



Sumário

Introdução

- Este guia é Open Source
 - Visão geral dos capítulos
-

1 Como a IA pode criar valor?

2 Como a sua organização pode criar valor a partir da IA?

- Dados como pré-requisito para a IA
 - Defina o nível certo de ambição
 - Escolha as áreas de valor certas
 - Experimente e aprenda!
 - Personalize e amplie!
-

3 Considerações éticas

- IA centrada no ser humano e *accountability*
 - Transparência e explicabilidade
 - Equidade e vieses
 - Padrões obscuros e manipulação
 - Dependência da IA
 - Impacto ambiental e climático
 - Hierarquias intencionais e dilemas éticos
-

4 Governança, qualidade e risco

- Governança
 - Gestão de Risco
 - Compliance
-

5 Compreensão das obrigações legais para a utilização da IA na Europa

6 AI Act (Lei de Inteligência Artificial da União Europeia)

- Funções dos operadores no AI Act
 - Modelos gerais – GPAI
 - Aprovação do AI Act
 - Impacto no Reino Unido e na Suíça
-

7 Privacidade e o GDPR

- Avaliação de riscos e Avaliação de Impacto à Proteção de Dados (DPIA)
 - Documentação
 - Preparação dos colaboradores
 - Privacidade e inovação
 - IA e os princípios fundamentais do GDPR
-

8 Legislação Trabalhista

- GDPR: Requisitos no ambiente de trabalho
 - AI Act: Requisitos e restrições no ambiente de trabalho
 - Guia de IA no ambiente de trabalho
-

9 Direitos de Propriedade Intelectual

- Direitos autorais sobre conteúdo gerado por IA
 - Risco de violação de direitos de propriedade intelectual de terceiros
 - Dados de treinamento
 - Proteção contra ações judiciais ao utilizar modelos de IA pré-treinados
-

10 Termos e condições de licença

- Serviços gratuitos de IA
-

Histórico do documento e agradecimento

- Fontes e colaboradores
 - Histórico de revisões
-



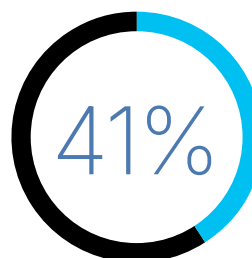
Introdução

A inteligência artificial (IA) evoluiu rapidamente e se tornou uma das tecnologias mais transformadoras do nosso tempo, especialmente após o lançamento do ChatGPT em 2022. A Experis e a Vaar Law elaboraram este guia para ajudar líderes, profissionais e tomadores de decisão a explorar o potencial da IA de forma responsável, sustentável e eficaz.

Em toda a Europa, a IA está remodelando empresas e instituições públicas. [Uma pesquisa realizada pelo Eurostat em 2024](#) revelou que **41% das grandes empresas** já integram IA em suas operações, um aumento em relação aos 30% do ano anterior. O setor público avança ainda mais rapidamente: um estudo de 2024 do [Centro Comum de Pesquisa da União Europeia](#) mostrou que mais da metade (51,8%) dos 576 gestores públicos entrevistados já havia implementado pelo menos um projeto de IA, e 63,1% planejavam novas iniciativas em breve.

A IA abre oportunidades substanciais para inovação e crescimento. Ela pode otimizar operações, aumentar a eficiência e viabilizar novos produtos, serviços e modelos de negócio. Ainda assim, muitas organizações enfrentam dificuldades para transformar o potencial da IA em resultados concretos. Desafios relacionados à qualidade dos dados, dilemas éticos, complexidade jurídica e riscos emergentes frequentemente impedem o sucesso. Este guia aborda essas questões ao responder a duas perguntas centrais:

- **Como podemos implementar a IA de forma estratégica para gerar valor real, evitando o desperdício de recursos em iniciativas com resultados limitados?**
- **Como podemos adotar a IA de maneira responsável e sustentável, garantindo conformidade legal, gestão de riscos e alinhamento com os valores fundamentais da organização?**



das grandes empresas agora integram IA nas suas operações.

A implementação de IA exige uma abordagem holística, que alinhe as iniciativas de IA à visão estratégica e aos valores da organização, estabeleça estruturas sólidas de governança e promova investimentos estratégicos em gestão de dados, desenvolvimento de competências, frameworks éticos e expertise jurídica. E, naturalmente, também é necessário investir na infraestrutura tecnológica adequada para dados e IA.

Este guia oferece orientações claras e práticas para ajudar sua organização a navegar pelo ecossistema da inteligência artificial e transformar oportunidades em sucesso sustentável.

