



OPORTUNIDADES

Jornada Inicial do **GESTOR DE PRIVACIDADE**

**INTELIGÊNCIA
ARTIFICIAL: UMA
OPORTUNIDADE**

Realização



Conteúdo atualizado em
15/02/2023

Aviso Legal

- O conteúdo desta Aula Aberta **não pode ser reproduzido ou redistribuído de qualquer forma ou por qualquer meio** sem autorização da **DataUX®** ou da **Tlexames**.
- A DataUX® registra em Blockchain todos os materiais produzidos para **garantia de autenticidade e de autoria**.
- A DataUX® e a Tlexames **não licenciam** o uso de seu material para outras empresas. Se você encontrar outra empresa utilizando este material ou parte dele em treinamentos, por favor denuncie pelos e-mails contato@tiexames.com.br e/ou contato@dataux.com.br para que as devidas medidas legais sejam tomadas.
- Algumas marcas registradas podem aparecer no decorrer desta aula aberta. O seu uso, bem como de logotipos, é apenas para fins educacionais, em benefício exclusivo do dono da marca registrada, sem intenção de infringir as regras de sua utilização.

Apresentação do Instrutor



<https://www.plataformadataux.com.br>

<https://dponapratica.com.br>

@profmatheuspassos



✓ Prof. Matheus Passos Silva

- *Doutor em Direito pela Universidade de Lisboa*
- *IAPP® CIPP/E, CIPM, CIPT, CDPO/BR, FIP*
- *ECPC-B Professional DPO Certification, Maastricht University*
- *EXIN® Certified Data Protection Officer, Certified Information Security Officer, Certified Blockchain Foundation*
- *ABNT Lead Implementer da Gestão da Privacidade da Informação*
- Sócio fundador da **DataUX** – *Privacy is made by us!*
- **Global Data Protection Officer** na *Bolt* – Estônia
- **Membro do Grupo de Peritos do Comitê Europeu para a Proteção de Dados (“EDPB”)**

Vamos começar!

Jornada Inicial do Gestor de Privacidade

INTELIGÊNCIA ARTIFICIAL: UMA OPORTUNIDADE PARA O GESTOR DE PRIVACIDADE

A explosão da inteligência artificial

Em 2017, 20% dos entrevistados relataram ter adotado IA em pelo menos uma área de negócios, enquanto hoje, esse número é de 50%, embora tenha atingido um pico de 58% em 2019.



Ao mesmo tempo, o número médio de capacidades de IA que as organizações utilizam, tais como geração de linguagem natural e visão computadorizada, também dobrou – de 1,9 em 2018 para 3,8 em 2022.

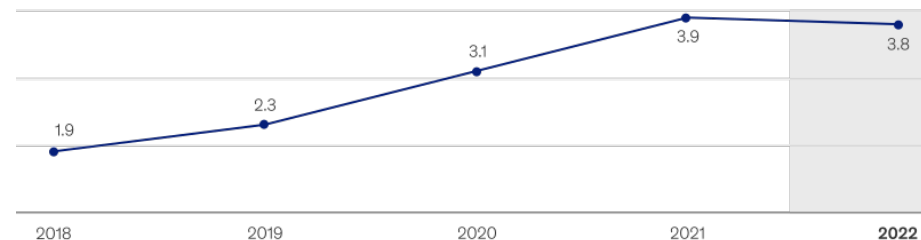


Entre estas capacidades, a automação de processos robóticos e a visão computadorizada continuam sendo as mais utilizadas a cada ano, enquanto a compreensão de textos em linguagem natural avançou do meio em 2018 para a frente da lista logo atrás da visão computadorizada.

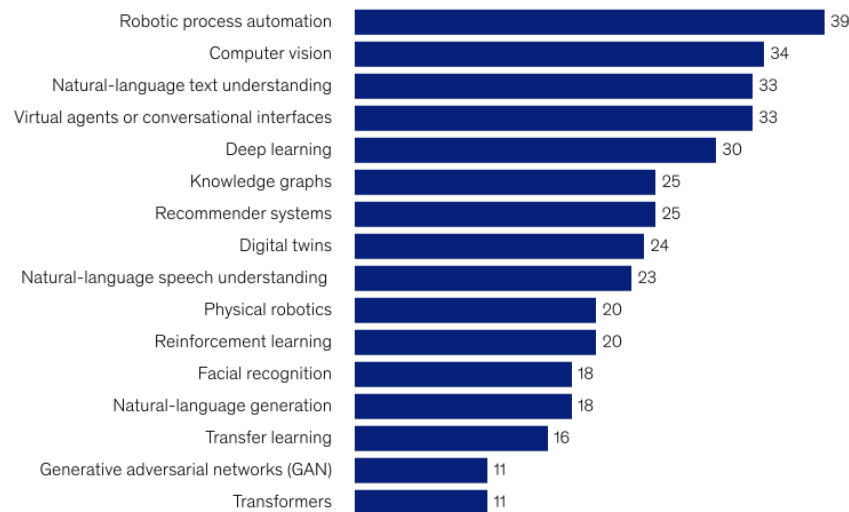
A explosão da inteligência artificial

Responses show an increasing number of AI capabilities embedded in organizations over the past five years.

Average number of AI capabilities that respondents' organizations have embedded within at least one function or business unit¹



Percentage of respondents who say given AI capability is embedded in products or business processes in at least one function or business unit²



¹The number of capabilities included in the survey has grown over time, from 9 in 2018 to 15 in the 2022 survey.

²Question was asked only of respondents who said their organizations have adopted AI in at least one function.

A explosão da inteligência artificial

Os casos mais populares de uso, no entanto, têm se mantido relativamente estáveis: a otimização das operações de serviço tem ocupado o primeiro lugar em cada um dos últimos quatro anos.

