24 de janeiro de 2020

RESPOSTA DO *CENTRE FOR INFORMATION POLICY LEADERSHIP*
CONSULTA PÚBLICA SOBRE A ESTRATÉGIA DE INTELIGÊNCIA ARTIFICIAL BRASILEIRA

O *Centre for Information Policy Leadership* (CIPL)[1] tem o prazer de responder à consulta pública sobre uma Estratégia Nacional de Inteligência Artificial para o Brasil organizada pelo Departamento de Telecomunicações do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). O CIPL valoriza essa iniciativa do MCTIC, especialmente no contexto do novo regime de proteção de dados do Brasil sob a Lei Geral de Proteção de Dados Pessoais (LGPD).[2]

O CIPL enaltece o trabalho do MCTIC por refletir profundamente sobre os vários aspectos integrais de uma estratégia nacional de IA, como comprovado pela amplitude das questões e da literatura internacional mencionadas no documento de consulta. Dada a experiência do CIPL na esfera de proteção de dados pessoais, esta resposta abordará as prioridades e objetivos da consulta pública em geral e, a seguir, focará especificamente nos seguintes eixos temáticos:

- Legislação, Regulamentação e Uso Ético
- Governança da IA
- Aspectos internacionais

I. Prioridades e objetivos

a. Quais problemas concretos devem ser prioritariamente endereçados por uma estratégia de IA?

Durante o final da década de 2010, muitos países começaram a criar e desenvolver estratégias nacionais de IA. De acordo com o Observatório de Informação do Setor Público da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), pelo menos 50 países desenvolveram ou estão desenvolvendo uma estratégia nacional de IA.[3] Como o MCTIC observa corretamente na sua consulta, o objetivo de uma estratégia nacional de IA é aprimorar o desenvolvimento e o uso da tecnologias de IA e abordar certos desafios colocados pela IA, incluindo questões de transparência, divulgação responsável ao usar sistemas de IA e garantir que tais sistemas respeitem o Estado de direito, os direitos humanos, os valores democráticos e a diversidade. O CIPL louva o reconhecimento pelo MCTIC do duplo objetivo de uma

[1] O CIPL é uma think tank global especializada em privacidade e cibersegurança de dados pessoais, que é parte do escritório de advocacia Hunton Andrews Kurth LLP. O CIPL recebe apoio financeiro do Hunton e de 90 empresas-membro que são líderes em setores-chave da economia global. A missão do CIPL é envolver-se na liderança de pensamento e desenvolver melhores práticas que garantam proteções eficazes à privacidade e ao uso responsável de dados pessoais na era da informação. O trabalho do CIPL facilita o engajamento construtivo entre líderes empresariais, profissionais de privacidade e segurança, reguladores e formuladores de políticas públicas em todo o mundo. Para obter mais informações, consulte o site do CIPL em http://www.informationpolicycentre.com/. Nada neste documento deve ser interpretado como representando as opiniões de qualquer empresa-membro do CIPL ou do escritório de advocacia da Hunton Andrews Kurth.

[2] Lei Geral de Proteção de Dados Pessoais (LGPD), disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[3] Estratégias de IA e componentes do setor público, Observatório de Informações do Setor Público, Organização para Cooperação e Desenvolvimento Econômico, novembro de 2019, disponível em https://oecd-opsi.org/projects/ai/strategies/.

estratégia eficaz de IA para não apenas abordar os riscos e desafios apresentados pelas tecnologias de IA, mas também para permitir a inovação e o uso benéfico de dados por meio dessas tecnologias.

A consideração de questões relacionadas à proteção de dados pessoais no que se refere às tecnologias de IA é essencial para a criação de uma estratégia de IA que facilite o seu uso responsável e, ao mesmo tempo, garanta a conformidade com as leis e políticas de proteção de dados. Como resultado, o CIPL acredita que, para o Brasil criar uma estratégia nacional robusta de IA, ele deve considerar e tratar prioritariamente os problemas de privacidade e proteção de dados no contexto da IA.

O CIPL escreveu extensivamente sobre os principais problemas de privacidade de dados relacionados à IA em seu projeto sobre "Inteligência Artificial e Proteção de Dados: Oferta de responsabilidade sustentável de IA na prática".[4] O primeiro relatório deste projeto, intitulado "Inteligência Artificial e Proteção de Dados em Tensão"[5] detalha o uso generalizado, os recursos e o potencial dos aplicativos de IA. Ele também examina algumas das tensões existentes entre as tecnologias de IA e os princípios tradicionais de proteção de dados. O segundo relatório deste projeto, intitulado "Problemas Difíceis e Soluções Práticas"[6] fornece abordagens concretas para mitigar alguns dos principais desafios descritos no primeiro relatório e detalha exemplos de melhores práticas e ferramentas que podem ser implantadas hoje para promover um futuro melhor no qual a IA seja centrada no ser humano, e a privacidade e a proteção de dados pessoais prosperem. Recomendamos que o MCTIC revise os relatórios sobre IA do CIPL mencionados acima ao formular sua estratégia nacional de IA e, em particular, sua posição em relação à proteção de dados.

II. Legislação, Regulamentação e Uso Ético

O MCTIC observa corretamente que houve muita discussão em torno do desenvolvimento tecnológico da IA. Também houve muita troca em torno da necessidade de desenvolver parâmetros legais, regulatórios e éticos para orientar o desenvolvimento da tecnologia da IA de uma maneira que equilibre a proteção de direitos – incluindo os direitos à privacidade e proteção de dados, à capacidade de organizações inovarem e desenvolverem aplicativos de IA, incluindo aqueles aplicativos que ainda não foram totalmente compreendidos.

A consulta pública em questão faz referência a diversas diretrizes e documentos que foram produzidos para aprofundar os aspectos legais, regulamentares e éticos da IA, incluindo iniciativas significativas no nível da União Européia. Esses incluem a Declaração de Ética e Proteção de Dados em Inteligência Artificial de 2018 da *International Conference of Data Protection Commission and Privacy Commissioners*[7] e as Diretrizes de Ética para IA Confiável, produzidas pelo *High-Level Expert Group on Artificial Intelligence* da

[4] Consulte o Projeto CIPL sobre Inteligência Artificial e Proteção de Dados: Oferta de responsabilidade sustentável de IA na prática, disponível em https://www.informationpolicycentre.com/ai-project.html.
[5] Primeiro relatório de IA: Inteligência Artificial e Proteção de Dados em Tensão, 10 de outubro de 2018, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.
[6] Segundo relatório de IA: Problemas Difíceis e Soluções Práticas, 17 de janeiro de 2018 (cópia prévia pré-publicada), disponível em https://www.informationpolicycentre.com/cipl-second-ai-report-01172020.html.
[7] Declaração do ICDPPC sobre Ética e Proteção de Dados em Inteligência Artificial, 23 de outubro de 2018, disponível em https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.