Caso tenha dúvidas ou comentários, entre em contato com Jørgen Longva, Diretor de Competências da Experis AS (jorgen.longva@no.experis.com), ou com Thor Beke, Sócio-Diretor da Vaar Advokat AS (thor@vaar.law).

Este guia é Open Source!

A Experis e a Vaar querem que todas as organizações tenham acesso ao melhor conhecimento possível sobre o uso da inteligência artificial. Por isso, este guia pode ser utilizado e adaptado livremente para atender às necessidades da sua organização!

O guia é licenciado sob a licença CC-BY, o que significa que você pode usar e modificar o texto deste documento, desde que reconheça que ele se baseia em conteúdo desenvolvido pela Experis e pela Vaar. Isso não se aplica a logotipos, identidade visual ou outros conteúdos proprietários da Experis e da Vaar.

Não hesite em entrar em contato caso deseje receber este documento em formato Word.

Visão geral dos capítulos



1 Como a IA pode criar valor?

- Reconheça a capacidade da IA de otimizar, transformar e modificar fundamentalmente processos e produtos nos setores público e privado.
- Explore diferentes tecnologias de IA para compreender como elas criam novas oportunidades.
- Identifique aplicações relevantes para sua organização a partir de exemplos concretos em diferentes setores.



2 Como sua organização pode criar valor a partir da IA?

- Alinhe o nível de ambição às condições estruturais e à maturidade tecnológica da sua organização para identificar as áreas de maior valor para implementação de IA.
- Experimente a IA por meio de pequenos projetos-piloto para compreender oportunidades e limitações antes de profissionalizar e escalar soluções. Familiarize-se com a *Lab Illusion* e o "efeito iceberg".
- Construa uma infraestrutura tecnológica robusta, incluindo uma plataforma de dados e uma plataforma de IA, e estabeleça um centro de expertise em IA.



3 Considerações éticas

- Garanta que a IA apoie, e não substitua, o julgamento e a tomada de decisão humanos.
- Mantenha transparência ao explicar os processos decisórios e assegure compreensão por todas as partes envolvidas.
- Teste e ajuste sistemas de forma proativa para lidar com vieses, garantir equidade e evitar resultados discriminatórios.



4 Governança, qualidade e risco

- Implemente estruturas de governança que alinhem a estratégia de IA aos objetivos gerais da organização, com papéis e responsabilidades claramente definidos.
- Monitore continuamente os sistemas de IA para garantir que funcionem conforme o esperado e mantenham alta qualidade dos dados.
- Avalie riscos de falhas ou interrupções nos sistemas de IA e estabeleça planos de redundância e mecanismos de controle para erros inesperados, especialmente em processos críticos.



5 Compreensão das obrigações legais para o uso de IA na Europa

- Garanta que o uso de IA esteja em conformidade com todas as leis e regulamentações aplicáveis, incluindo proteção de dados e legislações antidiscriminatórias, bem como DSA, DMA, DORA e o Cyber Resilience Act.
- Desenvolva uma estratégia de conformidade que integre conhecimento jurídico e medidas tecnológicas, com auditorias regulares para demonstrar conformidade.
- Documente avaliações de privacidade e jurídicas ao longo de todo o ciclo de vida dos sistemas de IA para garantir conformidade.



6 AI Act

- Avalie se o uso de IA pela organização está sujeito ao AI Act.
- Determine a categoria de risco das aplicações de IA.
- Esclareça o papel da organização como provedora ou usuária, pois isso afeta os requisitos aplicáveis.
- Identifique obrigações com base no nível de risco e no papel exercido e implemente as medidas de conformidade necessárias.



7 Privacidade e o GDPR

- Realize uma avaliação de riscos e considere ou realize uma DPIA antes da implementação.
- Implemente as medidas necessárias para reduzir os riscos.
- Desenvolva diretrizes e rotinas de treinamento, atualizando o protocolo de processamento, a declaração de privacidade e a documentação de conformidade.
- Mantenha esforços contínuos em matéria de privacidade com treinamentos regulares, políticas acessíveis, sistemas de comunicação e monitoramento contínuo dos riscos.



8 Legislação Trabalhista

- Envolver os colaboradores na implementação de ferramentas de IA, solicitando sugestões e informando-os sobre o uso.
- Ofereça treinamento para garantir o uso correto e legal das ferramentas de IA, disponibilizando guias e facilitando o feedback dos colaboradores.
- Garanta a conformidade com o GDPR, o IA Act e outras legislações relevantes ao usar IA para fins de RH.
- Certifique-se de que os colaboradores tenham acesso a recursos de apoio, como aconselhamento e assistência jurídica, caso tenham preocupações sobre o uso de ferramentas de IA.