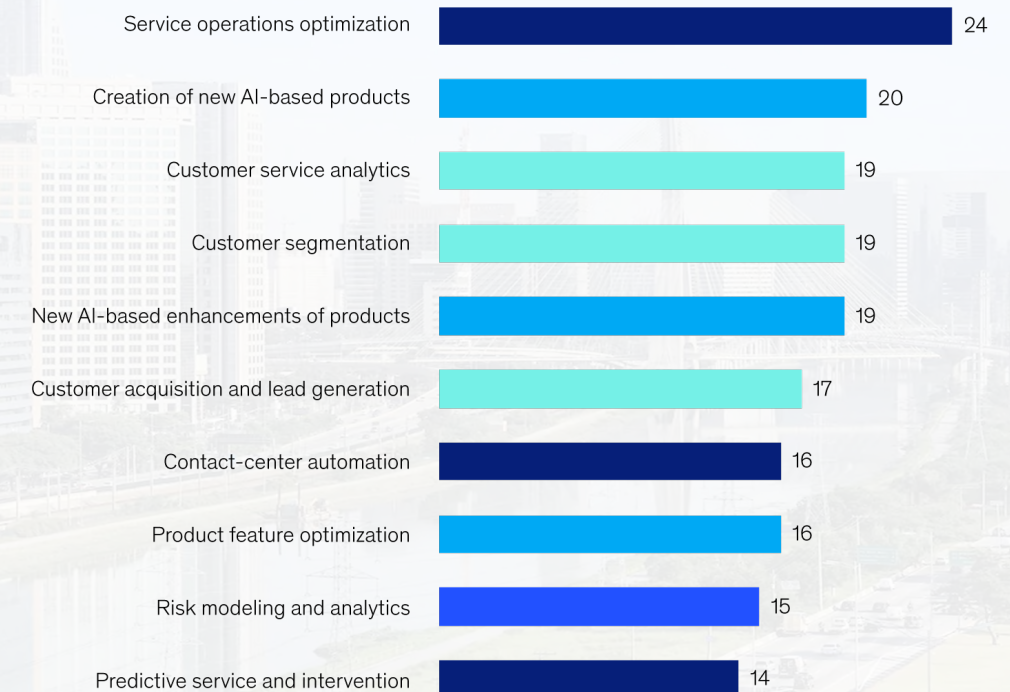
The most popular AI use cases span a range of functional activities.

Top use cases

Use cases by function

Most commonly adopted AI use cases, by function, % of respondents¹

■ Service operations² ■ Product and/or service development ■ Marketing and sales ■ Risk



¹ Out of 39 use cases. Question was asked only of respondents who said their organizations have adopted AI in at least one function.

² Eg, field services, customer care, back office.

A explosão da inteligência artificial

Em segundo lugar, o nível de investimento em IA aumentou junto com sua crescente adoção.

Por exemplo, há cinco anos, 40% dos entrevistados em organizações que usam IA relataram que mais de 5% de seus orçamentos digitais foram para a IA, enquanto agora mais da metade dos entrevistados relatam esse nível de investimento.

Seguindo adiante, 63% dos entrevistados dizem esperar que o investimento de suas organizações aumente nos próximos três anos.

A explosão da inteligência artificial

Em terceiro lugar, as áreas específicas em que as empresas veem o valor da IA têm evoluído.

Em 2018, a fabricação e o risco foram as duas funções nas quais as maiores partes dos entrevistados relataram ver o valor do uso da IA.

Hoje, os maiores efeitos de receita relatados são encontrados em marketing e vendas, desenvolvimento de produtos e serviços, estratégia e finanças corporativas, e os entrevistados relatam os maiores benefícios de custo da gripe aviária no gerenciamento da cadeia de fornecimento.

O valor de resultado obtido com a IA permanece forte e amplamente consistente. Cerca de um quarto dos entrevistados relatam este ano que pelo menos 5% do EBIT de suas organizações foi atribuível à IA em 2021, de acordo com os resultados dos dois anos anteriores, quando também rastreamos esta métrica.

A explosão da inteligência artificial

Por fim, uma coisa que tem permanecido preocupantemente consistente é o nível de comprometimento das organizações de mitigação de riscos para reforçar a confiança digital.

Embora o uso de IA tenha aumentado, não houve aumentos substanciais na mitigação relatada de qualquer risco relacionado à IA a partir de 2019 – quando começamos a capturar esses dados – até agora.

A explosão da inteligência artificial

Primeiro, não temos visto uma expansão no tamanho do grupo líder.



Nos últimos três anos, temos definido IA de alto desempenho como aquelas organizações que os respondentes dizem estar vendo o maior impacto da adoção de IA – isto é, 20% ou mais do EBIT do uso de IA.



A proporção de respondentes que se enquadram nesse grupo tem se mantido estável em cerca de 8%.



Os resultados indicam que este grupo está alcançando seus resultados superiores principalmente a partir da IA impulsionando os ganhos de primeira linha, pois é mais provável que eles informem que a IA está impulsionando as receitas ao invés de reduzir os custos, embora eles também informem que a IA está diminuindo os custos.

A explosão da inteligência artificial

Em seguida, é mais provável que os de alto desempenho sigam práticas essenciais que liberem valor, tais como ligar sua estratégia de IA aos resultados comerciais.



Também importante, eles estão se engajando mais frequentemente em práticas avançadas que permitem o desenvolvimento e a implantação de IA em escala, ou o que alguns chamam de “industrialização de IA”.



Por exemplo, os líderes estão mais propensos a ter uma arquitetura de dados que seja modular o suficiente para acomodar rapidamente novas aplicações de IA.

A explosão da inteligência artificial

Eles também automatizam frequentemente a maioria dos processos relacionados a dados, o que pode melhorar a eficiência no desenvolvimento de IA e expandir o número de aplicações que eles podem desenvolver, fornecendo mais dados de alta qualidade para alimentar os algoritmos de IA.



E as aplicações de IA de alto desempenho são 1,6 vezes mais prováveis que outras organizações de envolver funcionários não-técnicos na criação de aplicações de IA usando programas emergentes de código baixo ou sem código, que permitem que as empresas acelerem a criação de aplicações de IA.



