

Escola de Governo do Distrito Federal - EGOV




- Fundamentos de IA.
- Ética e LGPD no Uso de IA.

Textos e Exercícios Práticos



- Fundamentos de IA

Jogo de Associação: "É Deep Learning (DL). Mas é IA Generativa (IAG)?"

 **Objetivo do jogo:** Aprender a identificar e diferenciar uma IA Generativa de uma IA Analítica.

- IA Generativa (DL + geração criativa)
- IA Analítica (DL sem geração)

Desafio cerebral desbloqueado!

Chegou a hora de colocar esses neurônios pra dançar!   Abaixo tem uma lista de tecnologias que usam Deep Learning.

👉 Sua missão: **Marque com um “X”** aquelas que usam Deep Learning, mas **NÃO** são IAs Generativas.

🤖 Proibido colar, hein!

Nada de ChatGPT, Google ou ajuda do Ouvidor nerd que está do seu lado.

👁️ Tô de olho... e a IA também! 🤖⚡

Bora ver se você é raiz do conhecimento ou Nutella da IA? 😄😄

1. Reconhecimento facial
2. Tradutor neural automático
3. Diagnóstico por imagem médica
4. Classificador de sentimentos em redes sociais
5. Sistema de recomendação da Netflix
6. Leitor de placas de veículos (OCR + CNN)
7. Detecção de objetos em imagens urbanas
8. Detector de fraudes bancárias em tempo real

- **Ética e LGPD no Uso de IA**

Os **riscos da IA** são múltiplos e podem impactar desde a segurança individual até a estrutura social e econômica global.

- **Viés e Discriminação:** Os sistemas de IA são treinados com dados, e se esses dados refletem preconceitos existentes na sociedade (sejam eles raciais, de gênero, socioeconômicos, etc.), a IA pode perpetuar e até amplificar esses vieses. Isso pode levar a decisões discriminatórias em áreas críticas como contratação de empregos, concessão de crédito, diagnósticos médicos e até mesmo no sistema de justiça criminal.
- **Perda de Empregos:** A automação impulsionada pela IA pode substituir tarefas rotineiras e repetitivas em diversos setores, levando ao desemprego estrutural. Embora novas funções possam surgir, a transição pode ser desafiadora para muitos trabalhadores.
- **Preocupações com a Privacidade:** Sistemas de IA coletam e processam grandes volumes de dados pessoais. Há o risco de uso indevido desses dados, vigilância não consentida e vazamentos que podem comprometer a privacidade e a segurança dos indivíduos.
- **Desinformação e Manipulação:** A IA generativa, em particular, pode criar conteúdo falso, mas altamente realista, como *deepfakes* (vídeos e áudios manipulados), o que facilita a disseminação de desinformação, propaganda e manipulação da opinião pública, com sérias implicações para a democracia e a confiança social.
- **Riscos de Segurança Cibernética:** A IA pode ser usada por atores mal-intencionados para desenvolver ataques cibernéticos mais sofisticados, contornar defesas e explorar vulnerabilidades, aumentando a escala e o impacto de crimes digitais.
- **Concentração de Poder:** O desenvolvimento e controle da IA podem se concentrar nas mãos de poucas corporações ou governos, levando a um desequilíbrio de poder e a uma potencial falta de supervisão e regulação democrática.

- **Imprevisibilidade e Falta de Controle:** À medida que os sistemas de IA se tornam mais complexos e autônomos, entender como eles tomam decisões (o problema da "caixa preta") se torna um desafio. Comportamentos inesperados ou decisões com consequências imprevistas podem ocorrer, dificultando a atribuição de responsabilidade.
-

Limitações da Inteligência Artificial

Apesar dos avanços impressionantes, a IA ainda possui limitações inerentes que a distinguem da inteligência humana.

