ESTRATÉGIA NACIONAL BRASILEIRA DE INTELIGÊNCIA ARTIFICIAL

COMENTÁRIOS DA BSA | THE SOFTWARE ALLIANCE
31 DE JANEIRO DE 2020

Introdução e Resumo do Conteúdo

BSA | The Software Alliance (**BSA**)[1] agradece ao Ministério da Ciência, Tecnologia, Inovação e Comunicações (**MCTIC**) por esta oportunidade de contribuir com a consulta sobre a *Estratégia Nacional Brasileira de Inteligência Artificial* (**Estratégia**)[2].

A BSA é a principal defensora da indústria global de software perante governos e no mercado internacional. Nossos membros estão na vanguarda da inovação baseada em softwares que está alimentando o crescimento econômico global, incluindo produtos e serviços de computação em nuvem e inteligência artificial (**IA**). Os membros da BSA incluem muitos dos principais fornecedores mundiais de software e serviços online e fizeram investimentos significativos no desenvolvimento de soluções inovadoras de IA para uso em uma variedade de aplicativos.

Como líderes no desenvolvimento de IA, os membros da BSA têm ideias únicas sobre o tremendo potencial da IA e as políticas governamentais que podem melhor apoiar o uso responsável da IA e garantir a inovação contínua. Para esse fim, a BSA identificou cinco pilares[3] essenciais para o desenvolvimento de estruturas de IA responsáveis. Esses pilares, com os quais o documento de consulta da **Estratégia** está amplamente alinhado, refletem o fato de que tanto a indústria quanto o governo têm papéis importantes a desempenhar na promoção dos benefícios e na mitigação dos riscos potenciais envolvidos no desenvolvimento, implantação e uso da IA:

Criando confiança e responsabilidade em Sistemas de IA: Destacar os esforços do setor para garantir que os sistemas de IA sejam desenvolvidos de maneira a maximizar a equidade, a precisão, a proveniência dos dados, a explicabilidade e a responsabilidade.

Política Sólida de Inovação em Dados: Promover políticas de dados favoráveis ao desenvolvimento da IA, incluindo mecanismos legais confiáveis que facilitam a transferência transfronteiriça de dados, segurança jurídica para serviços de valor agregado (por exemplo, mineração de textos e dados, aprendizado automático) e acesso aprimorado a dados governamentais não sensíveis.

---

[1] Os membros da BSA' incluem: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, e Workday.

[2] Disponível em: http://participa.br/profile/estrategia-brasileira-de-inteligencia-artificial

[3] Para mais informações sobre tais pilares, visite https://www.ai.bsa.org

1) **Segurança Cibernética e Proteção à Privacidade:** Defender políticas que fortaleçam medidas de segurança aprimoradas e respeitem as escolhas informadas dos consumidores, ao mesmo tempo que garantem a capacidade de fornecer produtos e serviços personalizados valiosos.

2) **Pesquisa e Desenvolvimento:** Apoiar o investimento em esforços que promovam a confiança nos sistemas de IA; promovam a coordenação e a colaboração entre o setor e o governo e ajudem a desenvolver o fluxo da mão de obra de IA.

3) **Desenvolvimento de Mão-de-Obra**: Identificar oportunidades para o governo e a indústria colaborarem em iniciativas para preparar a mão de obra para novos e emergentes empregos.

A BSA agradece a oportunidade de contribuir para o desenvolvimento da Estratégia atualmente sendo desenvolvida pelo MCTIC e oferecemos os seguintes comentários e recomendações, que se concentram em aspectos importantes para a criação de um ecossistema de IA seguro e confiável, para aprimorar ainda mais a Estratégia. Nossos comentários detalhados seguem a ordem dos temas selecionados da discussão estabelecidos no formulário de consulta on-line da Estratégia. Nossos comentários também incluem um comentário adicional abrangente sobre a importância de incorporar a segurança de software como um princípio fundamental da Estratégia.

Comentários Detalhados

A. Comentário Abrangente: Incorporação de Segurança de Software como um Princípio Fundamental

A BSA sugere ao MCTIC considerar aprimorar ainda mais a **Estratégia**, incluindo a segurança de software como um de seus princípios fundamentais. À medida que a IA e outras tecnologias digitais criam cada vez mais uma economia globalmente conectada, é fundamental garantir que os sistemas de IA sejam projetados para mitigar riscos de segurança previsíveis. Portanto, o Framework se beneficiaria da inclusão de considerações relacionadas à proteção de software durante todo o seu ciclo de vida. Os recursos por softwares expandiram-se dos programas de computador tradicionais e sistemas de controle industrial para a IA e tecnologias emergentes. Isso inclui sensores amplamente implantados, dispositivos inteligentes, veículos conectados e sistemas robóticos. Portanto, é imperativo que os desenvolvedores de software, incluindo aqueles que desenvolvem soluções e aplicativos de IA, garantam que o software seja construído e mantido com segurança durante todo o seu ciclo de vida. Nesse sentido, a BSA publicou um *Framework para Software Seguro*[4] que serve como uma referência abrangente para considerações de segurança de software.