Comissão Europeia.[8] O CIPL respondeu a consultas públicas sobre esses dois documentos em 2019.[9] O CIPL também discutiu em mais detalhes muitas das questões descritas nesses documentos através de mesas-redondas organizadas em todo o mundo com reguladores, formuladores de políticas, líderes da indústria e acadêmicos[10]. O CIPL acredita que muitas das conclusões dessas reuniões são de relevância direta para as discussões relativas a este eixo temático da consulta pública.

a. Como é possível endereçar questões relacionadas à discriminação e ao viés em decisões tomadas por sistemas autônomos?

Embora o viés algorítmico e a discriminação sejam as principais preocupações em torno da tomada de decisões automatizadas, é importante lembrar que seres humanos raramente são consistentemente racionais, imparciais ou mesmo capazes de explicar por que tomam determinadas decisões. Em longo prazo, a IA tem o potencial de ajudar a identificar, corrigir e evitar muitos dos vieses irracionais que afetam a tomada de decisão humana. Qualquer estratégia nacional de IA deve reconhecer isso e aspirar para que a IA aja dessa maneira. Em curto prazo, no entanto, existe muita preocupação em relação a deixar o resultado de certas decisões unicamente nas mãos de um sistema automatizado que possa produzir resultados discriminatórios, por exemplo, devido a tendências derivadas dos dados utilizados.

Hoje em dia, existem muitas medidas que podem ser tomadas para resolver questões relacionadas a esse viés e discriminação algorítmica:

- **Facilitar o acesso aos dados, incluindo dados confidenciais**: os tecnólogos de IA confirmaram que, para evitar vieses, os algoritmos devem ser testados com categorias sensíveis de dados, como sexo, raça e saúde. Negar o acesso ou impedir a retenção ou o uso de dados confidenciais dificulta a detecção e correção de vieses e pode limitar ainda mais a capacidade de explicar por que o aplicativo de IA está chegando a conclusões discriminatórias. É importante observar, no entanto, que as proteções adequadas – incluindo mascaramento, anonimização,

[8] Diretrizes de Ética para IA Confiável, Grupo Europeu de Peritos de Alto Nível em Inteligência Artificial, 8 de abril de 2019, disponível em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

[9] Consulte os comentários do Centro para Liderança em Políticas de Informações na Declaração da International Conference of Data Protection Commission and Privacy Commissioner sobre Ética e Proteção de Dados em Inteligência Artificial, 25 de janeiro de 2019, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_icdppc_declaration_on_ethics_and_data_protection_in_artificial_intelligence.pdf; e os comentários do CIPL sobre o Grupo de Peritos de Alto Nível da Comissão da UE sobre os Projetos de Diretrizes de Ética na IA para IA Confiável, disponíveis em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57590 nas páginas 351-358.

[10] Os eventos incluíram Sessão de Trabalho Interativa Conjunta do CIPL/Comissão de Proteção de Dados Pessoais de Cingapura (PDPC) sobre "IA Responsável e Responsabilizada" (16 de novembro de 2018, Cingapura); Mesa-redonda com reguladores europeus e participantes do setor "Problemas Difíceis em IA" (12 de março de 2019, Londres); Mesa-redonda com o Grupo de Peritos de Alto Nível da Comissão da UE sobre "Diretrizes de Ética para IA Confiável" (27 de junho de 2019, Bruxelas); Mesa-redonda com reguladores asiáticos e participantes do setor sobre "Desafios e Soluções de Proteção de Dados Pessoais em IA" (18 de julho de 2019, Cingapura); Mesa-redonda com o Gabinete do Comissário da Informação do Reino Unido (ICO) sobre a "Estrutura de Auditoria de IA" (12 de setembro de 2019, Londres); Labs do CIPL/TTC Design Jam em "Explicabilidade da IA" (3 de dezembro de 2019, Cebu); e Oficina do Setor do CIPL sobre uma abordagem regulatória europeia da IA (14 de janeiro de 2020, Bruxelas).

pseudonimização e *accountability* – serão de maior importância onde dados confidenciais são processados para impedir a ocorrência de vieses.

- **Desenvolver técnicas para identificar e tratar do risco de viés algorítmico**: atualmente, muitas organizações estão desenvolvendo técnicas para abordar especificamente a questão da discriminação em aplicativos de IA. Por exemplo, algumas organizações confiam em testes de justiça contrafactuais. Essa técnica verifica a equidade nos resultados, determinando se o mesmo resultado é alcançado quando uma variável específica, como raça ou gênero, muda.[11] Um relatório de 2019 sobre "Perspectivas sobre Questões de Governança da IA", lançado pelo Google, detalha outras técnicas de justiça algorítmica projetadas para "desvio de superfície, análise de conjuntos de dados e teste e entendimento de modelos complexos, a fim de ajudar a tornar os sistemas de IA mais justos". Isso inclui facetas, a *What-If Tool*, modelos e cartões de dados, além de treinamento com restrições de justiça algorítmica.[12] A Accenture desenvolveu sua própria ferramenta de justiça para "identificar e remover qualquer influência coordenada que possa levar a um resultado injusto"[13] que ela usa internamente em relação a seus próprios projetos de IA, bem como externamente, em projetos de clientes que envolvem a implantação de aplicativos de IA para ajudá-los a abordar o princípio de justiça. A IBM também criou várias ferramentas para tratar de questões de ética e justiça na IA, incluindo a AI Fairness 360, "um abrangente conjunto de ferramentas de código-fonte aberto para verificar tendências indesejadas nos conjuntos de dados e nos modelos de aprendizado de máquina, além de algoritmos mais atuais para mitigar esse viés",[14]. A IBM também criou o IBM Watson OpenScale, uma ferramenta para rastrear e medir os resultados da IA para ajudar a detectar e corrigir o viés de maneira inteligente, além de explicar as decisões da IA.[15]

- **Treinamento de cientistas de dados**: as organizações que desenvolvem aplicativos e ferramentas de IA investiram pesadamente no treinamento dos cientistas de dados que estão projetando esses sistemas. Parte deste treinamento inclui aumentar a conscientização sobre diferentes fontes e tipos de vieses, instruções sobre como evitar e abordar vieses ao criar algoritmos e como detectar e testar algoritmos quanto a vieses antes da sua implantação.

