. O viés no sistema de IA ocorre principalmente nos dados ou no modelo algorítmico. Para desenvolver sistemas de IA nos quais podemos confiar, é essencial desenvolver e treinar esses sistemas com dados imparciais, íntegros e de alta qualidade.

Sob o ponto de vista prático, tendo em mente esse cenário, e acreditando que a IA é uma tecnologia que está constantemente em evolução e demandando atenção, algumas empresas atualmente já oferecem soluções nesse sentido.

A questão do viés nos sistemas de inteligência artificial é, sem sombra de dúvidas, um dos grandes desafios a serem enfrentados. Ela não é, contudo, um problema a ser demonizado. Devemos sim nos beneficiarmos justamente dos sistemas automatizados para mitigar os riscos e tendências de discriminações indevidas, e não necessariamente depender única e exclusivamente da supervisão humana para fazê-lo.

6. Supervisão humana

A Brasscom entende que nem todo e qualquer tipo de sistemas de IA deveria ser obrigatoriamente objeto de supervisão humana. Alguns sistemas de IA mais simples, utilizados por exemplo para a leitura de medição de consumo de água, devido ao seu baixo risco, não deveriam ser mandatoriamente objetos à supervisão humana, sob o risco de onerar e encarecer o uso da tecnologia.

Por outro lado, sistemas extremamente complexos não devem, necessariamente, estar sujeitos a mecanismos de supervisão humana pela própria inabilidade do ser humano de acompanhar o sistema em si. Nesses casos, há sim de se falar em desenvolvimento e/ou uso, conforme o caso, de maneira responsável, com a adoção de medidas de governança para o uso da tecnologia que garantam a perseguição de objetivos éticos e transparentes. Nos casos pontuais em que seja pertinente uma consideração de necessidade de supervisão humana, deve-se considerar, para a sua determinação, o risco potencial atrelado ao funcionamento e à finalidade de determinada solução baseada em IA, bem como às salvaguardas e medidas de mitigação adotadas.

No mesmo sentido, gostaríamos de ressaltar nossa preocupação com os problemas relacionados à supervisão humana em sistemas de IA. Apostar na supervisão humana como solução infalível contra potenciais vieses e discriminação pode consolidar a falsa sensação de que sistemas de IA estão funcionando normalmente, perpetuando resultados indesejados, caso outras questões, como a qualidade e precisão dos dados utilizados, conforme abordamos no item anterior, sejam ignoradas. Como contrapartida, vale destacar que empresas de tecnologia têm desenvolvido mecanismos próprios, inclusive baseados em IA, para avaliar os processos de decisões automatizadas e mitigar vieses, quando identificados.

Sendo assim, entendemos que eventual futuro projeto de lei sobre IA deve trazer linguagem incentivando os desenvolvedores de IA a se comprometem a adotar mecanismos eficientes para avaliação de processos de decisão e mitigação de vieses, independentemente da forma que elas sejam realizadas não cabendo ao arcabouço regulatório a determinação ou detalhamento dessas situações.

Vale lembrar que a Lei Geral de Proteção de Dados (LGPD) já versa sobre a revisão de decisões tomadas com base em tratamento automatizado de dados pessoais, em seu art. 20¹¹. Caso a Comissão de Juristas ainda entenda que seja necessário estabelecer a necessidade de revisão de decisão automatizada que não envolva dados pessoais por humanos, a Brasscom gostaria de sugerir alguns critérios condicionantes para tal. Nós entendemos que as revisões de decisões automatizadas não deveriam ser adotadas como regra em caráter individual, mas sim em caráter de exceção exclusivamente em casos de alto risco, mas no sentido de explicação da tomada de decisão e não de revisão de decisão individual propriamente dita.

7. Reconhecer que a transparência é um meio para um fim

A transparência não é um fim em si mesma — é um meio pelo qual possibilitar a responsabilidade e a prestação de contas, capacitar os usuários e construir confiança. Ao invés de discutirmos qual palavra

¹¹ “Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.”

deveríamos utilizar, seja transparência, explicabilidade ou compreensibilidade, propomos que seja discutido conceito de transparência propriamente dito. E nesse sentido, a Brasscom entende que, ao projetar os requisitos de transparência, deve-se considerar o que está tentando se alcançar e a melhor forma de atingir essas metas em um determinado contexto, tendo como norte empoderar os indivíduos com informações úteis sobre processos automatizados, de maneira a permitir que eles entendam o seu funcionamento e possam tomar decisões sobre este.

Por exemplo, diferentes partes interessadas exigirão diferentes formas de transparência em diferentes circunstâncias. Os requisitos devem ser adaptados para garantir que as informações sejam acionáveis e apresentadas quando as partes interessadas quiserem, em termos que possam entender e sem detalhes estranhos que possam distrair ou confundir. Em alguns contextos, informações detalhadas sobre decisões individuais podem ser importantes, enquanto em outros, informações gerais sobre como os sistemas funcionam ou como eles são desenvolvidos podem ser mais benéficas ou apropriadas.