9 Direitos de propriedade intelectual

- Reconheça que o conteúdo gerado por IA pode ser protegido por direitos autorais se expressar suficientemente o esforço intelectual.
- Verifique os modelos de IA pré-treinados quanto a possíveis violações dos direitos de propriedade intelectual de terceiros, verificando as restrições impostas pelos fornecedores.
- Documente o uso e o licenciamento dos dados de treino para garantir a conformidade com as leis de direitos autorais aplicáveis.



10 Termos e condições de licenciamento

- Analise cuidadosamente os termos da solução, com foco na propriedade dos dados, responsabilidade, limitações de uso e direitos de propriedade intelectual.
- Aceite a responsabilidade por erros ou danos causados por sistemas de IA, pois a responsabilidade geralmente recai sobre a organização que os utiliza.
- Evite soluções de IA gratuitas sempre que possível, pois elas geralmente apresentam riscos mais elevados de violação da segurança e privacidade dos dados.



Como a IA pode criar valor?



A inteligência artificial pode gerar valor significativo para sua organização ao melhorar processos existentes ou introduzir soluções inovadoras. A IA continua impulsionando a inovação e a eficiência nos setores público e privado.

Cada vez mais empresas precisarão considerar a IA como um fator competitivo essencial nos próximos anos. Compreender como a IA molda o mercado, como aproveitar seu potencial e como implementá-la de forma eficaz será decisivo para manter vantagem competitiva.

Para ajudar a entender como a IA cria valor, exploraremos diferentes tipos de IA e analisaremos como eles podem transformar diversos aspectos das operações empresariais. Começaremos pelos tipos de IA mais acessíveis e amplamente utilizados e avançaremos gradualmente para modelos mais avançados e especializados.

A **IA preditiva** prevê resultados futuros com base em dados históricos. Ela é particularmente útil para previsões financeiras, previsão de demanda de clientes, gestão de riscos e manutenção de equipamentos. A IA pode analisar grandes volumes de dados para identificar padrões que indicam eventos futuros.

Oda: Prevendo as necessidades dos clientes

Oda, um supermercado online, [utiliza modelos de IA preditiva para oferecer recomendações personalizadas de produtos](#) com base nas compras anteriores e nos padrões de consumo dos clientes. O sistema antecipa quando os clientes podem precisar de determinados itens e sugere produtos relevantes no momento certo.



O algoritmo de IA não apenas recomenda itens frequentemente comprados, mas também sugere produtos similares para aumentar a variedade no carrinho de compras. Isso simplifica a experiência de compra e incentiva os clientes a experimentar novos produtos. O objetivo é oferecer experiências de compra eficientes, que economizem tempo e forneçam inspiração.



Modelos de classificação organizam e estruturam grandes conjuntos de dados ao categorizar informações. Eles podem, por exemplo, classificar e-mails como spam, identificar clientes de alto risco, filtrar solicitações de crédito de maior risco ou analisar imagens médicas para fins de diagnóstico.

Modelos de transformação convertem dados de um formato para outro, como traduzir textos entre idiomas, converter imagens em texto ou transcrever gravações de áudio em texto. A IA também pode transformar dados não estruturados em formatos estruturados, viabilizando a automação de processos que antes eram inviáveis ou excessivamente caros. Isso é conhecido como hiperautomação.

Um conceito central aqui é o chamado “último gargalo”: eliminar a etapa manual final de um fluxo de trabalho pode reduzir o tempo de processamento de semanas ou dias para apenas minutos ou segundos. Essa mudança permite dinâmicas completamente novas — inovações verdadeiramente transformadoras. Um exemplo clássico são os bancos que oferecem verificações de crédito e aprovações de empréstimos instantâneas online, obtendo vantagem competitiva por meio de acesso rápido e fluido ao crédito.

A **IA generativa**, como o ChatGPT, cria novos conteúdos, como textos, imagens, áudios e vídeos. Isso a torna altamente adequada para geração de conteúdo, incluindo materiais de marketing e soluções criativas em design e desenvolvimento de produtos. A IA generativa também pode converter dados não estruturados em formatos estruturados para processamento automatizado em sistemas de TI. Ao permitir que máquinas operem por meio de linguagem natural, os modelos de transformação e generativos possibilitam que robôs realizem tarefas complexas e interajam de forma mais eficaz com humanos.