Em 2022, as empresas de alto desempenho tornaram-se ainda mais propensas do que outras organizações a seguir certas práticas avançadas de escalonamento, como o uso de conjuntos de ferramentas padronizadas para criar dutos de dados prontos para produção e o uso de uma plataforma ponta a ponta para ciência de dados relacionados à IA, engenharia de dados e desenvolvimento de aplicações que elas desenvolveram internamente.

A explosão da inteligência artificial

Os profissionais de alto desempenho também podem ter um avanço no gerenciamento de riscos potenciais relacionados à IA, tais como privacidade pessoal e equidade e justiça, que outras organizações ainda não abordaram.

Embora, de modo geral, tenhamos visto poucas mudanças nas organizações relatando o reconhecimento e a mitigação dos riscos relacionados à IA desde que começamos a perguntar sobre eles há quatro anos, os entrevistados de alto desempenho em IA são mais propensos do que outros a relatar que eles se envolvem em práticas que são conhecidas por ajudar a mitigar os riscos.

Estas incluem assegurar a governança da IA e dos dados, padronizar processos e protocolos, automatizar processos como o controle de qualidade dos dados para remover erros introduzidos através de trabalho manual e testar a validade dos modelos e monitorá-los ao longo do tempo para possíveis problemas.

A explosão da inteligência artificial

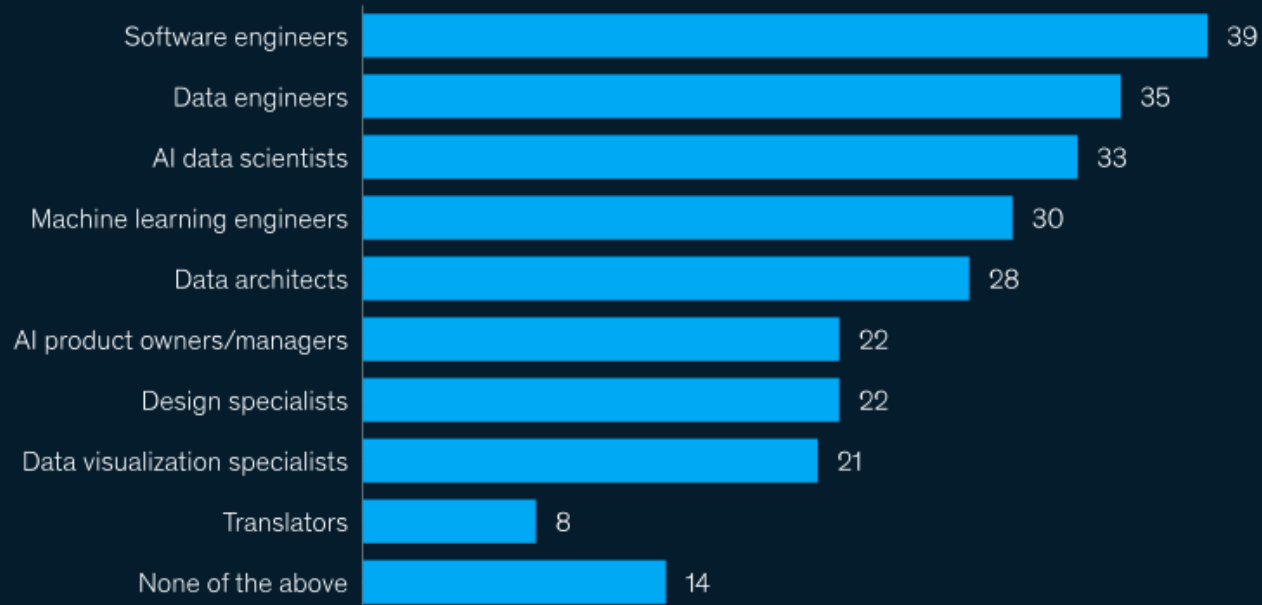
Os engenheiros de software surgiram como o papel da IA que as respostas à pesquisa mostram organizações contratadas com mais frequência no ano passado, mais frequentemente do que engenheiros de dados e cientistas de dados de IA.

Este é outro sinal claro de que muitas organizações deixaram de fazer experiências com IA para incorporá-la ativamente em aplicações empresariais.

A explosão da inteligência artificial

Responses suggest that organizations are most often hiring software engineers, data engineers, and AI data scientists.

AI-related roles that respondents' organizations hired, past year, % of respondents¹



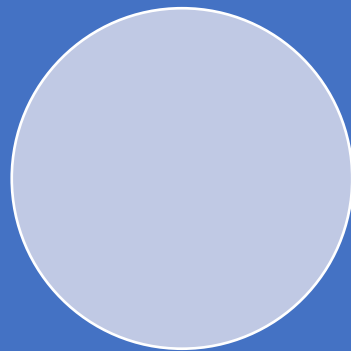
¹Only asked of respondents whose organizations have adopted AI in at least one function; n = 744.

McKinsey & Company

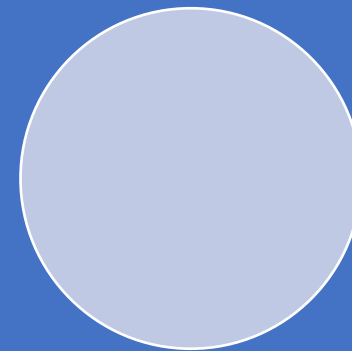
A explosão da inteligência artificial



Infelizmente, a escassez de talentos tecnológicos não mostra sinais de abrandamento, ameaçando retardar essa mudança para algumas empresas.



A maioria dos entrevistados relata dificuldades em contratar para cada função relacionada à IA no ano passado, e a maioria diz que ou não foi mais fácil ou foi mais difícil adquirir este talento do que em anos anteriores.