- **Processos de revisão ética**: muitas organizações já têm ou estão considerando a criação de conselhos de revisão de dados ou comitês de ética em relação à IA, que podem ser internos ou externos à essas organizações. Essa é vista como uma maneira de impulsionar *accountability*

[11] Consulte o Modelo de Estrutura de Governança de Inteligência Artificial, primeira edição, Comissão de Proteção de Dados Pessoais de Cingapura, janeiro de 2019, disponível em https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Model-AI-Framework---First-Edition.pdf?la=en na página 15. "Uma decisão é justa em relação a um indivíduo, se é a mesma no mundo real e em um mundo contrafactual, em que o indivíduo pertencia a um grupo demográfico diferente".

[12] Para ler mais sobre essas técnicas, consulte Perspectivas sobre Questões na Governança de IA, Google, 2019, disponível em https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf.

[13] Enfrentando o Desafio da Ética na IA, Rumman Chowdhury, Accenture, 6 de junho de 2018, disponível em https://www.accenture.com/gb-en/blogs/blogs-cogx-tackling-challenge-ethics-ai.

[14] Kush R. Varshney, "Introdução ao AI Fairness 360", IBM Research Blog (19 de setembro de 2018), disponível em https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/.

[15] "Gerenciar a IA, com Confiança e Segurança nos Resultados Comerciais", IBM, disponível em https://www.ibm.com/downloads/cas/RYXBG8OZ.

dentro da organização, promover tomadas de decisões responsáveis e garantir que novas utilizações de dados respeitem os valores corporativos e sociais. Com relação ao viés, uma empresa, ao usar esse processo, decidiu não implantar o reconhecimento facial em câmeras de segurança, devido à descoberta de preocupações éticas relacionados a viés e imprecisão, que não poderiam ser satisfatoriamente atenuadas.[16]

O CIPL recomenda que o MCTIC reconheça o potencial problema de viés algorítmico e discriminação na estratégia nacional de IA e destaca ainda que as soluções para resolver esse problema estão atualmente sendo desenvolvidas pela indústria. O CIPL também ressalta que organizações devem continuar trabalhando em tais soluções e compartilhando conhecimentos relevantes com a comunidade de IA.

b. Reconhecendo que sistemas de IA podem ser utilizados em variados contextos, com diferentes níveis de risco para a esfera de direitos dos indivíduos (e.g. traduções automatizadas versus aplicações na medicina), em quais circunstâncias e contextos deve ser preservada a determinação humana em decisões tomadas por sistemas de IA?

Um dos principais atributos da IA é a capacidade de tomar decisões sem intervenção humana. No entanto, existem preocupações justificáveis em entregar autoridade total de tomada de decisão a uma máquina quando sua decisão possa impactar negativamente o indivíduo sujeito de tal decisão. A LGPD tenta resolver esta questão através do Artigo 20, que fornece aos titulares de dados pessoais o direito de solicitar uma revisão das decisões tomadas apenas com base no processamento automatizado de dados pessoais quando estas afetam seus interesses. Isso inclui decisões que visam definir seu perfil pessoal, profissional, de consumidor e crédito, bem como quaisquer aspectos de sua personalidade.[17] O artigo 20(1) também requer que os controladores de dados pessoais ofereçam aos titulares dos dados, sempre que solicitado, informações claras e adequadas sobre os critérios e procedimentos usados para decisões automatizadas, sujeitas ao sigilo comercial e industrial. O artigo 20(2) observa que, quando essas informações não são fornecidas devido ao sigilo comercial ou industrial, a Agência Nacional de Proteção de Dados (ANPD) pode auditar as práticas do controlador de dados em relação a decisões automatizadas.

É importante observar que a LGPD não concede expressamente aos indivíduos o direito de solicitar a revisão humana de decisões automatizadas, mas, em vez disso, fornece a eles um direito mais geral de revisão, que pode incluir intervenção humana, mas também pode ser potencialmente automatizado por natureza.

O CIPL acredita que a metodologia e as ferramentas usadas para a revisão dos processos automatizados de tomada de decisão, incluindo quaisquer elementos de intervenção humana, variarão de acordo com os riscos e o impacto causado ao indivíduo pela decisão. Por exemplo, o uso de tecnologias de

[16] "Em um movimento raramente visto entre empresas de tecnologia, a [Axon] reuniu o conselho independente no ano passado para avaliar as possíveis consequências e custos éticos da inteligência artificial e do software de reconhecimento facial. O primeiro relatório do conselho, publicado quinta-feira, concluiu que 'a tecnologia de reconhecimento facial atualmente não é confiável o suficiente para justificar eticamente seu uso' – orientação que a Axon planeja seguir." Um fabricante de câmeras corporais policiais ainda não utilizará o reconhecimento facial, por dois motivos: Viés e imprecisão, Deanna Paul, 28 de junho de 2019, disponível em https://www.washingtonpost.com/nation/2019/06/29/police-body-cam-maker-wont-use-facial-recognition-yet-two-reasons-bias-inaccuracy/.

[17] Consulte a LGPD, Artigo 20.

reconhecimento facial por companhias aéreas para verificar cartões de embarque, ou por funcionários da alfândega para permitir a entrada de indivíduos em um país, produz decisões muito significativas, pois afetam a liberdade de locomoção de um indivíduo. Quando uma decisão incorreta é alcançada em tais cenários, a intervenção humana compõe um elemento crítico para fornecer reparação suficiente. Por outro lado, se uma tela inteligente em um espaço de varejo apresentar um anúncio destinado a aposentados para um jovem profissional com base no reconhecimento facial – portanto identificando incorretamente a faixa etária do indivíduo –, tal decisão não justificaria intervenção humana imediata ou potencialmente qualquer intervenção. Portanto, nos casos em que a avaliação de risco de decisões automatizadas indica um alto risco para os indivíduos, a intervenção humana pode ser um importante fator de mitigação do risco a ser considerado pelas organizações.

Com relação à estratégia nacional de IA do Brasil, o CIPL recomenda destacar a importância da intervenção humana em contextos de IA em que o resultado de uma decisão automatizada implica um alto risco de dano para o indivíduo. A estratégia nacional de IA também deve reconhecer que as organizações estão mais bem posicionadas e devem ter flexibilidade para definir metodologias e elementos de revisão com base nos riscos identificados para indivíduos, resultantes de atividades específicas de processamento de dados. De fato, a estratégia nacional de IA deve incentivar a exploração e o desenvolvimento de mecanismos de revisão apropriados em diferentes contextos de IA pelas organizações, tendo em vista que a maioria das decisões de IA não justifica qualquer intervenção e que outras medidas relacionadas à *accountability* protegerão adequadamente os indivíduos. Exemplos incluem avaliações éticas e algorítmicas de impacto e a implementação de atenuações adequadas antes da implantação de um sistema de IA, monitoramento contínuo, validações e verificações do algoritmo, uma vez implantado pelo provedor de serviços de IA, e até mecanismos de correção automatizados.

c. De que maneira é possível concretizar a ideia de explicabilidade em sistemas de IA?