A **IA de otimização** maximiza a eficiência na produção, no planejamento de rotas, no uso de materiais e na alocação da força de trabalho. Esses modelos resolvem problemas complexos demais para a programação tradicional. Quando a IA automatiza e acelera essas tarefas, ela desbloqueia novas eficiências de processo e permite simulações de cenários para planejamento estratégico.

O município de Bodø utiliza IA generativa para interação com documentos jurídicos

A solução reduz drasticamente o tempo necessário para resumir documentos jurídicos. Funcionários municipais conseguem encontrar informações precisas e relevantes rapidamente, pois o sistema utiliza modelos avançados de linguagem e tecnologias sofisticadas de busca.

Os modelos de linguagem geram resumos precisos de textos jurídicos complexos, reduzindo a necessidade de revisão manual de documentos.

Isso diminui os custos com serviços jurídicos.



O **design generativo** é um processo avançado no qual a IA explora inúmeras possibilidades de design com base em parâmetros e restrições predefinidos, antes de apresentar soluções ideais. Essa tecnologia é utilizada em arquitetura e engenharia — como no planejamento de estradas ou construção de pontes — para desenvolver projetos inovadores e funcionais. Também é aplicada para otimizar componentes automotivos e aeroespaciais, reduzindo peso e aumentando resistência.

Instituto de Pesquisa da Toyota aprimora o design de automóveis com IA



O modelo gera diversas alternativas de design que consideram requisitos estéticos, funcionais e técnicos.

Isso permite que designers avaliem e iterem rapidamente entre muitos conceitos, reduzindo o tempo de desenvolvimento e melhorando a qualidade do produto final.

Modelos de deep learning detectam padrões e relações complexas. Esses modelos alimentam carros autônomos e sistemas avançados de recomendação. Com milhares de parâmetros refinados por meio de treinamento extensivo, eles exigem grandes volumes de dados e significativo poder computacional. Devido à sua complexidade, esses modelos frequentemente funcionam como “caixas-pretas”, dificultando a interpretação de suas decisões. Essa falta de transparência levanta preocupações relacionadas à explicabilidade, tema que será abordado mais adiante ao discutirmos ética, gestão de riscos e regulamentações. Pesquisas contínuas buscam desenvolver métodos para explicar decisões tomadas por IA, especialmente em áreas como administração pública, saúde e finanças.

A **aprendizagem por reforço** treina modelos para “compreender” ambientes complexos, como mercados, sistemas de produção ou redes logísticas. Esses modelos melhoram por meio de simulações, aprendendo por tentativa e erro. Devido à sua complexidade e ao nível de especialização exigido, a aprendizagem por reforço é aplicada por pesquisadores e engenheiros principalmente a problemas particularmente desafiadores.

Agentes autônomos tomam decisões e executam ações sem intervenção humana. Eles operam em ambientes dinâmicos e complexos, como negociações automatizadas de compras ou robôs industriais que atuam em condições perigosas. Agentes autônomos podem gerenciar logística, controlar linhas de produção ou realizar manutenção em ambientes industriais. Modelos avançados de linguagem e IA generativa permitem que esses agentes atuem em domínios onde dados não estruturados antes representavam um obstáculo.

A AT&T desenvolveu assistentes autônomos de atendimento ao cliente baseados em IA

Diferentemente de chatbots tradicionais, que geralmente se limitam a respostas pré-programadas e diálogos simples, esses assistentes autônomos utilizam algoritmos avançados de IA para compreender e responder a solicitações complexas de clientes em tempo real.



Eles podem lidar com uma ampla variedade de demandas, desde suporte técnico até questões de faturamento, sem intervenção humana.

Isso resulta em operações mais eficientes, maior satisfação dos clientes e a capacidade de atender um número maior de usuários simultaneamente.

Planejamento urbano aprimorado

A [Bedrock](#) e a [INRIX](#) desenvolveram a solução Bedrock Compass, que cria simulações detalhadas de tráfego em ambientes urbanos.

Os modelos de IA são treinados com grandes volumes de dados relacionados ao fluxo de tráfego, estacionamento e movimentação de pedestres.

Urbanistas podem gerar e avaliar rapidamente múltiplas opções, ajudando a identificar as soluções mais eficientes e sustentáveis para o desenvolvimento futuro.