A BSA recomenda que as considerações de segurança de software sejam consideradas um princípio fundamental da Estratégia, para enfatizar a importância de sistemas e software seguros como parte da IA ética.

B. Tema de Discussão 1 – Legislação, Regulação e Uso Ético da IA

Legislação e Regulação

A consulta sobre **a Estratégia** convida as partes interessadas a compartilhar sua opinião sobre se uma lei ampla da AI seria apropriada ou, em vez disso, as leis e/ou regulamentos existentes devem ser atualizados para abordar questões relacionadas à AI.

Dado o amplo conjunto de questões subjacentes e os infinitos casos de uso em potencial para a IA, uma abordagem de regulamentação única seria contraproducente. Para muitas das questões, é

[4] Detalhes disponíveis em https://www.bsa.org/reports/bsa-framework-for-secure-software.

provável que uma abordagem excessivamente regulamentada iniba o desenvolvimento, a implantação e o crescimento da IA, em detrimento da economia brasileira. Em vez de focar em uma regulamentação única ou em uma série de novas regulamentações para abordar a IA, o Brasil deve garantir que as estruturas regulatórias existentes sejam modernizadas para acomodar a adoção da IA e, onde necessário, desenvolver respostas políticas personalizadas para questões específicas com base em ampla consulta a várias partes interessadas. Nesses casos, é importante que o Governo do Brasil mantenha esses regulamentos alinhados com as tendências internacionais emergentes e as melhores práticas.

Um exemplo de uma regulamentação atual que deve ser atualizada para promover o desenvolvimento da IA é a Lei de Direitos Autorais do Brasil. O Brasil deve alterar sua Lei de Direitos Autorais para incluir uma linguagem específica que permita usos de análise de dados (mineração de texto e dados) para evitar qualquer dúvida sobre a natureza não infratora de tais usos.

O desenvolvimento de algoritmos que alimentam os sistemas de IA exige que os pesquisadores desenvolvam modelos matemáticos treinados usando grandes quantidades de dados. Uma disposição da lei de direitos autorais para permitir a análise de informações é muito importante para estimular a inovação. A questão é que o processo de aprendizado automático pode envolver a criação de reproduções legíveis por máquina do material usado no aprendizado automático. Como as cópias incidentais criadas como parte do processo de aprendizado de máquina são feitas com o único objetivo de analisar as informações factuais (ou seja, não protegidas por direitos autorais) de conteúdo acessado legalmente e não estão relacionadas à expressão criativa incorporada nas obras subjacentes, elas são substituem original ou comprometem de alguma forma os interesses legítimos de um proprietário de direitos autorais. No entanto, na ausência de uma exceção de direitos autorais para essa atividade, os pesquisadores podem relutar em realizar P&D importantes devido à potencial incerteza jurídica.

Reconhecendo a enorme oportunidade que a IA apresenta para promover o crescimento econômico e enfrentando muitos dos desafios sociais mais incômodos, os governos ao redor do mundo estão tomando medidas para garantir que os direitos autorais não sejam uma barreira à inovação. À medida que os governos examinam suas estruturas legais para garantir que não estão impedindo inadvertidamente o desenvolvimento da IA, há uma crescente conscientização global sobre a necessidade de modernizar as leis de direitos autorais para facilitar o desenvolvimento da IA. Nos Estados Unidos, por exemplo, as reproduções usadas para análise ou pesquisa são consideradas um uso justo. Mas em sistemas jurídicos que não possuem uma disposição flexível de uso justo, como é o caso do Brasil, a tendência tem sido buscar exceções específicas para esclarecer que o tipo de cópia envolvido no treinamento de um sistema de IA não se trata de uma violação legal. Nos últimos anos, Japão, Canadá, Austrália, União Europeia e Cingapura tomaram medidas para garantir que os direitos autorais não sejam uma barreira ao desenvolvimento da IA. Portanto, é extremamente importante criar uma disposição de análise de dados específica para evitar qualquer dúvida sobre a natureza não infratora dos usos da análise de dados. Isso ajudará a promover a inovação por meio do uso contínuo da análise de dados para fins de inovação, sem barreiras potenciais que a ameaça de possíveis sanções legais por violação de direitos autorais possa representar.