A explicabilidade se enquadra no conceito mais amplo de transparência no contexto da IA. É uma maneira de fornecer transparência sobre o resultado de uma decisão ou processo de IA. Conforme observado na Estrutura de Governança de AI da Comissão de Proteção de Dados Pessoais de Cingapura, "[um] algoritmo implantado em uma solução de IA é explicável se for possível explicar como ele funciona e chega a uma previsão específica".[18]

O conceito de explicabilidade pode ser realizado nos sistemas de IA de várias maneiras. Por exemplo:

- **Implementar melhores práticas para facilitar a rastreabilidade**: a rastreabilidade requer a documentação de entradas de dados e outros "conjuntos de dados e processos que produzem a decisão dos sistemas de IA".[19] Ao criar e implementar as melhores práticas ou códigos de conduta com relação à coleta, implantação e uso de dados, as organizações podem melhorar sua rastreabilidade. Por sua vez, isso pode facilitar a explicabilidade.

- **Desenvolver e empregar ferramentas e técnicas de explicabilidade**: em resposta a uma pergunta anterior dessa consulta pública, nós mencionamos o teste de justiça contrafactual no que se refere à prevenção e detecção de viés. Essa técnica também é útil para facilitar a explicabilidade,

[18] Nota *supra* 11, página 13.
[19] Nota *supra* 8, página 20.

pois verifica a equidade nos resultados, determinando se o mesmo resultado é alcançado quando uma variável específica, como raça ou gênero, muda. Se um resultado diferente for alcançado por um sistema de IA quando essa variável for alterada, os cientistas de dados e os engenheiros de IA poderão analisar mais de perto a razão, não apenas para remediar o viés, mas também para explicar, pelo menos em parte, o que está levando o algoritmo a chegar a esse resultado.

- **Considerações no que diz respeito à forma como decisões humanas são tomadas**: frequentemente, seres humanos são incapazes de explicar consistentemente suas preferências por uma opção em detrimento de outra, e há várias situações em que as decisões não são feitas de maneira transparente, como aprovações de empréstimo ou crédito, ou decisões de contratação. Embora possamos pedir uma explicação posterior, essa explicação, na melhor das hipóteses, será lógica e quase certamente não será técnica ou matemática. Considerar abordagens à transparência no mundo off-line pode ajudar a definir o nível e o tipo de transparência a serem buscados ao criar sistemas de IA.

- **Considerações sobre o público envolvido e caso-a-caso**: o que a explicabilidade envolve e o que ela parece ser pode ser diferente dependendo do público envolvido. Por exemplo, uma organização pode precisar explicar um resultado de IA para um indivíduo que é impactado direta e negativamente por uma decisão, um regulador em casos de investigação e organização de *sandboxes* regulatórias de IA, parceiros de negócios interessados em utilizar a solução de IA, ou mesmo para audiências internas à organização ou Conselhos de Diretoria. Esses são públicos distintos que demandam diferentes tipos e requisitos de explicabilidade. Da mesma forma, a explicabilidade pode diferir dependendo do caso-a-caso. Por exemplo, a explicabilidade técnica completa no contexto da detecção e prevenção de fraudes não seria adequada, pois poderia permitir que os fraudadores contornem a solução de IA utilizada para tal detecção e prevenção de fraudes. No entanto, detalhes técnicos podem ser fornecidos aos reguladores, no caso de uma investigação, e sociedade civil e grupos de proteção ao consumidor, para que eles possam fornecer informações aos indivíduos.

- **Considerações alternativas onde a explicabilidade não é viável**: o conceito de explicabilidade é frequentemente desafiado pelo fenômeno da "caixa preta". Conforme observado pela autoridade de proteção de dados pessoais da Noruega, "a caixa preta torna praticamente impossível explicar como as informações são correlacionadas e ponderadas em um processo específico".[20] A caixa preta pode criar resultados surpreendentes e imprevisíveis com um raciocínio invisível ou ininteligível, mesmo para desenvolvedores. Além disso, os sistemas de IA se desenvolvem e mudam conforme mais informações são adicionadas a eles, o que faz com que seja difícil repetir certas tomadas de decisões. Quando não é possível explicar um resultado de IA para indivíduos devido ao problema da caixa preta, outras opções que fornecem informações significativas e empoderamento ao indivíduo devem ser consideradas. Isso inclui a revisão humana das decisões de IA, quando apropriado, além de mecanismos de correção e ferramentas de *feedback*.

Embora o conceito de explicabilidade da IA possa ser implementado de diveras maneiras, implementá-lo nem sempre é apropriado. É importante reconhecer que a divulgação demasiada de informações sobre um algoritmo ou um processo de IA pode não apenas resultar em confusão e sobrecarga de informações

[20] Inteligência Artificial e Privacidade, Datatilsynet (Autoridade Norueguesa de Proteção de Dados), janeiro de 2018, disponível em https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf na página 19.

para indivíduos, ajudando outros a enganar o sistema, como também ameaçar os interesses comerciais da propriedade intelectual, revelando segredos comerciais. De fato, o artigo 20(1) da LGPD estabelece que qualquer informação fornecida pelos controladores de dados aos titulares sobre os critérios e procedimentos de decisões automatizadas deve ser fornecida sob sigilo comercial e industrial. Embora o respeito ao Estado de Direito e aos direitos individuais seja de maior importância, deve-se equilibrá-los com os direitos de organizações inovarem e de propriedade intelectual associados a seus aplicativos e invenções de IA.

Conforme comprovado pelas medidas acima, existem muitas maneiras pelas quais o conceito de explicabilidade pode ser implementado nos sistemas de IA. É importante que organizações tenham flexibilidade em tal implantação com fundamento nos riscos aos indivíduos, dentro de padrões ou parâmetros regulatórios apropriados. Dessa forma, organizações estarão melhor posicionadas para decidir quais métodos são mais adequados para implementar a explicabilidade, uma vez que os aplicativos de IA diferem amplamente de um contexto para outro. Essa abordagem deverá fornecer a combinação necessária de flexibilidade e, conforme apropriado, segurança para que as organizações implementem a explicabilidade de forma efetiva.