- **Falta de Senso Comum:** A IA não possui o "senso comum" que os humanos adquirem através da experiência e da interação com o mundo. Ela pode realizar tarefas específicas de forma brilhante, mas falha em aplicar o conhecimento de forma flexível ou em contextos não previstos em seus dados de treinamento.
 - **Ausência de Empatia e Emoção:** A IA pode simular a compreensão de emoções ao analisar padrões de dados (como tom de voz ou expressões faciais), mas não as sente ou experimenta de fato. Ela não possui consciência, intuição ou capacidade de entender o sofrimento humano em um nível empático.
 - **Dependência de Dados:** A qualidade e a diversidade dos dados de treinamento são cruciais para o desempenho da IA. Se os dados são escassos, tendenciosos ou incompletos, o modelo de IA será limitado e propenso a erros. Ela não "cria" conhecimento do nada.
 - **Dificuldade com Raciocínio Abstrato e Criatividade Genuína:** Embora a IA generativa possa criar conteúdo "novo" que imita estilos existentes, a capacidade de raciocínio abstrato profundo, de formular ideias verdadeiramente inovadoras ou de ter uma criatividade original (no sentido humano) ainda é uma limitação. Ela recombina e extrapola a partir do que aprendeu.
 - **Falta de "Explicabilidade" (Problema da "Caixa Preta"):** Para muitas redes neurais profundas, é difícil ou impossível entender exatamente como o sistema chegou a uma determinada decisão ou resultado. Essa falta de transparência é um desafio, especialmente em aplicações críticas como medicina ou justiça.
 - **Custo Computacional:** O treinamento de modelos de IA grandes e complexos exige um poder computacional gigantesco, o que se traduz em alto custo energético e financeiro, e em uma pegada de carbono significativa.
-

Dilemas Éticos da IA

Os dilemas éticos surgem da necessidade de equilibrar os benefícios potenciais da IA com os valores humanos e a justiça social.

- **Responsabilidade e Autoria:** Quem é o responsável quando um sistema de IA comete um erro ou causa um dano? É o desenvolvedor, a empresa que o implementa, ou o próprio sistema (se tiver um alto grau de autonomia)? Além disso, quem detém a autoria de conteúdos gerados por IA? Essas são questões legais e morais complexas.

- **Transparência e Explicabilidade:** Como garantir que as decisões tomadas por sistemas de IA sejam compreensíveis e justificáveis para os humanos, especialmente em cenários de alto risco? A falta de transparência pode minar a confiança e dificultar a auditoria e a correção de falhas.
 - **Justiça e Equidade:** Como podemos garantir que a IA beneficie a todos igualmente e não exacerba as desigualdades existentes? Isso envolve garantir acesso equitativo à tecnologia e evitar que os algoritmos discriminem grupos marginalizados.
 - **Controle Humano vs. Autonomia da IA:** Qual o nível de autonomia que devemos conceder aos sistemas de IA? Em que ponto a tomada de decisão humana deve prevalecer sobre a decisão da máquina, especialmente em áreas como armas autônomas ou carros autodirigíveis?
 - **Impacto no Trabalho e na Sociedade:** Como a sociedade deve se adaptar às transformações no mercado de trabalho? Devemos implementar políticas de renda básica universal ou investir pesadamente em requalificação profissional para mitigar os impactos negativos?
 - **Privacidade vs. Vigilância:** Até que ponto podemos usar a IA para vigilância (por exemplo, reconhecimento facial em espaços públicos) em nome da segurança, sem comprometer os direitos de privacidade e liberdade individual?
-



Cuidados no uso da IA no serviço público

Privacidade, proteção de dados e aspectos da LGPD

Com o avanço da Inteligência Artificial nas instituições públicas, torna-se essencial garantir que seu uso respeite os direitos fundamentais dos cidadãos, especialmente no que diz respeito à privacidade e proteção de dados pessoais.

A LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) — estabelece os princípios, direitos e deveres sobre o uso de dados pessoais no Brasil. Isso se aplica diretamente ao uso de IA no setor público.

1. Dados pessoais e sensíveis: o que a IA não pode fazer?

Exemplos de risco:




- **X** Gerar respostas a manifestações públicas com nome e CPF do cidadão exposto.
- **X** Usar dados de servidores em treinamentos de IA sem consentimento.
- **X** Armazenar dados de saúde, religião ou orientação política para fins automatizados sem base legal.
- **X** Utilizar ferramentas de IA baseadas na nuvem sem avaliar os termos de uso e a política de privacidade, expondo dados protegidos.