A **IA causal** busca identificar causas subjacentes, enquanto modelos tradicionais apenas identificam correlações. Existe correlação, por exemplo, entre o consumo de sorvetes e incidentes de afogamento, mas isso não explica a causa de nenhum dos dois (clima quente é uma explicação mais plausível). Na pesquisa médica, uma compreensão mais profunda das causas das doenças pode levar a tratamentos mais eficazes. A IA causal também pode aprimorar a gestão financeira ao revelar explicações mais profundas para fenômenos econômicos.

A **simulação de sistemas complexos** utiliza IA para prever resultados em cenários nos quais experimentos no mundo real seriam arriscados ou excessivamente caros.

Por exemplo, esse tipo de IA pode simular reações químicas no desenvolvimento de medicamentos para identificar candidatos promissores antes de testes laboratoriais. No planejamento urbano, a IA baseada em simulação pode prever os efeitos de novas infraestruturas antes da implementação. Além disso, a IA é usada para simular impactos das mudanças climáticas, auxiliando na avaliação das consequências ambientais de longo prazo de diferentes políticas públicas. A tecnologia também permite testar modelos econômicos para compreender os efeitos de mudanças nas tendências de mercado.

Quer ver mais exemplos de como a IA cria

Exemplos de uso de IA nos setores público e privado na UE:

[AI Watch – Observatório Europeu de Inteligência Artificial](#)

Exemplos de IA da Gartner (serviço pago): [Casos de uso de IA e IA generativa](#)



Como sua organização pode criar valor a partir da IA?



A IA é complexa e deve ser alimentada com os dados da empresa para revelar todo o seu potencial. Isso requer que a organização tenha uma governança de dados adequada em vigor. Os dados devem ser acessíveis, bem documentados e de alta qualidade — o que não é um desafio pequeno! Para ter sucesso, a sua empresa deve primeiro explorar, desenvolver, testar e aprender de forma sistemática. O próximo passo é profissionalizar e escalar as iniciativas de IA, seguindo um plano ágil e de longo prazo: um roadmap para a IA.

Muitas organizações têm dificuldade em extrair valor da IA. Elas veem exemplos de outras empresas que obtêm sucesso, mas ficam presas na *lab illusion*. Muitas experiências permanecem presas na fase de teste ou não conseguem gerar benefícios duradouros e em grande escala.

Para evitar a ilusão do laboratório, é preciso reconhecer que a IA não é uma ferramenta mágica que resolverá todos os problemas simplesmente ao ser adicionada aos produtos e processos existentes. Não se pode confiar em experiências isoladas e esperar avanços. Em vez disso, é preciso trabalhar de forma sistemática, explorar as áreas certas e iterar rapidamente através do desenvolvimento e teste antes de passar para a escalabilidade e profissionalização. Uma abordagem estruturada torna mais provável evitar erros dispendiosos e encontrar as áreas certas onde a IA pode criar valor real.

A Lab Illusion (ilusão do laboratório)



A Lab Illusion ocorre quando uma empresa alcança sucesso com um protótipo de IA, mas não consegue replicar os mesmos resultados em produção.

Algumas organizações veem suas soluções falharem imediatamente, mas, mais frequentemente, a qualidade diminui após alguns meses ou anos em produção, ou os custos operacionais e de manutenção tornam-se mais altos do que o esperado.

Isso pode ocorrer devido à má integração com sistemas existentes, à qualidade inadequada dos dados ou à falta da expertise necessária para escalar a solução.

Como resultado, as empresas não conseguem obter os benefícios esperados, apesar dos resultados promissores nas fases iniciais.

Dados como pré-requisito para a IA

Os dados estão no centro de qualquer solução de inteligência artificial. Para que algoritmos gerem insights valiosos ou automatizem tarefas complexas, eles precisam ser treinados com dados que reflitam a situação real do negócio. Os dados devem ser acessíveis, de alta qualidade e bem documentados. **Empresas que têm controle sobre seus dados estão muito mais bem posicionadas para criar valor com a IA.**



Em 2012, iniciou-se uma nova onda de avanços em IA, impulsionada por três tendências tecnológicas: avanços em modelos de deep learning para reconhecimento de padrões, uma explosão no poder computacional prontamente disponível na nuvem e o surgimento de bibliotecas de machine learning acessíveis. Esses desenvolvimentos tornaram possível construir modelos avançados de forma mais rápida e com maior precisão do que antes. No entanto, muitas organizações logo perceberam que não dispunham de dados suficientes para liberar o potencial da IA. Não bastava ter algoritmos poderosos e recursos computacionais — era necessário dispor de dados relevantes para suas necessidades específicas.