Na estratégia nacional de IA, o CIPL recomenda que o MCTIC mencione algumas das várias maneiras pelas quais a explicabilidade pode ser implementada nos sistemas de IA. O CIPL também incentiva as organizações a desenvolverem outras maneiras de facilitar a explicabilidade e a transparência no que se refere aos resultados da IA. O CIPL acredita que o MCTIC deve destacar a importância da inovação e da concorrência, e como divulgações sobre o funcionamento de processos de IA e a tomada de decisões devem ser equilibradas com os direitos comerciais de propriedade intelectual e os interesses comerciais. Por fim, o MCTIC também deve destacar que a flexibilidade baseada no risco, dentro de padrões ou parâmetros regulatórios apropriados, é essencial para a implementação efetiva da explicabilidade em sistemas de IA, considerando a natureza contextual das aplicações de IA.

d. Faz sentido pensar na adoção de uma lei geral para tratar de IA, ou em atualizações pontuais à legislação existente?

Atualmente, muitos países estão considerando regulamentar a IA. Algumas nações alertam contra a regulamentação das tecnologias de IA e acreditam que a adoção de tais leis deve ser limitada. Por exemplo, no início de 2020, o Escritório de Gerenciamento e Orçamento dos EUA lançou um documento preliminar com orientações para a regulamentação de aplicativos de IA.[21] O documento introduz 10 princípios regulatórios para a regulamentação federal dos EUA de aplicativos de IA desenvolvidos e implantados pelo setor privado, enquadrados por um mandato geral para "evitar ações regulatórias ou não regulatórias que dificultam desnecessariamente a inovação e o crescimento da IA".[22] Por outro lado, há nações que são mais favoráveis à regulamentação da IA. Por exemplo, a recentemente nomeada Presidente da Comissão Europeia, Ursula von der Leyen, observou que, durante seus primeiros 100 dias no cargo ela "apresentará legislação para uma abordagem europeia coordenada sobre as implicações

[21] Memorando para os Chefes de Departamentos e Agências Executivas: Orientação para o Regulamento de Aplicações de IA, Escritório de Gerenciamento e Orçamento, 7 de janeiro de 2020, disponível em https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.
[22] *Id*., na página 2.

humanas e éticas da IA".[23] No entanto, parece agora que é mais provável que essa iniciativa assuma a forma de um documento de política que definirá diferentes opções para um arcabouço jurídico sobre IA que pode levar a propostas formais no final do ano.[24] Atualmente, o CIPL está redigindo um documento sobre esta iniciativa e se engajando em discussões com a Comissão Europeia sobre sua proposta.

É importante observar que a maioria dos desafios de proteção de dados identificados no contexto da IA é anterior à mesma e é apresentada por outras tecnologias que não a IA. Portanto, estruturas ou regulamentos legais específicos à IA podem falhar na resolução do problema subjacente e, ao mesmo tempo, potencialmente negar à sociedade os benefícios da IA implementada adequadamente. Além disso, qualquer tipo de regulamentação que não seja neutra em termos de tecnologia pode se sobrepor ou duplicar regulamentações (horizontais) já existentes, o que seria prejudicial à segurança jurídica. Nos casos em que a regulamentação da IA é inevitável, ela deve ser desenvolvida com ponderação e com tempo suficiente para permitir que várias partes interessadas identifiquem, articulem e implementem os principais princípios e melhores práticas.[25] Em curto prazo, no entanto, atender aos objetivos de aprimorar a proteção de dados exigirá soluções e ferramentas neutras em termos de tecnologia que podem ser aplicadas em uma variedade de situações e contextos.

Na medida em que o Brasil opta por regulamentar a tecnologia da IA, o CIPL acredita que os legisladores devem abordar a legislação da IA em relação aos seguintes princípios gerais:

- **Desenvolver estruturas legais existentes** – incluindo leis horizontais e setoriais específicas – que já fornecem as estruturas de linha de base, requisitos, ferramentas e soluções para governança responsável e uso da IA.

- **Adotar uma abordagem regulatória baseada em princípios e resultados** capaz de se adaptar à variedade e à natureza em rápida evolução das tecnologias relacionadas à IA e aos desafios exclusivos de setores específicos. Essa abordagem também deve evitar regras excessivamente rígidas e prescritivas e permitir que organizações operacionalizem esses princípios desenvolvendo práticas de IA responsáveis e baseadas em riscos, que alcancem os resultados identificados.

[23] "Uma união que luta por mais: meus planos para a Europa, diretrizes políticas para a próxima Comissão Europeia", Ursula von der Leyen, disponível em https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, na página 13 ("Nos meus primeiros 100 dias de mandato, apresentarei legislação para uma abordagem europeia coordenada sobre as implicações éticas e humanas da inteligência artificial").

[24] Consulte "As próximas regras de inteligência artificial da Europa, explicadas" Janosch Delcker, Politico.eu, 10 de janeiro de 2020, disponível em https://www.politico.eu/pro/europes-upcoming-artificial-intelligence-rules-explained-european-commission/.

[25] "A tecnologia da IA precisa continuar se desenvolvendo e amadurecendo antes que possam ser criadas regras para governá-la. É necessário chegar a um consenso sobre os princípios e valores da sociedade para governar o desenvolvimento e o uso da IA, seguidos pelas melhores práticas para cumpri-los. Então, provavelmente estaremos em uma posição melhor para os governos criarem regras legais e regulamentares para que todos sigam." O Futuro Computado, Microsoft (2018), disponível em https://blogs.microsoft.com/wp-content/uploads/2018/02/The-Future-Computed_2.8.18.pdf, na página 9.

- **Fazer um "teste de equilíbrio de riscos/benefícios" e avaliação de impacto contextual**, que são ferramentas-chave para apoiar o uso benéfico da IA, evitar retenção de riscos e permitir mitigação adequada de riscos.

Além disso, o CIPL apoia uma abordagem regulatória em camadas para a IA que, no contexto brasileiro, significa:

- Basear-se nas regras da LGPD e tornar a LGPD um facilitador da IA por meio de uma visão prospectiva e interpretação progressiva dos requisitos da ANPD;

- Alavancar e incentivar práticas de *accountability* relacionadas à IA nas organizações (consulte a resposta às perguntas de consulta relacionadas à Governança da IA); e

- Promover abordagens inovadoras para a supervisão regulatória (por exemplo, *sandboxes* e *hubs* regulatórios, onde os reguladores de diferentes disciplinas com interesse em IA podem trocar pontos de vista, resolver conflitos de leis, etc.).

