

BOAS PRÁTICAS PARA O USO DE DADOS PESSOAIS EM SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

A inteligência artificial lida com dados pessoais em várias situações, seja no treinamento de sistemas ou no uso para apoiar tarefas do dia a dia. Organização que tem um programa de governança de proteção de dados, tem uma **vantagem significativa** para a contratação, uso e desenvolvimento de novos sistemas de IA.

Neste material, reunimos recomendações e boas práticas* para ajudar na gestão da relação entre privacidade, proteção de dados e inteligência artificial, considerando diferentes contextos de uso. Esse processo exige diálogo constante entre as áreas da organização, incluindo quem toma decisões estratégicas.



VAMOS ÀS BOAS PRÁTICAS:



LIDERANÇA E RESPONSABILIDADES

- **Ampliar o papel das equipes de privacidade para incluir responsabilidades relacionadas ao tratamento de dados pessoais no contexto da IA.**

Independentemente da estrutura de governança adotada, é recomendado envolver essas equipes nas discussões de IA, inclusive aproveitando práticas já existentes, como o Privacy by Design.

- **Promover a colaboração em times de múltiplas especialidades.**

A proteção de dados é só uma parte da governança de IA. A organização deve ter clareza sobre sua estrutura e recursos — técnicos e humanos — para garantir que os profissionais certos estejam envolvidos na gestão dos dados, especialmente os pessoais usados em sistemas de IA.



POLÍTICAS E PROCEDIMENTOS

- **Atualizar ou criar políticas de privacidade e segurança da informação**

Elas devem garantir que a proteção de dados esteja presente desde o início dos projetos de IA e ao longo de todo o seu ciclo de vida. Elas precisam cobrir coleta, uso, compartilhamento e armazenamento de dados, sempre em conformidade com a legislação e a minimização de riscos à privacidade.

- **Definir diretrizes claras para o uso de dados pessoais.**

Ao treinar ou usar modelos de IA, é importante indicar quando e como dados sensíveis serão utilizados. Isso inclui especificar o uso de dados protegidos no treinamento, como dados criptografados, pseudonimizados, tokenizados ou sintéticos. Essas técnicas ajudam a proteger a privacidade das pessoas e a reduzir os riscos no uso de dados sensíveis.

- **Realizar due diligence e avaliações de impacto.**

É recomendado a criação de checklists e ferramentas de due diligence para avaliar parceiros que oferecem soluções de IA. Também é importante criar relatórios de impacto à privacidade e avaliações de impacto algorítmico para analisar e reduzir os riscos de privacidade e discriminação em projetos de IA.



ANÁLISE DE RISCO E CONFORMIDADE

- **Aproveitar mecanismos já existentes de avaliação de riscos.**

É recomendado usar metodologias que já são aplicadas na análise de riscos do tratamento de dados pessoais e adaptá-las para os projetos de inteligência artificial. Isso ajuda a tornar o processo mais eficiente e a garantir que os riscos relacionados ao uso da IA sejam avaliados de forma consistente.

- **Registrar os principais aspectos de proteção de dados nos sistemas de IA.**

Quando os sistemas de IA lidam com dados pessoais, é fundamental aplicar os cuidados básicos de governança de dados. Isso inclui: definir a base legal para o tratamento, registrar as atividades realizadas com os dados, avaliar os riscos envolvidos, garantir transparência sobre o uso dos dados e permitir que os titulares exerçam seus direitos. Esses pontos ajudam a manter a conformidade com as leis de proteção de dados e a reduzir riscos jurídicos e reputacionais.

- **Fazer avaliações contínuas de riscos e de viés algorítmico.**

É essencial monitorar os modelos de IA ao longo do tempo para evitar viés e discriminação injusta. É recomendado desenvolver ferramentas para avaliar o impacto algorítmico e aplicá-las em diferentes fases do ciclo de vida do sistema. Isso é especialmente importante sempre que houver novas aplicações ou mudanças no uso dos modelos. A avaliação contínua permite ajustes proativos e maior segurança na operação das soluções de IA.



TRANSPARÊNCIA

- **Priorizar rastreabilidade e explicações claras sobre decisões tomadas por IA.**

Sempre que um sistema de IA tratar dados pessoais, deve-se manter uma trilha de documentação que permita entender como as decisões foram tomadas. É importante que esse processo seja transparente e compreensível, explicando o papel da IA de forma acessível para o público envolvido.

- **Apresentar informações sobre o sistema de forma simples e visual.**

Recomenda-se disponibilizar materiais curtos e objetivos — como cartões explicativos — que mostrem onde e como o sistema de IA deve ser usado, além de descrever seu comportamento em diferentes situações. Isso facilita o entendimento dos usuários e reforça a confiança no uso da tecnologia.



DIREITOS DOS TITULARES

- **Criar formas de revisar decisões automatizadas ou assistidas por IA.**

A organização deve garantir que qualquer pessoa impactada por uma decisão automatizada tenha o direito de contestá-la, especialmente quando envolver seus dados pessoais. Essas decisões devem poder ser revistas por um profissional qualificado que analise o caso com atenção, ouça os argumentos do titular e, se necessário, corrija eventuais erros ou injustiças.

Cumprir as leis de proteção de dados e adotar boas práticas no uso de dados pessoais em sistemas de IA não é só uma obrigação legal, mas também uma chance de ganhar vantagem competitiva. Ao mostrar compromisso com a privacidade e proteção de dados, as organizações podem fortalecer a confiança dos clientes, atrair e reter talentos, e construir uma reputação de inovação responsável e ética.

*White Paper on Accountable AI Best Practices – CIPL: referencial adotado na construção deste material, com interpretação contextual de Opice Blum