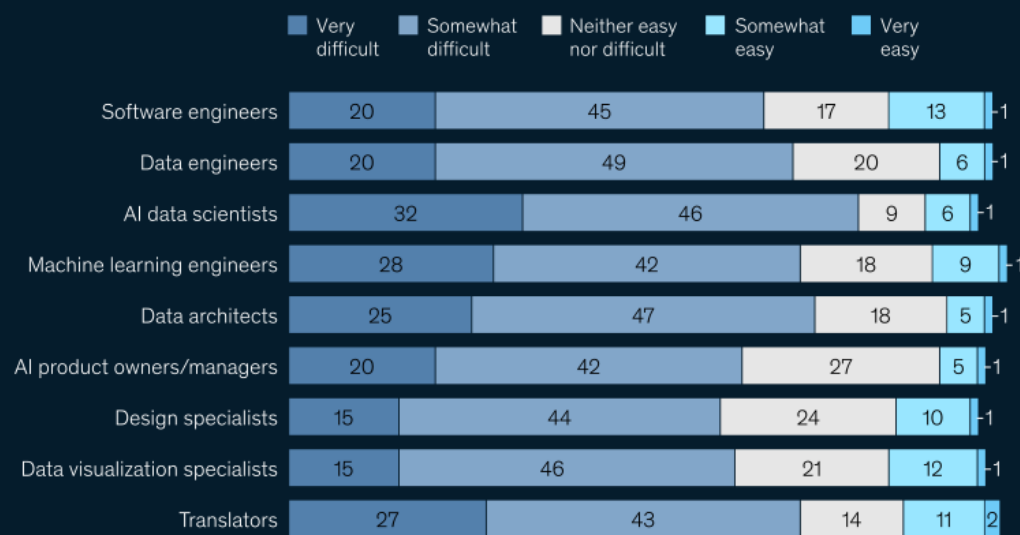
Os cientistas de dados de IA continuam sendo particularmente escassos, com a maior parte dos entrevistados classificando os cientistas de dados como uma função que tem sido difícil de preencher, fora das funções sobre as quais perguntamos.



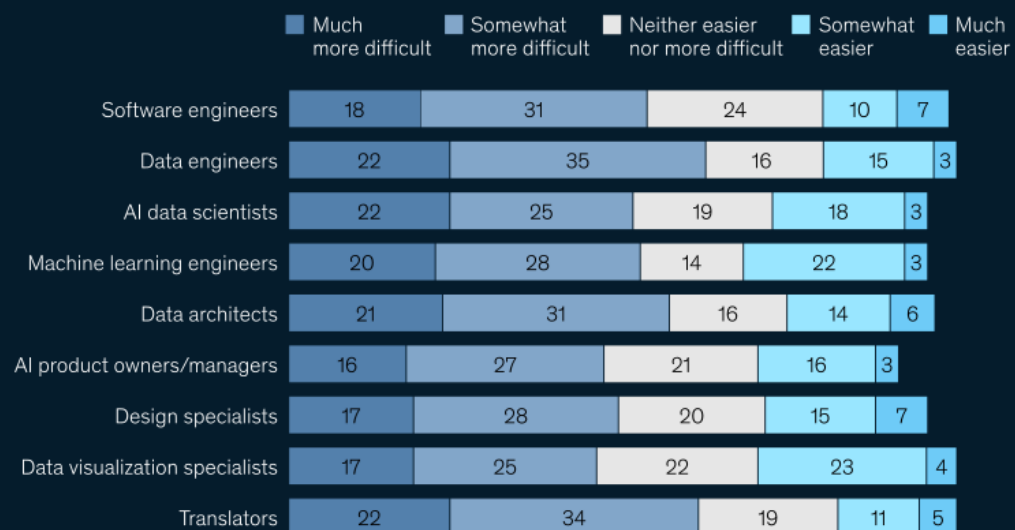
A explosão da inteligência artificial

Most respondents say that hiring for each AI-related role has been difficult in the past year and hasn't become easier over time.

Difficulty in organizations' hiring of AI-related roles, past year, % of respondents¹

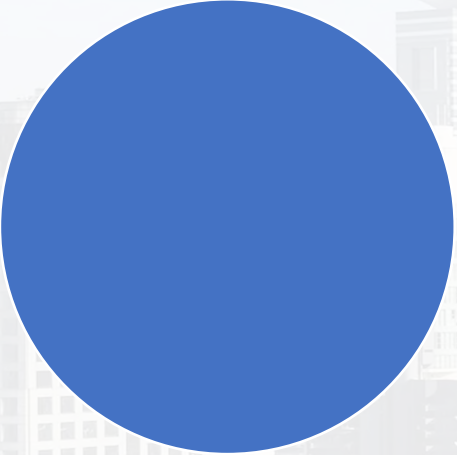


Change of difficulty in organizations' hiring of AI-related roles, past 3 years, % of respondents¹

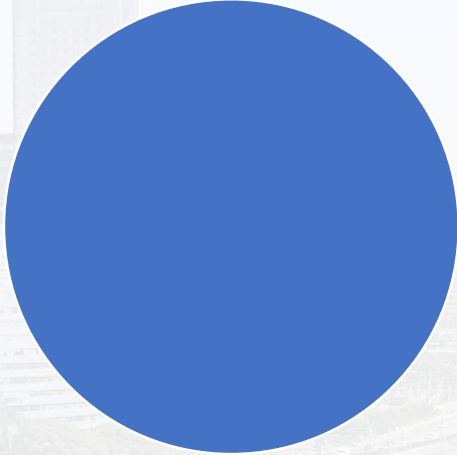


¹Only asked of respondents whose organizations have adopted AI in at least one function. Figures do not sum to 100%, because respondents who said "don't know" are not shown.