Como o MCTIC deseja saber se deve haver uma lei geral para abordar a IA ou se atualizar a legislação existente seria mais apropriado, o CIPL recomenda que a estratégia nacional de IA envolva, antes de tudo, consideração às regras contidas na LGPD e sua interseção com a tecnologia da IA. De fato, a LGPD fornece um bom limiar de proteção com relação aos aplicativos de IA que processam dados pessoais e consagra princípios e valores éticos importantes que são de particular relevância para resolver os desafios impostos pela IA (por exemplo, justiça e transparência). Qualquer política ou esforço legislativo relacionado à AI deve permanecer consistente com a LGPD e deve evitar duplicar as regras que já estão em vigor.

Além disso, o MCTIC deve promover a *accountability* como um meio eficaz de governança da IA na estratégia nacional de IA (consulte a resposta às perguntas de consulta relacionadas à governança da IA). Na medida em que o Brasil adotar qualquer forma de regulamentação da IA, o MCTIC deve solicitar que essa regulamentação seja tecnologicamente neutra e baseada em princípios e resultados. Além disso, a estratégia nacional de IA do Brasil deve promover abordagens inovadoras de regulamentação, incluindo *sanboxes* regulatórias (veja a resposta às perguntas de consulta relacionadas à governança da IA) e iniciativas de prototipagem de políticas.

Finalmente, o MCTIC deve exigir consistência na regulamentação da IA. A IA é uma indústria global e ter vários regimes regulatórios divergentes e potencialmente conflitantes pode impedir o uso benéfico da IA e prejudicar a capacidade do Brasil de participar da economia global baseada na IA, sem fornecer proteção significativa aos indivíduos.

e. Que papel pode ser desempenhado por códigos de conduta, regras de boas práticas corporativas e padrões voluntários?

- **Códigos de Conduta e Certificações**: o CIPL acredita que códigos de conduta, certificações e esquemas de prestação de contas equivalentes podem desempenhar um papel importante para garantir a prestação de contas dos sistemas de IA e seu desenvolvimento deve ser promovido na estratégia nacional de IA do Brasil. Por exemplo, a criação de códigos de conduta relacionados à coleta, implantação e uso de dados pode ajudar a melhorar rastreabilidade. Isso pode ajudar a

garantir a equidade, a realização de auditorias e a promover explicabilidade. Esses esquemas também podem demonstrar a devida diligência no contexto dos provedores de serviços de IA e permitir que as organizações transfiram dados de forma responsável, segura e eficiente, onde essas entidades possuem uma certificação relevante ou participem de um código de conduta relevante. O uso de certificações e códigos de conduta para este último objetivo é especialmente importante, pois a IA requer quantidades substanciais de dados para um desempenho ideal e, como resultado, os dados devem poder fluir e ser distribuídos entre os diferentes sistemas de IA. A estratégia nacional de IA também deve destacar que qualquer estrutura proposta para códigos de conduta ou certificações deve ser ágil e flexível para atender às demandas de novas tecnologias, dado o ritmo dos desenvolvimentos na área de IA.

- **Regras de boas práticas corporativas**: o CIPL acredita que as regras de boas práticas corporativas são essenciais para alcançar e operacionalizar a responsabilidade da IA nas organizações e formam o núcleo do uso responsável e ético dos aplicativos de IA. O CIPL discute a responsabilidade da IA em detalhes em nossa resposta às perguntas de consulta relacionadas à Governança da IA.

- ***Standards* (padrões) voluntários**: da mesma maneira que códigos de conduta e certificações voluntários podem garantir *accountability* relacionada à IA, o CIPL acredita que padrões voluntários, e ainda assim executáveis, tenham um papel igualmente importante a esse respeito. Os padrões voluntários se mostraram úteis em muitas áreas de privacidade e proteção de dados, incluindo transferência e segurança de dados. O CIPL recomenda que o MCTIC exija o desenvolvimento de tais padrões voluntários em sua estratégia nacional de IA, que devem ser desenvolvidos em colaboração com a indústria, reguladores (incluindo a ANPD), profissionais de privacidade e outras partes interessadas. Tais normas devem ser complementares ao quadro jurídico existente, a fim de garantir segurança jurídica.

III. Governança da IA

Na consulta pública em questão, o MCTIC observa que estão começando a evoluir os debates sobre estruturas de governança que promovem métodos e procedimentos para garantir o cumprimento dos princípios de uso ético da IA. O CIPL acredita que uma estrutura de governança baseada nos elementos essenciais de *accountability* fornece uma estrutura flexível e robusta que permite usos inovadores e responsáveis da IA, e facilita a implementação de todos os requisitos de proteção de dados aplicáveis, ou outros padrões de privacidade, por meio de um programa abrangente de privacidade.

a. De que maneira pode-se avaliar se os sistemas de inteligência artificial, especialmente no âmbito do setor público, estão atingindo seus objetivos?

- ***Accountability* nas organizações**: o MCTIC destaca a importância de criar rotinas de gerenciamento, monitoramento e supervisão de riscos no uso de sistemas de IA ao longo de todo o ciclo de vida da IA. Esses processos são parte integrante do conceito de *accountability*. De fato, orientações para a implementação de tais processos que promovsm a implementação responsável e *accountable* da IA, enquanto ainda permitem inovação tanto em tecnologia quanto nos processos usados para obter proteção de dados, já foram desenvolvidas em outros países, incluindo Cingapura (por meio do Modelo de Estrutura de Governança de Inteligência Artificial da

Comissão de Proteção de Dados Pessoais de Cingapura Estrutura de Governança),[26] Reino Unido (através da Estrutura de Auditoria de IA do Gabinete do Comissário da Informação) [27] e União Europeia (por meio do *High Level Expert Group on AI Ethics* da Comissão Europeia sobre as Diretrizes de Ética da IA para IA Confiável).[28]

Há muitos anos, o CIPL tem atuado como um defensor da *accountability* na proteção de dados pessoais e escreveu extensivamente sobre o assunto.[29] O *Accountability Framework* do CIPL, que compreende os elementos essenciais da *accountability* (ou seja, liderança e supervisão; avaliação de riscos; políticas e procedimentos; transparência; treinamento e conscientização; monitoramento e verificação; resposta e execução), foi usada para promover a prestação de contas organizacional no contexto mais amplo da construção, implementação e demonstração de programas abrangentes de conformidade com regras sobre privacidade e proteção de dados pessoais. Da mesma forma, conforme discutido no segundo relatório de IA do CIPL,[30] este *framework* também pode ser usado para ajudar organizações, tanto no setor público quanto privado, a desenvolver, implementar e organizar medidas de proteção de dados robustas e abrangentes no contexto da IA e demonstrar *accountability* em IA.