Nesse mesmo sentido tem se posicionado o filósofo italiano Luciano Floridi. Pioneiro no campo da Filosofia da Informação e da Ética da Informação, Luciano Floridi realizou diversos estudos sobre transparência e propõe um modelo tridimensional para suportá-la, baseado na¹²:

- Precisão: é necessário levar em consideração o sujeito;
- Simplicidade: o detalhamento deve ser limitado ao necessário, de maneira objetiva;
- Relevância: levando em consideração o contexto e o destinatário

É importante equilibrar cuidadosamente o desejo de transparência com outras ações importantes, por exemplo, velocidade, segurança, proteção e privacidade. É importante ressaltar que algumas formas de transparência que são intuitivamente atraentes podem trazer alguns dos riscos mais significativos e fornecer pouco benefício real em termos de habilitação de responsabilidade e construção de confiança. Por exemplo, a divulgação de código-fonte ou dados de usuários individuais pode fornecer poucas informações sobre como um sistema funciona ou por que ele tomou uma determinada decisão, mas pode permitir o abuso ou a exploração de sistemas e traz riscos significativos à privacidade e outros direitos fundamentais do usuário.

8. Responsabilidade civil

Primeiramente, cabe destacar quais os objetivos da responsabilidade civil: (i) possibilitar o ressarcimento de eventual dano; (ii) estimular as organizações a evitarem situações que possam ensejar responsabilização ou, em outras palavras, desestimular atos ilícitos; e (iii) penalizar aqueles que vierem a efetivamente causar danos. No contexto do ecossistema de IA, é fundamental que a estrutura de responsabilidade civil encontre um equilíbrio entre a proteção eficaz por possíveis danos e, ao mesmo tempo, o fornecimento de margem de manobra suficiente para que as empresas possam desenvolver a IA.

Neste sentido, entende a Brasscom que o futuro projeto de lei sobre inteligência artificial deve reconhecer o arcabouço jurídico do direito civil já existente. Mais especificamente no contexto da IA, a Brasscom entende que a responsabilidade pelos sistemas de inteligência artificial deve levar em

¹² <https://philpapers.org/archive/TURTEO-4.pdf>

consideração a efetiva participação de cada agente ao longo da cadeia de desenvolvimento e operação de IA, bem como os danos específicos que se deseja evitar ou remediar. Isto porque, são diversos os atores envolvidos ao longo da cadeia, desde a concepção da IA até sua efetiva aplicação, cada um deles com um escopo de atuação e uma capacidade de ingerência limitados. São exemplos: (a) o fornecedor de dados usados por aquele sistema; (b) o desenvolvedor da inteligência artificial; (c) o fornecedor da IA; (d) aquele que é efetivamente proprietário da IA; (e) o usuário do sistema; etc.

A questão da cadeia de produção e de aplicação da IA é relevante para fins de responsabilização, pois é preciso identificar qual agente estaria na melhor posição para identificar, controlar e gerenciar a parte do sistema ou a parcela do desenvolvimento e aplicação que efetivamente gerou o dano. Sendo assim, é preciso que a estrutura escolhida seja hábil a atribuir a responsabilidade pelo dano àquele agente que efetivamente o gerou, sem atribuir encargos desproporcionais aos partícipes da cadeia, nesta toada, a responsabilidade subjetiva seria a escolha mais acertada.

Além disso, não se pode olvidar que os sistemas de inteligência artificial operam com certa autonomia, o que pode ser exemplificado por sua capacidade de autoaprendizagem. Neste sentido, muitas vezes, o dano ocasionado pode advir não propriamente de uma falha que possa ser atribuída a algum dos agentes envolvidos ou até mesmo a um "defeito" presente naquele sistema de IA, mas sim à própria imprevisibilidade que advém de sua habilidade de agir de forma autônoma e independente. Em outras palavras, existem casos nos quais, apesar de determinado agente participante da cadeia relativa à IA ter adotado todas as medidas que lhe eram possíveis e cabíveis, ainda assim, um dano imprevisível poderá vir a ser causado.

Ademais, é necessário pontuar que, muitas vezes, os sistemas de inteligência artificial não atuam de forma isolada, mas sim integrados a outros serviços e/ou produtos. Ou seja, o sistema de IA não opera em um vácuo, podendo estar agregado a um ecossistema de tecnologias, ser apenas um de muitos componentes de um produto, estar englobado pela prestação de um serviço, etc. Nesta toada, na ocorrência de um determinado dano, é preciso que se avalie não só qual dos agentes pertencentes à cadeia de desenvolvimento e aplicação da IA seria efetivamente responsável, mas, também, se o sistema de inteligência artificial foi de fato o causador daquele dano.