Cuidados:

- Minimização de dados: só colete o estritamente necessário.
 - Anonimização sempre que possível: remova informações identificáveis de documentos processados por IA.
 - Consentimento claro: sempre que usar dados fora do escopo legal, deve haver autorização formal.
-

2. Bases legais para uso de IA no setor público segundo a LGPD

O tratamento de dados pessoais por órgãos públicos pode ocorrer sem consentimento, mas precisa se enquadrar em hipóteses legais, como:

-  Execução de políticas públicas previstas em lei
-  Tratamento para cumprimento de obrigação legal ou regulatória
-  Proteção do interesse público, com avaliação de impacto

Boas práticas:

- Registre e documente a finalidade do uso da IA.
 - Evite treinamentos ou decisões automatizadas com base em dados pessoais sem validação jurídica.
 - Consulte a ANPD (Autoridade Nacional de Proteção de Dados) para dúvidas específicas.
-

3. IA e decisões automatizadas: limites e transparência

A LGPD garante ao cidadão o direito de revisão de decisões automatizadas que afetem seus interesses. Exemplo:

Se um sistema de IA rejeita automaticamente uma solicitação de benefício com base em parâmetros opacos, o cidadão tem o direito de saber o motivo e solicitar revisão humana.

Cuidados:

- Evite decisões exclusivamente automatizadas em políticas públicas.
 - Sempre ofereça um canal de revisão e recurso humano.
 - Garanta a explicabilidade dos critérios da IA (mesmo que por aproximação).
-







4. Privacidade desde a concepção ("Privacy by Design")

A LGPD orienta que a proteção de dados deve ser prevista desde o início do projeto de IA — não apenas como correção posterior.

Boas práticas:

- Mapear os fluxos de dados antes de implementar a IA.
 - Avaliar os riscos por meio de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) - O que é isso? Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
 - Designar um encarregado de dados (DPO) para acompanhar projetos com IA.
-

✓ 5. Checklist de cuidados essenciais para o uso de IA com dados pessoais

Item	Verificação Rápida
 Finalidade clara e legítima?	
 Dados anonimizados ou protegidos adequadamente?	
 Consentimento obtido ou base legal bem definida?	
 Decisões automatizadas possuem possibilidade de revisão humana?	
 Há registro e documentação do uso da IA com dados?	
 Foi feito relatório de impacto (RIPD) quando necessário?	

Conclusão: Uso estratégico da IA começa pela proteção de direitos

A inteligência artificial pode impulsionar a eficiência pública, mas só será legítima se for ética, transparente e legalmente responsável.

No serviço público, usar IA com responsabilidade é proteger a cidadania digital.

2. LGPD no Uso de IA

◆ Fundamentos e Princípios da LGPD

A LGPD (Lei nº 13.709/2018) estabelece regras para o tratamento de dados pessoais, promovendo:

- Respeito à privacidade
- Autodeterminação informativa
- Liberdade de expressão e comunicação
- Inviolabilidade da intimidade, honra e imagem
- Desenvolvimento tecnológico e inovação
- Livre iniciativa e defesa do consumidor
- Direitos humanos e cidadania

No contexto da IA, isso exige que os algoritmos e modelos de linguagem operem com **transparência, finalidade legítima e responsabilidade institucional**.

◆ Direitos dos Titulares de Dados Pessoais

Ao integrar IA nas práticas públicas, é fundamental garantir os **direitos dos titulares**, tais como:

1. Confirmação e acesso aos dados
2. Correção de dados incompletos ou desatualizados
3. Anonimização, bloqueio ou eliminação de dados desnecessários
4. Portabilidade dos dados
5. Informação sobre uso compartilhado
6. Revogação do consentimento
7. Revisão de decisões automatizadas (Art. 20 da LGPD)

Aplicação prática: A IA usada em ouvidorias deve permitir que o cidadão tenha clareza sobre como seus dados são tratados, com opção de revisão humana.

