

SÍNTESE DA CONTRIBUIÇÃO PARA CONSULTA PÚBLICA - ESTRATÉGIA BRASILEIRA DE INTELIGÊNCIA ARTIFICIAL

O **Instituto Brasileiro de Defesa do Consumidor (IDEC)**, associação de consumidores, sem fins lucrativos, participou da Consulta Pública para a *Estratégia Brasileira de Inteligência Artificial*, realizada entre dezembro de 2019 e março de 2020. A iniciativa da Secretaria de Telecomunicações do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) foi dividida entre nove eixos temáticos: (i) prioridades e objetivos; (ii) qualificações para um futuro digital; (iii) força de trabalho; (iv) pesquisa, desenvolvimento, inovação e empreendedorismo; (v) aplicação pelo governo; (vi) aplicação nos setores produtivos; (vii) segurança pública; (viii) legislação, regulação e uso ético; (ix) aspectos internacionais; (x) governança de IA.

Dentre os temas, o **Programa de Telecomunicações e Direitos Digitais do Instituto Brasileiro de Defesa do Consumidor (IDEC)** se aprofundou em contribuições a alguns dos eixos de maior impacto no direito do consumidor. Abaixo, apresentamos a síntese com os pontos centrais da contribuição enviada, especialmente a partir da análise de seus princípios éticos, *standards* que devem guiar as tecnologias de inteligência artificial de modo a promover o desenvolvimento inclusivo e sustentável e o bem-estar da população.

LEGISLAÇÃO, REGULAÇÃO E USO ÉTICO

É essencial que se crie um marco legal específico da inteligência artificial, de modo a estabelecer as maneiras e processos necessários para implementá-los, previsões de reparação a eventuais violações e especialmente princípios éticos a serem incorporados desde o seu design, analisados a seguir.

IA centrada no ser humano, equidade (fairness) e não-discriminação

- A IA deve ter como base os direitos humanos, incluindo o **respeito ao Estado de Direito, valores democráticos e diversidade**;
- Por meio de um **trabalho interdisciplinar** com autoridades de proteção de dados e entidades de proteção a direitos humanos e direitos dos consumidores;

- Devem ser estabelecidos **mecanismos de cooperação** com a academia, o setor privado e a sociedade civil, permitindo a participação política e popular na regulação de IA.
- Como estas tecnologias trazem grande possibilidade de impacto social e econômico, esses sistemas devem ser desenvolvidos por **equipes capacitadas plurais e multidisciplinares** dotadas de recursos adequados e com independência funcional, capazes de avaliar o respeito do sistema de IA aos direitos humanos.
- Como forma de endereçar as questões de não discriminação, os indivíduos devem também ser compreendidos por seu **pertencimento coletivo**, considerando a possibilidade de impacto ainda maior para grupos já vulneráveis e marginalizados.
- Devem ser **respeitadas as peculiaridades de cada contexto**, com especial atenção às peculiaridades do Sul Global e aos grupos em condição especial de vulnerabilidade em decorrência desses sistemas.
- Para casos de **alto e provável risco de discriminação**, recomenda-se o **banimento** total do uso de IA naquele setor.

Transparência, explicabilidade, previsibilidade, confiabilidade, robustez, auditabilidade e dever de prestação de contas

- O compartilhamento de informações relevantes deve ser feito de forma **compreensível e clara**. Deve-se buscar, especialmente por maneiras criativas (como recursos visuais e técnicos para facilitar sua compreensão), uma maior acessibilidade nas informações que diminuam a desigualdade de poder e a assimetria informacional entre os desenvolvedores e os usuários-consumidores. Isso é ainda mais positivo para usos pelo poder público e para que os grupos e indivíduos afetados pela discriminação dos sistemas autônomos sejam capazes de refutar e recorrer de seu funcionamento.
- É recomendável a **utilização de base de dados abertas** de modo a se permitir maior auditabilidade dos sistemas de IA, mas desde que respeitem a proteção de dados e a representatividade e a diversidade em seu desenvolvimento. Bases de dados abertas devem ser utilizadas especialmente pelo Poder Público, sempre em respeito à finalidade pública e à legislação pertinente, como a LGPD, a Lei de Acesso à Informação e o Código de Defesa do Usuário do Serviço Público.
- Para facilitar uma efetiva prestação de contas e se buscar uma mitigação da opacidade das tecnologias de IA, é também recomendável a elaboração de um **Relatório de Prévio de Avaliação de Impacto**, de modo semelhante ao Relatório de Impacto em Proteção de Dados (“RIPD”, disposto na LGPD), contendo informações sobre quais

dados são utilizados, a metodologia e mecanismos de mitigação de risco. Eventualmente, para casos que envolvam altos riscos para a proteção de dados, pode-se determinar que seja obrigatória a sua produção, ou até necessária a aprovação do relatório de avaliação de impacto pela ANPD.

- Esta transparência é também necessária para facilitar **mecanismos de supervisão** desses sistemas durante todo o seu ciclo de vida. Isso torna o sistema mais rastreável, auditável e, conseqüentemente, responsável. Concretamente, é recomendável a criação de estruturas institucionais para fiscalização da aplicação de padrões éticos mínimos, a publicação de relatórios periódicos e a submissão periódica de revisão das regras e riscos dessas tecnologias, considerando seu alto potencial inovador e disruptivo.