Considerando, portanto, toda a complexidade da cadeia de valor de IA que destacamos acima, cabe ressaltar que um regime de responsabilidade objetiva caminharia em absoluto descompasso com: (i) o próprio funcionamento da tecnologia em questão; (ii) a capacidade de atuação das organizações no que diz respeito aos riscos gerados pela IA; e (iii) o fato de que estes sistemas não encontram-se isolados. Sendo assim, se uma regra de responsabilidade objetiva for estabelecida, é possível que organizações venham a ser responsabilizadas: (a) por atos que eram de fato imprevisíveis; (b) por questões foram de seu escopo de controle; (c) por práticas que não poderiam ser atribuídas à IA; e (d) apesar de terem adotado todas as medidas que lhe cabiam. Desnecessário discorrer sobre os impactos que uma disposição neste sentido teria em investimentos voltados para a inteligência artificial e, conseqüentemente, no desenvolvimento da tecnologia no país, seja pela distribuição de um significativo ônus por toda a cadeia produtiva em vista dos moldes de responsabilização, seja por gerar insegurança jurídica ao focar apenas na penalização e não no estabelecimento de ações consideradas adequadas para minimizar os riscos da tecnologia.

Entendemos que a estrutura de responsabilidade deveria incentivar as organizações a tomarem medidas e mecanismos para evitar riscos e, se o risco se concretizar em um contexto onde todas as

iniciativas viáveis e necessárias para evitá-lo, esses esforços devem ser levados em consideração. Nesse sentido, para além das premissas denexo de causalidade e o dano efetivamente constituído, em casos específicos deverá oferecer a possibilidade de inversão de ônus da prova.

A inclusão de um requisito de responsabilidade explícito possibilitará que as organizações ponderem sobre os riscos e impactos de seus sistemas de IA e as ajudará a estabelecer processos e controles para desenvolver e implementar sistemas de IA responsáveis, confiáveis e sustentáveis, ou seja, proverá a segurança jurídica necessária. Importa ressaltar que o artigo em questão também se adequa à realidade de existência de diversos tipos de IA, com distintos graus de risco e aplicáveis a setores variados, dado que requer que sejam considerados a natureza, escopo, contexto, propósitos, impactos, riscos e benefícios do sistema.

Além do exposto acima, a Brasscom defende que a estrutura regulatória de IA também deve fornecer recompensas e incentivos adequados para estimular e ajudar a acelerar ainda mais a responsabilidade e prestação de contas em IA e as melhores práticas organizacionais. Esses “incentivos” podem incluir: vincular a responsabilidade a certificações externas; reconhecer os compromissos autorregulatórios ou códigos de conduta de organizações que definem publicamente os valores e princípios de IA que implementam; usar a responsabilidade demonstrada como uma “licença para operar”, permitindo que organizações responsáveis e/ou certificadas tenham maiores oportunidades de usar e compartilhar dados de forma responsável para facilitar o crescimento no uso responsável de IA; permitir o uso mais amplo de dados em IA para projetos socialmente benéficos; usar a responsabilidade de IA demonstrada como critério para projetos de contratação pública; e reconhecer a responsabilidade demonstrada pela IA como um fator de mitigação ou como um fator de redução de responsabilidade no contexto de aplicações de sanções.

9. Do Conselho Consultivo

Se por um lado a Brasscom entende que não deve ser estabelecida uma agência reguladora central para IA, devendo os usos da IA em setores regulados serem endereçados pelos respectivos reguladores setoriais, nós entendemos que neste momento seria interessante a criação de um Conselho de caráter consultivo para a disseminação de conhecimento e aprofundamento das discussões em torno da temática, com uma necessária paridade de representação entre o Poder Público, setor empresarial e sociedade civil, garantindo-se assim uma representação igualitária de todos os envolvidos no processo de desenvolvimento e estruturação da IA no Brasil.

Tendo em vista a complexidade da temática de IA, e a sua aplicação transversal em diversos setores econômicos, tal Conselho poderá vir a ser um *locus* para que as discussões sobre IA aconteçam, com o compartilhamento de experiências entre setores e áreas econômicas, permitindo uma ampla compreensão sobre o tema pelo Poder Público. A participação de representantes de agências reguladoras, como Agência Nacional de Telecomunicações (ANATEL) e Agência Nacional de Energia Elétrica (ANEEL), é de suma importância para discussões das especificidades e contextos setoriais.

Em nosso entendimento, esse Conselho deveria ter as seguintes competências:

- a) a promoção de estudos sobre pesquisa científica e tecnológica, desenvolvimento, padrões, educação, governança, aplicação comercial, segurança, competitividade econômica e outros tópicos relacionados à IA;
- b) a edição de recomendações sobre padrões, governança, aplicação comercial, segurança, e outros tópicos relacionados à IA;
- c) propor programas de pesquisa e desenvolvimento relacionados à IA, bem como estimular a sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados; e
- d) ser representado nos fóruns técnicos nacionais e internacionais relativos à IA.

Esperamos que essas contribuições possam ser de valia para a Comissão de Juristas e agradecemos a oportunidade de participar e contribuir em tão relevante debate para a sociedade brasileira.