◆ Requisitos Legais para Uso de IA

O tratamento de dados pessoais com apoio de IA só é permitido com **base legal** definida no Art. 7º da LGPD. Exemplos:

- Consentimento livre, informado e destacado
- Cumprimento de obrigação legal ou regulatória
- Execução de políticas públicas (especialmente em ouvidorias)
- Estudos de órgãos de pesquisa (com anonimização sempre que possível)
- Proteção da vida, tutela da saúde, interesse legítimo

⚠ A ausência de base legal clara pode tornar o uso da IA **ilegal ou abusivo**, mesmo com boas intenções.

♦ Minimização e Anonimização de Dados

Dois pilares fundamentais para proteção no uso de IA:

- **Minimização:** Coletar **somente os dados estritamente necessários** à finalidade da atividade com IA. Evita excesso de dados e reduz riscos.
- **Anonimização:** Utilizar técnicas para impedir que o dado possa identificar alguém diretamente (ex: em análises estatísticas ou para treinamento de IA).

💡 *Na ouvidoria, isso significa que os dados usados para treinar ou testar IA devem ser anonimizados sempre que possível.*

♦ Medidas de Segurança e Conformidade

A LGPD impõe que os agentes de tratamento (controlador e operador) adotem:

- **Medidas técnicas e administrativas** para proteção contra vazamentos e acessos não autorizados (Art. 46)
- **Auditorias, protocolos de resposta a incidentes e planos de mitigação**
- **Registro das operações de tratamento**
- **Nomeação de um Encarregado de Dados (DPO)**
- **Relatórios de impacto à proteção de dados (DPIA)**, especialmente ao usar IA de forma sensível

⚙️ *Em projetos de IA na ouvidoria, a conformidade com esses mecanismos demonstra governança, boa-fé institucional e compromisso com a cidadania digital.*



■ Situação Hipotética: “Resposta Ágil, Erro Crítico”

Contexto:

Carlos é ouvidor da Secretaria de Desenvolvimento Social do DF. Em busca de mais agilidade e empatia nas respostas aos cidadãos, ele decide testar uma ferramenta de IA generativa gratuita (baseada na web) para **melhorar a linguagem de uma resposta**.

Ele copia e cola, na íntegra, o texto da manifestação recebida por e-mail, com o seguinte conteúdo:

"Meu filho Gabriel, de 8 anos, tem diagnóstico de transtorno do espectro autista (CID F84.0) e está sem acompanhamento psicológico desde março. Meu endereço é Rua da Esperança, nº 12, Sol Nascente. Já protocolei três vezes e ninguém me atende."

Carlos pede à IA:

"Melhore a redação desse texto de resposta para torná-la mais empática e clara, sem parecer padronizada."

⚠ O Problema

Carlos não percebeu que, ao enviar o texto integral da manifestação para a IA, ele também transmitiu **dados pessoais e sensíveis do cidadão**, incluindo:

- Nome e idade de uma criança;
- Endereço residencial completo;
- Informação de saúde (diagnóstico psicológico);
- Número de protocolos (histórico de atendimento).

O sistema de IA, por ser baseado na web e fora dos servidores institucionais, **armazenou temporariamente o conteúdo** para melhorar seu próprio desempenho, conforme seus termos de uso — que Carlos **não leu**.

Dias depois, ao fazer um novo teste, Carlos percebe que a ferramenta gerou uma resposta com o nome “Gabriel” e referências ao caso anterior, mesmo sem ele tê-lo mencionado novamente.

Riscos cometidos com base na LGPD

Violações identificadas:

- **Art. 6º, III (necessidade):** uso de mais dados do que o necessário para gerar a resposta.
- **Art. 11 (dados sensíveis):** tratamento de dado sensível (saúde) sem base legal.
- **Art. 46 (segurança):** ausência de medida para proteger os dados em ambiente controlado.
- **Art. 48 (vazamento):** envio não autorizado a terceiro sem consentimento ou salvaguardas.
- **Art. 18 (direitos do titular):** cidadão não foi informado nem consentiu com o uso de seus dados por terceiros.