Regulamentos e a falta de regulamentos




UE: Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (“Regulamento Inteligência Artificial”) e altera determinados atos legislativos da União [Europeia]

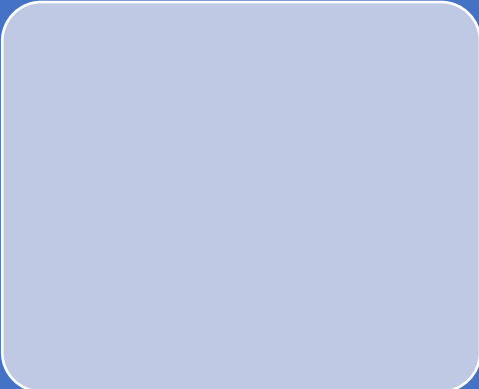


BR: PL 21/2020 – Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências.

Regulamentos e a falta de regulamentos



UE: «Sistema de inteligência artificial» (sistema de IA), um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage;



BR: Por inteligência artificial, entende-se o “sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões, que possam influenciar o ambiente virtual ou real.”

Regulamentos e a falta de regulamentos

UE, Anexo I – técnicas e abordagens à IA

A) Abordagens de aprendizagem automática, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos, designadamente aprendizagem profunda;

B) Abordagens baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais;

C) Abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização.

Regulamentos e a falta de regulamentos

UE, Art.

5º:

Proibições
– sistemas
de IA que:

Empregue técnicas subliminares que contornem a consciência de uma pessoa para distorcer substancialmente o seu comportamento de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

Explore quaisquer vulnerabilidades de um grupo específico de pessoas associadas à sua idade ou deficiência física ou mental;

Regulamentos e a falta de regulamentos

UE, Art. 5º: Proibições – sistemas de IA que:

Autoridades públicas ou em seu nome para efeitos de avaliação ou classificação da credibilidade de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas ou previsíveis, em que a classificação social conduz a tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos, ou tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas que é injustificado e desproporcionado face ao seu comportamento social ou à gravidade do mesmo;

A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública - exceções: investigação seletiva de potenciais vítimas específicas de crimes; prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física (ataque terrorista); detecção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal.

Regulamentos e a falta de regulamentos

UE, Art.
5º:
Risco
elevado:

Independentemente de a colocação no mercado ou a colocação em serviço de um sistema de IA ser feita separadamente dos produtos a que se referem as alíneas a) e b), esse sistema de IA é considerado de risco elevado quando estejam satisfeitas ambas as condições que se seguem:

A) O sistema de IA destina-se a ser utilizado como um componente de segurança de um produto ou é, ele próprio, um produto abrangido pela legislação de harmonização da União enumerada no anexo II;

B) Nos termos da legislação de harmonização da União enumerada no anexo II, o produto cujo componente de segurança é o sistema de IA, ou o próprio sistema de IA enquanto produto deve ser sujeito a uma avaliação da conformidade por terceiros com vista à colocação no mercado ou à colocação em serviço.

Regulamentos e a falta de regulamentos

UE, Art. 5º:
Risco elevado:

Além dos sistemas de IA de risco elevado referidos no n.º 1, os sistemas de IA referidos no anexo III são também considerados de risco elevado.

Regulamentos e a falta de regulamentos

UE, Anexo III: Risco elevado:

Identificação
biométrica e
categorização de
pessoas
singulares

Gestão e
funcionamento
de
infraestruturas
críticas

Educação e
formação
profissional

Emprego, gestão
de trabalhadores
e acesso ao
emprego por
conta própria

Regulamentos e a falta de regulamentos

UE, Anexo III: Risco elevado:

Acesso a serviços privados e a serviços e prestações públicas essenciais, bem como o usufruto dos mesmos

Manutenção da ordem pública

Gestão da migração, do asilo e do controlo das fronteiras

Administração da justiça e processos democráticos

Regulamentos e a falta de regulamentos

Art. 9º: Um sistema de gestão de riscos é obrigatório quando houver utilização de IA de risco elevado.

Art. 13, transparência: Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que assegure que o seu funcionamento seja suficientemente transparente para permitir aos utilizadores interpretar o resultado do sistema e utilizá-lo corretamente. Deve ser garantido um tipo e um grau adequado de transparência, que permita cumprir as obrigações que incumbem ao utilizador e ao fornecedor.

Art. 14, supervisão humana: Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de IA.

Art. 15, exatidão, solidez e cibersegurança: Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que alcancem, tendo em conta a finalidade prevista, um nível apropriado de exatidão, solidez e cibersegurança e apresentem um desempenho coerente em relação a tais aspetos durante o ciclo de vida.

Art. 51, registro: Antes da colocação no mercado ou da colocação em serviço de um sistema de IA de risco elevado, o fornecedor ou, se for caso disso, o mandatário deve registrar esse sistema na base de dados da UE.

Uso de dados e definição de perfil

O que é definição de perfis? Sem definição na LGPD.

RGPD, Art. 4º, nº 4: «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

LGPD, Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Uso de dados e definição de perfil

Desafio:
treinamento de
inteligência
artificial – uso
secundário dos
dados pessoais

Estabelecimento de *sandboxes* (“ambiente de testagem”) sob certas condições (apenas algumas a seguir):

Os sistemas de IA inovadores devem ser desenvolvidos para salvaguarda de um interesse público substancial;

Todos os dados pessoais a tratar no contexto do ambiente de testagem se encontram num ambiente de tratamento de dados funcionalmente separado, isolado e protegido sob o controlo dos participantes, sendo apenas acessíveis a pessoas autorizadas;

Nenhuns dados pessoais tratados são transmitidos, transferidos ou cedidos, de outro modo, por terceiros.

Uso de dados e definição de perfil

Primeiro, as organizações devem colocar equipes jurídicas e de gestão de risco voltadas para os negócios, juntamente com a equipe de ciência dos dados, no centro do processo de desenvolvimento da IA.

Esperar até depois do desenvolvimento dos modelos de IA para determinar onde e como mitigar os riscos é muito ineficiente e demorado em um mundo de implantações rápidas de IA.

Em vez disso, a análise de risco deve ser parte do projeto inicial do modelo de IA, incluindo os processos de coleta de dados e governança.