Finalidade, integridade, segurança da informação e proteção de dados

- Deve-se evitar o uso de critérios genéricos e abstratos para a superação da necessidade de consentimento no tratamento de dados, sem expor os usuários-consumidores a riscos desproporcionais de controle de sua autonomia e identidade;
- Além da busca pela anonimização dos dados, deve ser incentivado que desenvolvedores de tecnologias deem **controle dos dados aos usuários**;
- Em contextos de risco de impacto ao exercício de direitos dos cidadãos (enquanto indivíduos ou grupos), deve ser **preservada a determinação humana** em decisões tomadas por IA;
- Tendo em vista a excessiva utilização de dados por meio de tecnologias de IA, deve-se atuar em **cooperação com a Autoridade Nacional de Proteção de Dados (ANPD)**, além do Sistema Nacional de Defesa do Consumidor (em caso de relações de consumo, nos termos do CDC, Art. 2º, caput e parágrafo único).

Responsabilidade

- Em relações de consumo, deve ser **aplicado o Código de Defesa do Consumidor**, inclusive no tocante à **inversão do ônus da prova** (art. 6º, inc. VIII, CDC) e à **responsabilidade objetiva e solidária** (arts. 12 e 14) da cadeia de fornecimento pela reparação de danos por defeitos (no caso, falta de segurança) no produto ou serviço;
- **Mesmo em relações que não são de consumo, pode-se aplicar responsabilidade objetiva** por danos causados com o uso da IA, tendo em vista a assimetria

informacional e a atividade de risco, nos termos do art. 927 do Código Civil, bem como a inversão do ônus da prova (art. 373, §1º, Código de Processo Civil)

OUTROS TEMAS RELEVANTES

Qualificação para um futuro digital

- IA como **ferramenta pedagógica em sala de aula** deve ser utilizada somente de modo a potencializar as capacidades humanas e promoção da educação, nunca como mecanismo de vigilância, em respeito às salvaguardas e à situação de vulnerabilidade das crianças e adolescentes, além de depender do consentimento dos pais.

Aplicação nos setores produtivos

- O **Governo tem um papel essencial** no estabelecimento de métricas de avaliação e monitoramento contínuo dessas tecnologias. Isto deve ser efetivado por meio de garantia de um debate público e democrático sobre o uso dessas tecnologias e tendo foco no investimento em explicabilidade e interpretabilidade desses sistemas, além do endereçamento de questões relativas aos vieses algorítmicos.
- Deve-se atentar às **problemáticas concorrenciais** no uso de IA em setores produtivos relativas (i) ao alargamento de condutas anticompetitivas por meio de algoritmos (por colusão tácita por exemplo); (ii) à insuficiência dos conceitos tradicionais do antitruste para análise de mercados que envolvam tecnologias de IA e dados em geral; (iii) ao potencial de transações abusivas e fraudulentas com consumidores.

Poder Público

- O uso de IA **pode ser utilizado para o aumento de eficiência da máquina governamental**, desde que respeitados os princípios da Administração Pública (Art. 37, CF) e que se garanta a aplicação de princípios gerais à IA.
- Devem ser realizadas avaliações prévias de eficiências concretas e rastreamento das decisões. Para tanto, o Poder Público deve ter atenção especial na **convergência entre necessidade e finalidades do uso de tecnologias de IA**, que devem sempre atender ao interesse público, ponderando entre as eficiências e os impactos a serem incorridos (por meio de avaliações prévias), especialmente no tocante à afetação de direitos fundamentais.

- Suas decisões devem ser rastreáveis, preferencialmente por meio de **softwares com formatos abertos e livres** (tanto em cumprimento à diretriz do art. 24 do Marco Civil da Internet como para facilitar a auditabilidade).
- O compartilhamento de dados entre o poder público ou para outros setores deve ser justificado por uma base legal, tendo uma finalidade adequada, específica e legítima, bem como repassar o mínimo de dados necessários e sendo transparente, nos termos da LGPD.

Segurança Pública

- A preocupação com a utilização de tecnologias de inteligência artificial deve ser ainda maior no âmbito da segurança pública (bem como na educação) devido ao grande risco de **violação de direitos fundamentais**, com restrições ao direito de ir e vir, à presunção de inocência e às liberdades individuais e coletivas de maneira geral, em contradição com o Estado Democrático de Direito. O reconhecimento facial, por exemplo, pode acarretar a detenção equivocada de indivíduos, tendo em vista seus índices de erros, que afetam especialmente a população negra.
- Desta maneira, deve-se ter uma avaliação prévia especial para determinar o uso da tecnologia, e caso implementada, garantir uma transparência ainda maior para possibilitar acesso à informação de seu uso e de sua finalidade. Deve ser possibilitada também a **revisão por um humano** das decisões tomadas que impactam direitos humanos.
- Embora a LGPD tenha sua aplicação, em parte, afastada no campo de segurança pública, é recomendável a aplicação de algumas **salvaguardas, ou até mesmo de moratória ou banimento** - assim como ocorreu em outros países -, de modo a estudar a melhor forma de implementação de regulação no setor.

Sem mais, agradecemos a oportunidade de participação nesta importante consulta pública,

DIOGO MOYSES

Coordenador do programa de Telecomunicações e Direitos Digitais

BÁRBARA SIMÃO

Advogada e pesquisadora do programa de Telecomunicações e Direitos Digitais

JULIANA OMS

Advogada e pesquisadora do programa de Telecomunicações e Direitos Digitais

CAMILA LEITE

Pesquisadora do programa de Telecomunicações e Direitos Digitais