O CIPL recomenda que, na estratégia nacional de IA, o MCTIC enfatize a importância da *accountability* para alcançar uma governança eficaz da IA. A *accountability* foi codificada na LGPD (Artigo 6 (X) e o Artigo 50 da LGPD) e os seus requisitos mapeiam os elementos essenciais da *accountability* mencionados acima.

- ***Sandbox* regulatória**: outro mecanismo que pode ser usado para avaliar se os sistemas de IA estão atingindo seus objetivos é testar o sistema em uma *sandbox* regulatória de IA antes de sua implantação no mercado mais amplo. A *sandbox* regulatória é um "porto seguro" supervisionado, que incentiva e apoia a inovação de maneira a cumprir requisitos legislativos e outros. A participação na *sandbox* normalmente envolve o estabelecimento de um fórum por um regulador, onde as organizações podem experimentar e testar produtos, serviços, modelos de

[26] Consulte nota *supra* 11.
[27] Estrutura de auditoria da AI, Gabinete do Comissário de Informação do Reino Unido, disponível em https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework/.
[28] Consulte nota *supra* 8, geral.
[29] Consulte os *whitepapers* do CIPL sobre Caso sobre Prestação de Contas: como ela permite proteção e confiança de dados efetivas na sociedade digital, 23 de julho de 2018, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; Incentivando a Responsabilidade: Como as autoridades de proteção de dados e legisladores podem estimular a responsabilização, 23 de julho de 2018, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; e as Perguntas e Respostas do CIPL sobre Responsabilidade, 3 de julho de 2019, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf.
[30] Consulte nota *supra* 6.

negócios e mecanismos de entrega inovadores em um mercado ao vivo, com um número limitado de consumidores reais, sob a supervisão do regulador.

O conceito de *sandbox* regulatória surgiu no setor de serviços financeiros. De fato, em junho de 2019, a Secretaria Especial de Finanças do Ministério da Economia, o Banco Central do Brasil, a Comissão de Valores Mobiliários do Brasil e a Superintendência de Seguros Privados do Brasil anunciaram sua intenção de coordenar e implementar um regime de *sandbox* regulatória no Brasil em resposta à transformação que está ocorrendo nos setores financeiro, de capitais e de seguros.[31] O anúncio destaca ainda que a *sandbox* regulatória tratará de tecnologia de contabilidade distribuída, blockchain, bots e IA.

Sandbox regulatórios estão sendo adotados cada vez mais no âmbito da proteção de dados. Por exemplo, o Gabinete do Comissário de Informação (agência reguladora de proteção de dados) do Reino Unido lançou uma fase beta de sua *sandbox* regulatória de proteção de dados em 2019.[32]

Também estamos vendo *sandbox* regulatórios sendo adotados no âmbito da IA. O conceito foi mencionado nas estratégias nacionais de IA de vários países. Por exemplo, em dezembro de 2017, o Ministério Finlandês de Assuntos Econômicos e Emprego publicou um relatório sobre a estratégia nacional de IA da Finlândia, que observa que uma estrutura que garante a disponibilidade de dados deve ser criada e que um ambiente de experimentação de *sandbox* regulatórios pode ser criado como forma de incentivar o compartilhamento de dados.[33] Além disso, em dezembro de 2019, o Ministério da Ciência e ICT da Coreia do Sul anunciou que estaria criando uma *sandbox* regulatória na estratégia nacional do país para o desenvolvimento de IA.[34]

Os *sandbox* regulatórios de IA também parecem ser exigidos por novas leis de proteção de dados em todo o mundo. Por exemplo, em Malta, uma legislação específica abriu caminho para uma *sandbox* regulatória para testar a IA em relação a resultados funcionais predeterminados.[35] Além disso, o Projeto de Lei de Proteção de Dados Pessoais da Índia, recentemente introduzido no Parlamento, inclui uma disposição que exige que a autoridade de proteção de dados da Índia, com

[31] Comunicação conjunta da Comissão de Valores Mobiliários sobre a intenção de implementar uma sandbox de regulamentação para os setores brasileiro de finanças, seguros e indústria de valores mobiliários, 13 de junho de 2019, disponível em http://www.cvm.gov.br/noticias/arquivos/2019/20190613-1.html.
[32] Sandbox de Regulamentação (Fase Beta), Gabinete do Comissário de Informação do Reino Unido, disponível em https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/.
[33] Era da Inteligência Artificial da Finlândia, Ministério de Assuntos Econômicos e de Emprego da Finlândia, dezembro de 2017, disponível em http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y na página 44.
[34] Estratégia Nacional da Coreia do Sul para Inteligência Artificial, dezembro de 2019, disponível em https://www.msit.go.kr/cms/www/m_con/news/report/__icsFiles/afieldfile/2019/12/24/%EC%9D%B8%EA%B3%B5%EC%A7%80%EB%8A%A5%20%EA%B5%AD%EA%B0%80%EC%A0%84%EB%9E%B5.pdf
[35] Lei de Autoridade de Inovação Digital de Malta, disponível em http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12873&l=1.

o objetivo de incentivar a inovação em IA, aprendizado de máquina ou qualquer outra tecnologia emergente de interesse público, crie uma *sandbox* regulatória.[36]

O CIPL recomenda que o MCTIC requisite que a ANPD crie *sandbox* regulatórios relacionados à IA em sua estratégia de IA e que recorra à experiência de reguladores e governos, tanto interna quanto globalmente, para estabelecer sua própria *sandbox*. O CIPL também escreveu extensivamente sobre *sandbox* regulatórios de proteção de dados[37] e esses estudos podem ser úteis ao MCTIC já que este considera incluir o conceito de *sandbox* regulatória em sua estratégia de IA.

b. Seria útil conveniente estabelecer a obrigatoriedade de elaboração de relatórios prévios de avaliação de impacto quanto ao uso de IA em determinados setores?