Como sanar e prevenir a situação

Ações corretivas imediatas:

1. **Comunicar à autoridade competente (ANPD)** sobre o incidente, conforme o Art. 48.
 2. **Informar o cidadão afetado** de forma transparente e documentada.
 3. **Documentar o incidente** e as medidas adotadas.
 4. **Remover os dados da plataforma externa**, se possível, ou solicitar sua exclusão.
-

✚ Ações preventivas recomendadas:

- Criar uma **política institucional sobre uso de IA**, com orientações claras.
- **Nunca inserir dados pessoais ou sensíveis em ferramentas não homologadas** pela instituição.
- **Anonimizar as manifestações** antes de usá-las com IA (substituir nomes, endereços, diagnósticos etc.).
- Usar plataformas de IA que estejam **em ambiente seguro (on-premise ou com contrato de privacidade)**.
- Treinar servidores públicos sobre **boas práticas de proteção de dados e uso de IA com ética**.

Quadro Prático: O que fazer nessa situação

Etapa	Ação prática recomendada
1. Identificar o erro	Verifique se dados pessoais e sensíveis foram enviados à IA sem tratamento prévio.
2. Mitigar o impacto	Solicite remoção dos dados da ferramenta, documente a falha e isole o conteúdo vazado.
3. Comunicar o incidente	Notifique a ANPD e o titular da manifestação com base no Art. 48 da LGPD.
4. Corrigir o processo	Estabeleça procedimento de anonimização para uso de IA.
5. Prevenir novas ocorrências	Use IA apenas em ambiente institucional seguro e treine os servidores sobre privacidade.

1. Dados pessoais e sensíveis: o que a IA não pode fazer?

Exemplos de risco em ouvidorias públicas:

- ✘ Gerar respostas a manifestações públicas com **nome e CPF do cidadão exposto**.
- ✘ Usar **dados de servidores** em treinamentos de IA sem consentimento.
- ✘ Armazenar **dados de saúde, religião ou orientação política** para fins automatizados **sem base legal**.
- ✘ Utilizar ferramentas de IA baseadas na nuvem **sem avaliar os termos de uso e a política de privacidade**, expondo dados protegidos.

✓ Resumo didático

Dado sensível armazenado sem base legal	Por que infringe a LGPD?
Saúde, religião, opinião política	Art. 11: exige base legal específica e explícita
Finalidade não informada	Art. 6º, I: fere o princípio da finalidade
Coleta sem necessidade comprovada	Art. 6º, III: fere o princípio da necessidade
Sem consentimento nem política pública	Invalida a base jurídica e gera risco institucional

Quadro-Resumo: Dados Pessoais Sensíveis na LGPD e Exemplos em Ouvidorias

Tipo de Dado Sensível (LGPD, Art. 5º, II)	Exemplo em uma manifestação à ouvidoria	Cuidados necessários segundo a LGPD
Saúde	"Tenho câncer e o hospital do Gama não marcou minha quimioterapia."	Exige base legal específica (Art. 11); nunca usar para treinar IA sem anonimizar.
Religião / convicção religiosa	"Sou umbandista e sofri discriminação em escola pública."	Dado sensível; proíbe qualquer uso automatizado sem consentimento ou previsão legal clara.
Opinião política	"Sou militante e fui impedido de distribuir panfletos dentro de órgão público."	Dado de alta proteção; jamais usar para agrupamentos, análises automatizadas ou IA sem respaldo legal.
Filiação a sindicato / organização política	"Sou representante sindical e a diretoria se recusa a dialogar."	Base legal obrigatória; o tratamento indevido pode configurar discriminação institucional.
Vida sexual	"Fui vítima de violência sexual e não obtive atendimento adequado no hospital."	Altamente sensível; anonimização rigorosa é indispensável.
Dados biométricos	"Fiz cadastro facial no posto, mas não consigo acessar meus dados."	Usado para identificação; exige segurança reforçada (Art. 46).
Dados genéticos	"Meu filho tem uma condição genética rara e precisa de tratamento."	Equipara-se a dados de saúde; requer base legal robusta e anonimização se usado para fins analíticos.
Origem racial ou étnica	"Sou negro e fui tratado com desdém por um servidor público."	Dados protegidos por leis antidiscriminatórias e pela LGPD.