A BSA sugere ao governo do Brasil evitar uma regulação única ou regulamentação excessiva da IA e, em vez disso, desenvolver respostas políticas personalizadas para questões específicas com base em uma ampla consulta de várias partes interessadas e nas melhores práticas internacionais. Um exemplo dessa abordagem seria uma emenda à atual Lei de Direitos Autorais para incluir uma linguagem que permita claramente o uso da análise de informações (exceção para Mineração de Textos e Dados).

Uso Ético da IA

A BSA também aprecia o foco da **Estratégia** na importância dos princípios éticos da IA destacados ao longo do documento de consulta. Nesse sentido, é importante reconhecer as diferentes partes interessadas na cadeia de valor da IA e a importância de suas respectivas funções e responsabilidades na promoção da IA ética (por exemplo, fornecedores de soluções de IA, entidades que implantam e usam a IA e usuários finais). Assim como a segurança de software, a "IA ética" requer uma abordagem ao longo do ciclo de vida para gerenciamento de riscos, que inclui antecipar

e abordar riscos que podem surgir quando os sistemas são projetados, depois de implementados e quando estão sendo desativados.

Não existe uma abordagem única para o gerenciamento de riscos ao longo do ciclo de vida da IA. De fato, as melhores práticas de gerenciamento de riscos devem ser adaptadas para levar em consideração o modelo de desenvolvimento e o contexto de implantação de um sistema de IA. A alocação das funções e responsabilidades apropriadas para gerenciar os riscos de IA também deve levar em consideração essas considerações. Por exemplo, a entidade que implanta uma solução de IA provavelmente estará melhor posicionada (em comparação com o desenvolvedor da solução de IA) para implementar mecanismos de recurso apropriados para abordar os problemas que possam surgir através do uso do sistema.

A Organização para Cooperação e Desenvolvimento Econômico (OCDE) reconheceu a importância crítica de distinguir os vários envolvidos na IA quando adotou os princípios subjacentes à Recomendação do Conselho de Inteligência Artificial[5]. Os princípios da OCDE reconhecem que a comunidade de partes interessadas da IA "abrange todas as organizações e indivíduos envolvidos, ou afetados por sistemas de IA, direta ou indiretamente". Além disso, os princípios da OCDE reconhecem que políticas efetivas de IA devem necessariamente levar em conta as "partes interessadas de acordo com seu papel e o contexto "no qual a IA está sendo implantada. Incluir essa distinção conceitual seria útil para diferentes partes interessadas, pois elas realizam avaliações de risco para determinar as medidas apropriadas a serem adotadas para o desenvolvimento, implantação e uso da IA. Além disso, também seria útil, tanto para os fornecedores de soluções de IA quanto para as entidades que implantam e usam a IA, considerar quem será o usuário final da solução de IA - em geral, as empresas de usuários finais devem ser consideradas usuários mais sofisticados do que os indivíduos-usuários finais - e isso, por sua vez, teria implicações nas avaliações internas de riscos e na viabilidade comercial.

A BSA recomenda que a Estratégia reconheça e discuta os papéis e responsabilidades importantes que vários interessados, incluindo o governo brasileiro, têm na implementação da IA ética e no gerenciamento dos riscos correspondentes.

C. Tema de Discussão 2 – Governança da IA

A **Estratégia** acolhe os pensamentos das partes interessadas sobre se o Brasil deve adotar políticas de dados abertos que respeitam à privacidade para ajudar a treinar algoritmos de IA e evitar desvios.

A BSA suporta uma política de dados abertos por meio da qual os dados governamentais não sensíveis devem ser abertos, disponíveis e utilizáveis pelo público em geral. Essa abordagem será mais eficaz se promover um ecossistema robusto de compartilhamento de dados entre partes interessadas governamentais e não governamentais. Para atingir esse objetivo, o Governo do Brasil deve considerar mecanismos para identificar e mitigar fontes de atrito que possam inibir o compartilhamento de dados do governo. Esse esforço deve incluir uma avaliação de como as agências podem alavancar tecnologias emergentes e processos de governança de dados para aprimorar as proteções de privacidade, além de disponibilizar mais dados ao público. As agências governamentais devem considerar o uso de tecnologias de ponta e processos de governança de dados que possam facilitar um maior acesso aos dados, salvaguardando a privacidade do usuário, incluindo a possibilidade de utilizar abordagens de "acesso em camadas" para proteção de dados[6], frameworks de privacidade diferencial [7], e encriptação homomórfica [8].