A avaliação de riscos é um componente essencial da *accountability* e um requisito essencial das leis modernas de proteção de dados. Uma maneira comum de avaliar o impacto do tratamento de dados pessoais é a chamada avaliação de impacto na proteção de dados (*Data Protection Impact Assessment*, DPIA). Por exemplo, na Lei Geral de Proteção de Dados da União Europeia (GDPR), DPIAs são necessários no contexto da tomada de decisões automatizadas que produzem efeitos legais ou de significância semelhante.[38] De fato, no Brasil, o Artigo 38 da LGPD afirma que a ANPD pode exigir que um responsável pelo tratamento de dados pessoais elabore um relatório de impacto sobre a proteção de dados pessoais, incluindo dados confidenciais, relacionado ao seu processamento de dados. Esse relatório deve conter, pelo menos, uma descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para garantir a segurança da informação, bem como as medidas, salvaguardas e mecanismos adotados para mitigar os riscos.

Essas avaliações podem ter valor adicional no contexto da IA e algumas organizações estão desenvolvendo DPIAs específicas à IA (ou avaliações de impacto da IA), como um complemento às avaliações exigidas pela lei de proteção de dados ou como uma avaliação totalmente separada. Essas avaliações de impacto da IA podem estruturar a maneira como as organizações avaliam questões de justiça, direitos humanos ou outras considerações na implantação de novas tecnologias de IA. Elas também podem ajudar as organizações a incorporarem valores corporativos em seus processos e, eventualmente, fornecerão uma estrutura de casos pré-aprovados para definir guias para avaliar inovações futuras. Além disso, essas avaliações podem ajudar organizações a desenvolverem a documentação necessária para fornecer transparência efetiva aos reguladores e indivíduos.

---

[36] Lei de Proteção de Dados Pessoais da Índia nº 373 de 2019, disponível em http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[37] Sandboxes de regulamentação em proteção de dados – engajamento construtivo e regulamentação inovadora na prática, 8 de março de 2019, disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

[38] GDPR, artigo 22; veja também GDPR, Artigo 35(1) ("Quando um tipo de processamento em particular, que utiliza novas tecnologias e leva em conta a natureza, escopo, contexto e objetivos do processamento, provavelmente resultará em um alto risco para os direitos e liberdades das pessoas, o responsável pelo tratamento dos dados deve, antes do processamento, avaliar o impacto das operações de processamento previstas na proteção de dados pessoais").

É importante ressaltar que qualquer processo de avaliação de impacto de IA também deve equilibrar os benefícios e riscos concretos da IA. Riscos relacionados a um sistema específico de IA considerados altos podem ser superados por benefícios aos indivíduos e à sociedade em geral. Por exemplo, a IA oferece enormes benefícios quando usada para monitorar o conteúdo em plataformas on-line, a fim de evitar terrorismo, abuso infantil ou outro comportamento criminoso, o que pode superar o risco associado ao tratamento de dados pessoais.

Para ajudar ainda mais as organizações a avaliarem adequadamente o impacto da IA e equilibrarem benefícios e riscos, os chamados "riscos de reticência" (ou seja, qual seria a consequência para os indivíduos e a sociedade de não avançar com um projeto específico relacionado à IA devido a riscos potenciais?) também devem fazer parte da avaliação para garantir que todos os fatores relevantes sejam considerados e para informar a decisão final.

Além disso, deve ser mais explorado e promovido o desenvolvimento de *frameworks* de avaliação de impacto específicos à determinados setores indústria.

Embora o CIPL acredite que a estratégia de IA do Brasil deva mencionar e fazer referência à importância das avaliações de impacto no contexto da IA, o CIPL adverte contra impor uma exigência geral de preparar avaliações de impacto prévias para o uso da IA em determinados setores da indústria. Como exemplo, inúmeras “listas de restrições” nacionais sobre o tratamento de dados que automaticamente exigem uma DPIA foram emitidas por diferentes autoridades de proteção de dados da União Europeia em cumprimento à GDPR. Tais listas levaram à exigências e expectativas irreais e incontroláveis por organizações que operam na União Europeia. Na visão do CIPL, qualquer referência à risco ou abordagem baseada em risco no contexto de aplicativos de IA descrita na estratégia nacional de IA deve permitir a calibração de requisitos legais e medidas de conformidade com os riscos reais para os indivíduos associados ao aplicativo de IA e ao contexto em questão. A LGPD já é bastante prescritiva, pois a ANPD possui ampla autoridade para exigir que um controlador de dados realize uma avaliação de impacto.

A estratégia nacional de IA deve destacar ainda que as estruturas de avaliação de impacto específicas à determinados setores da indústria podem ajudar organizações a lidarem com riscos exclusivos a tais setores e devem constituir parte essencial dos recursos de avaliação de riscos de uma organização. No entanto, não deve haver um requisito padrão para realização de avaliação de risco prévia em todas as aplicações de IA em um determinado setor, pois isso pode levar a milhares de avaliações de risco sendo conduzidas em tecnologias de IA que representam pouco ou nenhum risco para os indivíduos.

IV. <u>Aspectos internacionais</u>

a. Quais parcerias internacionais, seja com governo, empresas ou instituições de pesquisa e ensino, deveriam ser buscadas em prol do desenvolvimento de IA no Brasil?

Como as tecnologias de IA impactam muitas partes interessadas diferentes, áreas de regulamentação e a sociedade em geral, o CIPL recomenda que o Brasil procure trabalhar com diversos parceiros internacionais no desenvolvimento do uso e implantação responsáveis da IA. Isso pode incluir fóruns internacionais, como a Organização de Cooperação e Desenvolvimento Econômico ou grupos regionais, como o *High-Level Expert Group on AI* da Comissão Europeia ou o *Ad Hoc Committee on AI* do Conselho

da Europa. Outras parcerias incluem instituições de pesquisa internacionais, universidades e empresas multinacionais que trabalham em aplicações e iniciativas de IA.

O CIPL colaborou com muitas partes interessadas internacionais na discussão e formulação de soluções para algumas das questões mais prementes e desafiadoras da IA. Isso inclui autoridades globais de proteção de dados, legisladores e formuladores de políticas, instituições da União Europeia, órgãos governamentais nacionais, organizações multinacionais e academia. O CIPL continuará trabalhando em questões relacionadas à IA e, nesse sentido, louva a oportunidade de responder a outras consultas do MCTIC e de se envolver com o Brasil em importantes tópicos relacionados à IA.

Conclusão

O CIPL agradece a oportunidade de responder ao Departamento de Telecomunicações do Ministério da Ciência, Tecnologia, Inovações e Comunicações em sua consulta pública sobre uma estratégia nacional de inteligência artificial para o Brasil.

Se desejar discutir algum dos comentários deste documento ou precisar de informações adicionais, entre em contato com Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Sam Grogan, sgrogan@huntonAK.com; Matthew Starr, mstarr@huntonAK.com ou Giovanna Carloni, gcarloni@huntonAK.com.