Autor do Artigo: Jean Santana

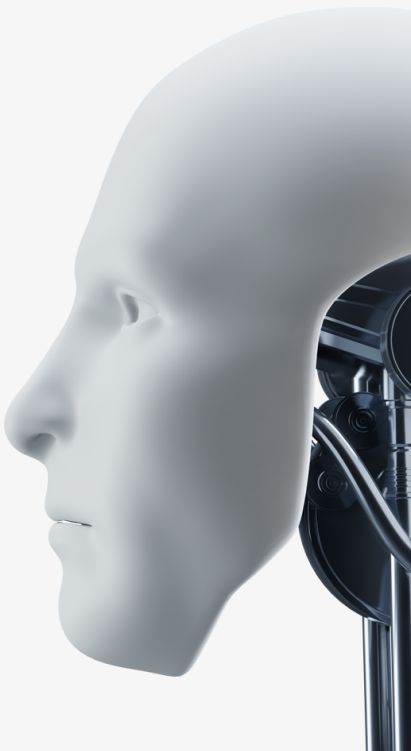
Inteligência Artificial e Proteção de Dados

Análise introdutória ao tema

A IA é uma ferramenta poderosa que pode nos tornar muito mais produtivos. Ao mesmo tempo, ela traz desafios legais importantes, como a **necessidade de se atender a requisitos de Privacidade e Proteção de Dados, inclusive durante a sua etapa de desenvolvimento.**

Muitos desses sistemas dependem de grandes conjuntos de dados para funcionar, os quais, não raramente, são categorizados como dados pessoais. Essa prática, naturalmente, atrai a **aplicação de normas que regem o tratamento desses dados, como a Lei Geral de Proteção de Dados e o Marco Civil da Internet.**

O objetivo deste artigo é apresentar alguns **cuidados gerais sobre como desenvolver ou aplicar sistemas de IA de forma segura** e em atenção aos requisitos da LGPD, com base em boas-práticas e literatura especializada, inclusive expedidas por Autoridades de Proteção de Dados estrangeiras, como o ICO e a CNIL.



AUTOR DO ARTIGO: JEAN SANTANA

Finalidade, Adequação & Necessidade

Qual a finalidade da IA? Os dados e atributos selecionados podem te ajudar a atingir essa finalidade? É razoável e proporcional a utilização dos atributos selecionados para se atender a essa finalidade?

Responder essas perguntas durante a etapa de desenvolvimento ou aplicação da IA é essencial para garantir a licitude do tratamento. **Confira algumas dicas!**

Determine com precisão a finalidade: **qual é o problema que o sistema busca resolver?**

Documente as razões pelas quais vocês selecionou os atributos/dados a serem utilizados, destacando como eles auxiliam a atingir a sua finalidade.

Realize testes eliminando e incluindo alguns dos atributos. Avalie se eles, de fato, apresentam diferença significativa a acuracidade do modelo. Em caso negativo, elimine-os.

AUTOR DO ARTIGO: JEAN SANTANA

Base legal

O primeiro desafio é determinar qual base legal da LGPD pode fundamentar o desenvolvimento, treinamento e a validação de sistemas de IA que envolvam dados pessoais.

A seguir, apresentamos possibilidades a serem consideradas, sendo certo que se faz necessário consultar cada situação em concreto para confirmar com precisão a escolha mais adequada.

LEGÍTIMO INTERESSE

(art. 7º, IX)

*Desde que **satisfeito o teste de balanceamento**, o legítimo interesse é a base legal em potencial para o desenvolvimento de sistemas de IA, dada a sua flexibilidade natural e o fato de que, via de regra, o desenvolvimento de sistemas será entendido como interesse legítimo do desenvolvedor (minimamente, interesse comercial),fundado em uma situação concreta (problema que o sistema objetiva resolver), usualmente, ainda, representando benefícios potenciais para outros indivíduos ou mesmo para a sociedade como um todo. O papel do legítimo interesse é ainda mais destacado ao avaliamos as dificuldades (ou até inviabilidade) de enquadramento da operação de tratamento em outras hipóteses legais.*

AUTOR DO ARTIGO: JEAN SANTANA

Isso não significa afirmar que o legítimo interesse é a única base legal possível. Apenas que, para a maioria dos casos, ela será a hipótese mais adequada ao se avaliar não apenas a possibilidade de enquadramento, mas também seus benefícios e malefícios potenciais.

Com efeito, existirão casos em que o legítimo interesse sequer poderá ser aplicável (ex. tratamento de dados pessoais sensíveis). Ou seja, nessas ou outras hipóteses, importante sempre avaliar o enquadramento adequado, como:

REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA

(art. 7º, IV, e art. 11º, II, d)

Se sua organização atende aos critérios para ser classificada como um "órgão de pesquisa", avalie usar essa base legal no desenvolvimento e treinamento de modelos experimentais.