O envolvimento de profissionais jurídicos, de risco e tecnológicos desde o início permite que eles funcionem como uma “equipe de confiança tecnológica” que assegura que os modelos estejam em conformidade com as normas sociais e os requisitos legais, ao mesmo tempo em que ainda oferecem o máximo valor comercial.

Uso de dados e definição de perfil

Em segundo lugar, como não há uma solução definitiva para o amplo espectro de riscos de IA, as organizações devem aplicar um plano de priorização de risco informado como passo inicial de uma abordagem eficaz e dinamicamente atualizada de gerenciamento de risco de IA ancorada tanto na orientação legal quanto nas melhores práticas técnicas.

Tal plano de priorização envolve a criação de um catálogo dos riscos específicos de IA de sua organização para definir os danos que você procura evitar, e então seguir uma metodologia clara para avaliar e priorizar esses riscos para mitigação.

IA – 6 principais erros

Privacidade. Os dados são a força vital de qualquer modelo de IA. As leis de privacidade em todo o mundo determinam como as empresas podem (e não podem) usar os dados, enquanto as expectativas dos consumidores estabelecem padrões normativos. A violação dessas leis e normas pode resultar em responsabilidade significativa, bem como em danos aos consumidores. A violação da confiança dos consumidores, mesmo que o uso dos dados fosse tecnicamente lícito, também pode levar a riscos à reputação e a uma diminuição da lealdade do cliente.

Segurança. Novos modelos de IA têm vulnerabilidades complexas e evolutivas que criam tanto riscos novos quanto familiares. Vulnerabilidades como extração de modelos e envenenamento de dados (nos quais dados "ruins" são introduzidos no conjunto de treinamento, afetando a produção do modelo) podem representar novos desafios para abordagens de segurança de longa data. Em muitos casos, as estruturas legais existentes exigem padrões mínimos de segurança a serem cumpridos.

IA – 6 principais erros

Equidade. Pode ser fácil codificar inadvertidamente o viés nos modelos de IA ou introduzir o viés que se esconde na alimentação de dados no modelo. O viés que possa ou realmente prejudique classes e grupos particulares pode expor a empresa a riscos e responsabilidades de justiça.

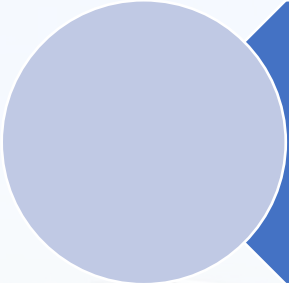
Transparência e explicabilidade. A falta de transparência em torno de como um modelo foi desenvolvido (como, por exemplo, como os conjuntos de dados que alimentam um modelo foram combinados) ou a incapacidade de explicar como um modelo chegou a um determinado resultado pode levar a problemas, o que não é o menor dos quais é potencialmente prejudicial aos mandatos legais. Por exemplo, se um consumidor inicia um inquérito sobre como seus dados foram usados, a organização que usa os dados precisará saber em quais modelos os dados foram alimentados.

IA – 6 principais erros

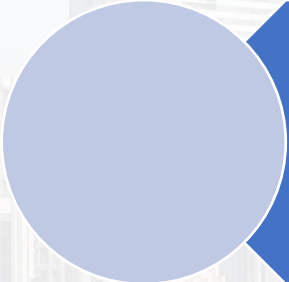
Segurança e desempenho. As aplicações de IA, se não forem implementadas e testadas adequadamente, podem sofrer problemas de desempenho que violam as garantias contratuais e, em casos extremos, representam ameaças à segurança pessoal. Suponha que um modelo seja usado para assegurar atualizações oportunas de máquinas na fabricação ou mineração; uma falha deste modelo poderia constituir negligência sob um contrato e/ou levar a danos aos funcionários.

Riscos de terceiros. O processo de construção de um modelo de IA frequentemente envolve terceiros. Por exemplo, as organizações podem terceirizar a coleta de dados, seleção de modelos ou ambientes de implantação. A organização que envolve terceiros deve conhecer e compreender os padrões de mitigação de riscos e governança aplicados por cada terceiro, e deve testar e auditar independentemente todos os inputs de alto risco.


Os riscos da IA



A maioria dos riscos de IA mapeia pelo menos um dos tipos de riscos globais descritos acima, e eles frequentemente abrangem vários tipos.



Por exemplo, um ataque de extração de modelo, no qual um modelo é roubado com base em um conjunto de amostras de resultados, compromete tanto a privacidade quanto a segurança do modelo.



Portanto, as organizações devem perguntar se cada categoria de risco pode resultar de cada modelo ou ferramenta de IA que a empresa está considerando ou já está usando.

Os riscos da IA



O ChatGPT

Como funciona o ChatGPT?

O que é o ChatGPT? “O ChatGPT é aperfeiçoado a partir do GPT-3.5, um modelo de linguagem treinado para produzir texto. O ChatGPT foi otimizado para o diálogo usando o Reforço da Aprendizagem com Feedback Humano (RLHF) – um método que usa demonstrações humanas e comparações de preferências para guiar o modelo em direção ao comportamento desejado.”

Por que a IA parece tão real e natural?

“Estes modelos foram treinados em grandes quantidades de dados da Internet escritos por humanos, incluindo conversas, de modo que as respostas que ela fornece podem soar como humanas. É importante ter em mente que este é um resultado direto do projeto do sistema (ou seja, maximizar a similaridade entre as saídas e o conjunto de dados nos quais os modelos foram treinados) e que tais saídas podem ser imprecisas, inverídicas e, de outra forma, enganosas às vezes.”

O ChatGPT

Quem pode ver
minhas
conversas?

Vocês vão usar
minhas conversas
para
treinamento?