[5] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[6] Uma abordagem de acesso em camadas à governança de dados permitiria às agências disponibilizar versões públicas de conjuntos de dados sensíveis, eliminando informações pessoais. *Consultar* Comm'n on Evidence-Based Policymaking, The Promise of Evidence-Based Policymaking [Comentário sobre Formulação de Políticas com Base em Evidências, a Promessa de Formulação de Políticas com Base em Evidências] 5 (2017) na p. 38 (“O acesso em camadas é uma aplicação de minimização de dados, uma importante proteção da privacidade para a construção de evidências, conforme incorporada nos Princípios da Prática Justa de Informações (descritos no Capítulo 3). Minimização de dados significa dar acesso à menor quantidade de dados necessária para concluir um projeto aprovado. Por exemplo, o projeto de um pesquisador qualificado pode obter aprovação para acesso a informações confidenciais em um data center de pesquisa altamente seguro que requer

A BSA sugere ao governo do Brasil se comprometer a garantir que as agências governamentais disponibilizem todos os ativos de dados governamentais não sensíveis livremente sob uma licença aberta e em formatos legíveis por máquina.

A **Estratégia** também deve reconhecer expressamente o papel exclusivamente importante que as transferências transfronteiriças de dados desempenham no desenvolvimento e uso da IA. O fluxo livre de dados é parte integrante de todas as etapas do ciclo de vida da IA, desde o desenvolvimento de modelos preditivos até a implantação e o uso de sistemas de IA. Os dados usados nos sistemas de IA geralmente se originam de muitas fontes geograficamente dispersas. Muitas soluções de IA usadas no Brasil são desenvolvidas internacionalmente e oferecidas em nuvem. Da mesma forma, as soluções de IA desenvolvidas no Brasil precisam contar com fluxos de dados, tanto para seu desenvolvimento quanto para sua implantação. Portanto, é imperativo evitar mandatos de localização de dados injustificados e permitir que os dados se movam livremente através das fronteiras de maneira interoperável e segura.

A BSA recomenda que a Estratégia mencione especificamente a importância das transferências transfronteiriças de dados e que sejam feitos todos os esforços para evitar e/ou eliminar as exigências injustificadas de localização de dados das leis e regulamentos brasileiros.

D. Temas de Discussão 3 e 5 – Qualificação para um Futuro Digital e Treinamento de Mão de Obra

Segundo relatório divulgado recentemente pelo Fórum Econômico Mundial, 65% das crianças de hoje terão empregos que ainda não foram inventados[9]. É muito importante que o Governo do Brasil trabalhe com o setor privado para desenvolver uma estratégia nacional para garantir que os trabalhadores brasileiros tenham as habilidades necessárias para prosperar na nova economia de dados.

A **Estratégia** identifica, certeiramente, a necessidade de promover o treinamento dos trabalhadores na área de Inteligência Artificial. A futura mão de obra deve ter acesso a treinamento sobre as habilidades necessárias não apenas para desenvolver soluções de inteligência artificial, mas, o mais

---

análise especializada de todos os resultados. O projeto de outro pesquisador pode precisar apenas de acesso a uma ferramenta de consulta de dados que executa uma análise, verifica o risco de divulgação sem nunca exibir registros individuais e fornece estatísticas de grupo (consulte a caixa "Ferramentas de consulta de dados"). . . .Uma estratégia de minimização de dados bem projetada e implementada adequadamente, como acesso em camadas, pode reduzir o risco de uso não autorizado e danos não intencionais a indivíduos.").

[7] *Consultar* Kobbi Nissim, Thomas Steinke, Alexandra Wood, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, David O'Brien, e Salil Vadhan, *Differential Privacy: A Primer for a Non-technical Audience* [Privacidade Diferencial: Uma Cartilha para um Público Não Técnico] (Fevereiro de 2018), disponível em https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_new.pdf ("Privacidade diferencial é uma definição matemática forte de privacidade no contexto da análise estatística e de aprendizado de máquina. É usado para permitir a coleta, análise e compartilhamento de uma ampla gama de estimativas estatísticas, como médias, tabelas de contingência e dados sintéticos, com base em dados pessoais, protegendo a privacidade das pessoas nos dados. . . . Os cientistas da computação desenvolveram uma teoria robusta para a privacidade diferencial nos últimos quinze anos, e as principais implementações comerciais e governamentais começaram a surgir.").