CONSENTIMENTO

(art. 7º, I e Art. 11, I)

Embora o consentimento seja uma opção disponível na LGPD, é limitado, na prática, devendo ser consideradas suas grandes limitações e desvantagens. Isso inclui a exigência de ter uma relação prévia com o titular, a complexidade de cumprir com os requisitos de transparência e a possibilidade de revogação a qualquer momento, o que pode gerar prejuízos ao sistema, sobretudo se feita em volume significativo.

AUTOR DO ARTIGO: JEAN SANTANA

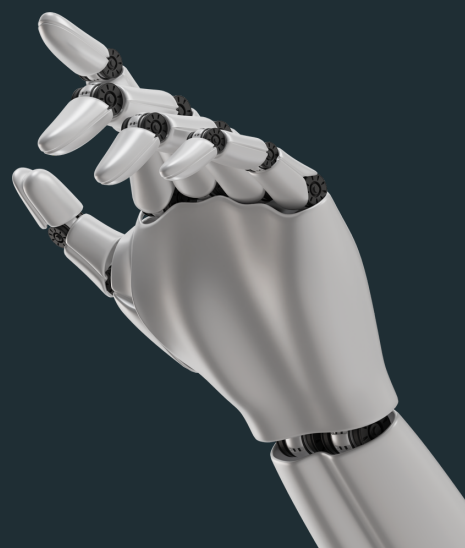
E SE NENHUMA FOR ADEQUADA?

Caso nenhuma das bases legais seja aplicável, avalie a possibilidade de trabalhar com dados anonimizados. Lembre-se de realizar avaliação técnica e jurídica a respeito da possibilidade de reidentificação dos dados anonimizados.

Qualidade & Não Discriminação

Ao tratarmos de Proteção de Dados e IA, um dos pontos de preocupação é garantir **a precisão e a ausência de vieses discriminatórios do sistema.**

Embora soluções únicas não existam, alguns cuidados podem ser adotados para mitigar esses riscos. **Vamos conferir alguns deles?**



AUTOR DO ARTIGO: JEAN SANTANA

- Garanta que as bases de treino e a validação sejam adequadamente representativas da população afetada pelo sistema.

- Esteja atento às boas práticas de governança de dados para garantir que as bases de treino e validação são precisas, atualizadas, razoáveis, válidas e sem contradições.

- Realize testes exaustivos nos sistemas, buscando identificar potenciais vieses discriminatórios e ausência de precisão, adotando controles corretivos.

AUTOR DO ARTIGO: JEAN SANTANA

Garantindo a Transparência

Um dos pontos cruciais da maioria das legislações de privacidade, e a LGPD não é exceção, é garantir a transparência do tratamento de dados para com o titular.
Veja alguns pontos de atenção:

- Caso sua organização utilize dados de titulares com quem tenha relacionamento prévio, **insira essa informação em seu aviso de privacidade ou documento correlato.**

- Caso você colete dados de fontes terceiras, **avalie a possibilidade de comunicar o titular sobre seu uso.** Algumas autoridades de dados podem requerer que você informe o titular sobre isso (ex. o ICO requer que seja feita em até um mês).

- Caso o sistema tome decisões sobre os titulares, busque **garantir a explicabilidade por padrão.** É recomendável que, no mínimo, você consiga identificar quais dados foram considerados pelo sistema na decisão e sua origem (Tema 710, STJ).

AUTOR DO ARTIGO: JEAN SANTANA

Segurança & Prevenção

A LGPD exige que os responsáveis pelo tratamento **adotem medidas técnicas e administrativas proporcionais aos riscos,** sob pena de o tratamento de dados ser considerado irregular.

Quais precauções devemos tomar ao lidar com o treinamento de sistemas de IA? Sem esgotar o assunto, pois as práticas podem variar de projeto para projeto, seguem algumas sugestões:

NÃO SE DESCUIDE DO PADRÃO

Os cuidados comumente adotados (controles de acesso, criptografia de dados em repouso e em trânsito, guarda e monitoramento de logs...) devem ser observados, na medida do possível, nos processos envolvendo IA, buscando-se sempre garantir a segurança *by design*.

CUIDADO COM ATAQUES VOLTADOS A IA

No entanto, é necessário se atentar para ataques especificamente voltados para a IA, como ataques adversarias, adotando-se controles para mitigar os riscos de ocorrência desses ataques (ex. treinando o modelo para ser robusto a ataques adversariais).

AUTOR DO ARTIGO: JEAN SANTANA

AVALIE ELABORAR RIPD

Em seu “FAQ” sobre o RIPD, a ANPD traça os critérios para que o tratamento seja considerado de alto risco. É comum que operações em sistemas de IA envolvam o tratamento automatizado de dados pessoais em larga escala. Nesses casos avalie a elaboração do RIPD.

AVALIE ELABORAR AIA

A AIA é um mecanismo de gerenciamento de riscos voltado a sistemas de IA, sendo previsto no PL nº 2338/2023. Embora não seja legalmente mandatório e nem se limite a aspectos de Privacidade, sua elaboração pode ser considerada salvaguarda importante, especialmente se a IA se enquadrar na categoria de “alto risco” prevista no Projeto de Lei.

Material de autoria do nosso advogado Jean Santana
jean.santana@vlklaw.com.br

VLK ADV