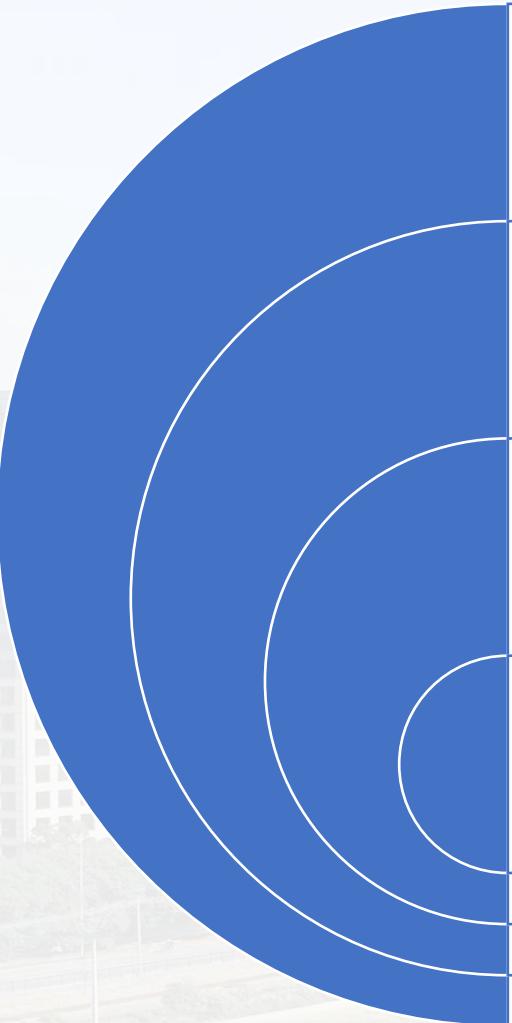
Você pode
apagar meus
dados?

“Como parte de nosso compromisso com a IA segura e responsável, revisamos as conversas para melhorar nossos sistemas e garantir que o conteúdo esteja em conformidade com nossas políticas e exigências de segurança.”

“Sim. Suas conversas podem ser revisadas por nossos instrutores de AI para melhorar nossos sistemas.”

“Sim, por favor, siga o processo de exclusão de dados.”

O ChatGPT



O ChatGPT é sustentado por um modelo de linguagem de grande porte que requer grandes quantidades de dados para funcionar e melhorar.

Quanto mais dados o modelo for treinado, melhor ele conseguirá detectar padrões, antecipando o que virá em seguida e gerando texto plausível.

A OpenAI, a empresa por trás do ChatGPT, alimentou a ferramenta com cerca de 300 bilhões de palavras sistematicamente “raspadas” da Internet: livros, artigos, sites e posts – incluindo dados pessoais obtidos sem consentimento.

Se você já escreveu um post em um blog ou uma revisão de produto, ou comentou um artigo online, há uma boa chance de que esta informação tenha sido utilizada pelo ChatGPT.

O ChatGPT



A coleta de dados usada para treinar o ChatGPT é problemática por várias razões.

Primeiro, nenhum de nós foi perguntado se a OpenAI poderia usar nossos dados. Isto é uma clara violação de privacidade, especialmente quando os dados são sensíveis e podem ser usados para nos identificar, aos membros de nossa família, ou à nossa localização.

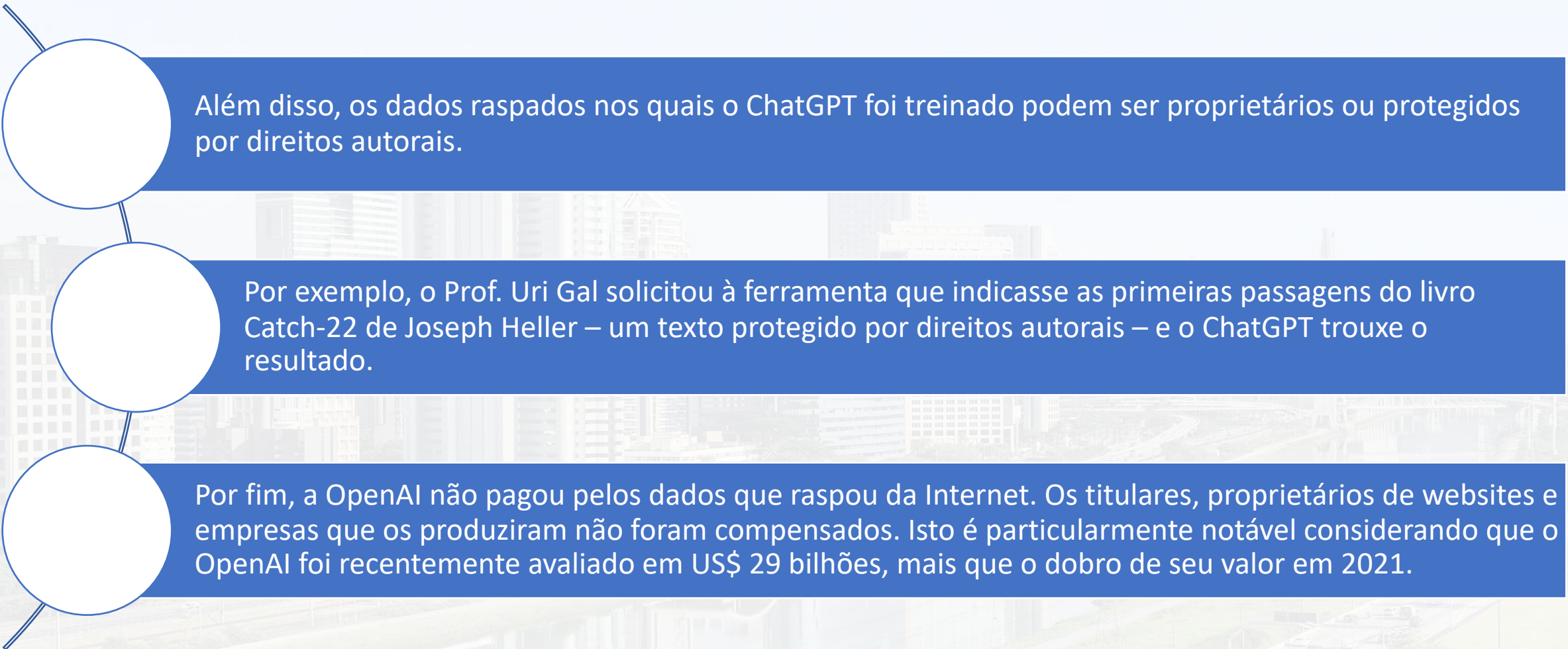
Mesmo quando os dados estão disponíveis publicamente, seu uso pode violar o que chamamos de integridade contextual. Este é um princípio fundamental nas discussões jurídicas sobre privacidade: ele exige que os dados dos indivíduos não sejam revelados fora do contexto no qual eles foram originalmente produzidas.