[8] A criptografia homomórfica é uma forma de criptografia que permite uma análise computacional dos dados criptografados, garantindo que os dados permaneçam confidenciais. O uso da criptografia homomórfica poderia, por exemplo, permitir o compartilhamento de dados médicos agregados para facilitar a pesquisa de IA sem arriscar a confidencialidade do paciente. Consultar Jean Louis Raisaro, Jeffrey Klann, Kavishwar Wagholikar, Hossein Estiri, Jean-Pierre Hubaux, e Shawn Murphy, *Feasibility of Homomorphic Encryption for Sharing I2B2 Aggregate-Level Data in the Cloud* [Viabilidade da Criptografia Homomórfica para Compartilhamento de Dados de Nível Agregado I2B2 em Nuvem], AMIA Jt Summits Translational Science (Maio de 2018), disponível em https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5961814/#

[9] Fórum Econômico Mundial, "This is what coachmen from the 1920s can tell us about robots and jobs" [É isso que os cocheiros da década de 1920 podem nos dizer sobre robôs e empregos], julho de 2016, disponível em https://www.weforum.org/agenda/2016/07/this-is-what-coachmen-from-the-1920s-can-tell-us-about-robots-and-jobs/?utm_content=bufferb59f7&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

importante, para alavancar essas ferramentas de várias maneiras. As tecnologias de IA por softwares estão criando novos tipos de empregos em todos os setores, criando novas carreiras e gerando oportunidades econômicas. A Estratégia deve incentivar parcerias público-privadas para capacitar, recapacitar e aprimorar a força de trabalho, começando com programas-piloto que poderão ser ampliados.

A **Estratégia** deve incentivar iniciativas para aumentar o interesse e o acesso à educação em ciências da computação para os alunos do ensino básico, com foco na expansão de parcerias público-privadas, na revisão da educação profissional e na capacitação de mais professores qualificados em Ciência, Tecnologia, Engenharia e Matemática. Também devem ser feitos esforços para melhorar as competências essenciais ensinadas às crianças do ensino fundamental e médio - as quais devem incluir a resolução de problemas, o pensamento analítico e criativo, as habilidades interpessoais, além das habilidades de alfabetização digital.

Também é importante focar em programas de reciclagem durante a carreira para fornecer aos trabalhadores treinamento em habilidades tecnológicas de alta demanda. As estratégias também devem incluir treinamento técnico fornecido fora dos programas universitários tradicionais.

A BSA sugere que o Governo do Brasil trabalhe com o setor privado para desenvolver uma estratégia robusta para impulsionar esforços para promover o treinamento e a educação atuais da força de trabalho em todos os níveis nas áreas STEM, incluindo ciência da computação e engenharia de software. Também é importante se concentrar nas habilidades básicas de alfabetização em computação.

E. Tema de Discussão 4 – Considerações Internacionais

A capacidade de transferir dados livremente através das fronteiras é a força vital da IA. As regras que limitam as transferências de dados entre fronteiras invariavelmente limitam os *insights* e outros benefícios que os sistemas de IA podem oferecer. Barreiras aos fluxos de dados transfronteiriços, incluindo exigências para armazenamento de dados em instalações locais, comprometem a enorme eficiência de escala e os benefícios econômicos resultantes da inovação de dados e devem ser evitadas.

Uma vez que o governo do Brasil considera uma **Estratégia** para promover o uso e a implantação da IA, é importante que não seja dado apenas um foco especial às políticas nacionais que apoiam o fluxo transfronteiriço de dados, mas a questão também deve fazer parte das discussões internacionais. O Brasil deve se esforçar para desempenhar um papel de liderança apoiando internacionalmente acordos que promovam fluxos de dados.

A BSA recomenda que, ao negociar acordos comerciais bilaterais ou multilaterais, o Brasil apoie o estabelecimento de regras que estimulem a atividade econômica orientada por dados, incluindo regras sólidas que promovam fluxos transfronteiriços de dados.

Conclusão

A BSA agradece o processo consultivo do MCTIC e espera que os comentários sejam úteis para ajudar os esforços no desenvolvimento da "**Estratégia**". Por favor, não hesitem em nos contatar caso haja quaisquer perguntas ou comentários sobre nossas sugestões. Permanecemos abertos a discussões adicionais e esperamos mais oportunidades para trabalhar com o MCTIC, quando finalizada e implementada **a Estratégia**.