O ChatGPT

Além disso, a OpenAI não oferece procedimentos para que os titulares verifiquem se a empresa armazena seus dados pessoais, ou para solicitar a sua eliminação. Este é um direito garantido de acordo com o Regulamento Geral sobre a Proteção de Dados e também com a LGPD – embora ainda esteja em debate se o ChatGPT está de acordo com as exigências destas legislações.

Este “direito a ser esquecido” é particularmente importante nos casos em que as informações são inexatas ou enganosas, o que parece ser uma ocorrência regular com o ChatGPT.

O ChatGPT



Além disso, os dados raspados nos quais o ChatGPT foi treinado podem ser proprietários ou protegidos por direitos autorais.

Por exemplo, o Prof. Uri Gal solicitou à ferramenta que indicasse as primeiras passagens do livro Catch-22 de Joseph Heller – um texto protegido por direitos autorais – e o ChatGPT trouxe o resultado.

Por fim, a OpenAI não pagou pelos dados que raspou da Internet. Os titulares, proprietários de websites e empresas que os produziram não foram compensados. Isto é particularmente notável considerando que o OpenAI foi recentemente avaliado em US\$ 29 bilhões, mais que o dobro de seu valor em 2021.

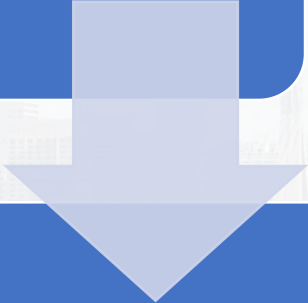
O ChatGPT

O OpenAI também acaba de anunciar o ChatGPT Plus, um plano de assinatura paga que oferecerá aos clientes acesso contínuo à ferramenta, tempos de resposta mais rápidos e acesso prioritário a novos recursos. Este plano contribuirá para uma receita esperada de US\$1 bilhão até 2024.

Nada disto teria sido possível sem os dados – nossos dados – coletados e utilizados sem nossa permissão.

O ChatGPT

Outro risco à privacidade envolve os dados fornecidos ao ChatGPT sob a forma de solicitações do usuário. Quando pedimos à ferramenta para responder perguntas ou executar tarefas, podemos inadvertidamente entregar dados sensíveis e colocá-los em domínio público.



Por exemplo, um advogado pode solicitar à ferramenta que reveja um rascunho de acordo de divórcio, ou um programador pode solicitar que ela verifique um pedaço de código. O acordo e o código, além das redações produzidas, fazem agora parte do banco de dados do ChatGPT. Isto significa que eles podem ser usados para treinar ainda mais a ferramenta, e ser incluídos em respostas a pedidos de outras pessoas.

O ChatGPT

Além disso, a OpenAI reúne um amplo escopo de outras informações do usuário. De acordo com o aviso de privacidade da empresa, ele coleta o endereço IP dos usuários, tipo de navegador e configurações, e dados sobre as interações dos usuários com o site – incluindo o tipo de conteúdo com o qual os usuários se envolvem, as características que eles usam e as ações que tomam.



Ela também coleta informações sobre as atividades de navegação dos usuários ao longo do tempo e através dos sites. De maneira alarmante, a OpenAI afirma que pode compartilhar informações pessoais dos usuários com terceiros não especificados, sem informá-los, para cumprir seus objetivos comerciais.

O ChatGPT cumpre com a LGPD?

Uma das principais preocupações com esses modelos de aprendizagem de linguagem como o ChatGPT é a privacidade, e pode ser difícil para as pessoas saber se seus dados foram usados para treinar um modelo de aprendizagem de máquinas.

O GPT-3, por exemplo, é um modelo de linguagem de grande porte que foi treinado em uma grande quantidade de dados da Internet, incluindo sites pessoais e conteúdo de mídia social.

Isto levou à preocupação de que o modelo possa usar os dados das pessoas sem sua permissão e que possa ser difícil controlar ou apagar os dados que foram usados para treinar o modelo.

O ChatGPT cumpre com a LGPD?

Atualmente, não há nenhum método amplamente aceito para que os titulares solicitem a remoção de seus dados de um modelo de aprendizagem de máquina uma vez que este tenha sido usado para treinar o modelo.

Alguns pesquisadores e empresas estão trabalhando em métodos para permitir a remoção ou o “esquecimento” de pontos de dados específicos ou informações do usuário, mas estes métodos ainda estão nos estágios iniciais de desenvolvimento e ainda não está claro o quão viável ou eficaz eles serão.

Além disso, existem desafios técnicos para remover dados de modelos de aprendizagem de máquinas, pois os dados podem ter sido usados para treinar o modelo e sua remoção pode fazer com que o modelo perca sua precisão.

O ChatGPT cumpre com a LGPD?

O ChatGPT cumpre com os princípios da finalidade, necessidade e adequação (além dos demais, é claro)?

Para além dos princípios, o controlador deve cumprir com os direitos da LGPD, tais como o direito de ser informado, direito de acesso, direito de retificação, direito de apagamento, direito de objeção e direito de portabilidade de dados.

Parece que os modelos de aprendizagem de linguagem natural não estão de acordo com a LGPD.

Inteligência Artificial e Privacidade





Obrigado pela parceria e pela paciência 😊

Instagram: @profmatheuspassos, @tiexames, @data_ux