No final de 2022, surgiu uma nova onda de entusiasmo em torno da IA, pois modelos pré-treinados prontamente disponíveis reduziram a quantidade de dados necessária para utilizar a IA de forma eficaz. Esses modelos haviam sido treinados com conjuntos de dados massivos, o que lhes permitiu desenvolver conhecimentos fundamentais, como a compreensão da linguagem ou o reconhecimento de objetos em imagens. Como resultado, as empresas passaram a conseguir explorar a IA utilizando apenas pequenas quantidades de seus próprios dados. Isso facilitou o início do uso da IA, especialmente para empresas menores ou organizações que não dispõem de grandes volumes de dados históricos.

A vantagem competitiva frequentemente decorre daquilo que torna uma empresa única, seja conhecimento especializado, produtos proprietários ou a capacidade de adotar novas tecnologias. É possível gerar valor com a IA por meio da implementação e combinação de soluções prontas para uso (*off-the-shell*). A disponibilidade dos chamados modelos *zero-shot* — modelos que não exigem treinamento específico antes do uso — aumentou significativamente. Exemplos incluem o ChatGPT e o Microsoft Copilot, que utilizam modelos pré-treinados nos quais os usuários simplesmente fornecem entradas por meio de prompts ou linguagem natural, por vezes combinadas com técnicas avançadas de busca, como a Geração Aumentada por Recuperação (Retrieval-Augmented Generation – RAG). Isso torna as ferramentas baseadas em IA mais acessíveis, permitindo que os usuários gerem valor rapidamente.

Ao mesmo tempo, organizações com acesso a dados ricos e específicos do negócio podem ajustar e adaptar modelos com maior precisão. Isso representa uma vantagem competitiva fundamental e duradoura. A IA gera mais valor quando você aproveita o poder dos dados da sua organização. Ao construir soluções com base em algo único, você cria diferenciação em relação aos concorrentes.

Para alcançar isso, são essenciais processos e infraestrutura robustos de gestão de dados. Dados acessíveis e de alta qualidade permitem a melhoria contínua dos modelos e a adaptação a necessidades em constante mudança. Além disso, as organizações devem lidar com preocupações relacionadas à privacidade e cumprir o GDPR. Simplesmente possuir dados não é suficiente — eles devem ser acessíveis, bem documentados e utilizados de forma lícita e ética. Retomaremos esses temas em capítulos posteriores.

Defina o nível correto de ambição

O primeiro passo que sua organização deve dar para criar valor com IA é estabelecer um nível de ambição claro e realista, alinhado às competências e à capacidade da organização.

O gráfico abaixo apresenta algumas perguntas-chave a serem consideradas:

Áreas de valor

A organização possui produtos, processos ou ativos que podem ser significativamente aprimorados por meio de IA? Em caso afirmativo, quais? Busque altos volumes, execução frequente ou alto comprometimento de capital, garantindo ao mesmo tempo a existência de dados digitais estruturados.

Disposição para investir e apetite ao risco

- Quais investimentos sua organização está disposta a realizar em termos de capital, competências e priorização de outros recursos?
- Sua organização está disposta a testar aplicações de IA mesmo havendo um risco significativo de que os resultados não se concretizem?

Restrições operacionais

- Existem limitações no ambiente operacional da sua empresa que influenciam áreas de valor que podem ser exploradas? Isso inclui, por exemplo, regulamentações específicas do seu setor.

Maturidade

- Sua organização possui a infraestrutura tecnológica necessária para implementar soluções de IA?
- Existem processos estabelecidos que possam ser ampliados para apoiar o uso e a integração eficientes da IA nas operações?
- A organização possui competências internas suficientes ou acesso a especialistas em IA?
- Caso contrário, essas competências podem ser desenvolvidas internamente ou adquiridas externamente?

Dados

- Sua organização possui dados suficientes e de alta qualidade relacionados às áreas de valor?
- Existem dados livres de restrições legais ou outras limitações? Os dados são tecnicamente acessíveis?
- Os dados estão bem documentados e são facilmente acessíveis para quem deseja experimentar?

Algumas empresas começam de forma cautelosa, otimizando processos internos específicos. Outras têm capacidade e disposição para “apostar tudo” em uma abordagem *AI-first*, colocando a IA no centro de seus produtos e processos produtivos.

Organizações com alto nível de ambição em IA devem estar preparadas para investir em uma infraestrutura abrangente de IA, equipes dedicadas, plataformas avançadas de dados e processos voltados à inovação contínua e à melhoria constante.

Escolha as áreas de valor certas

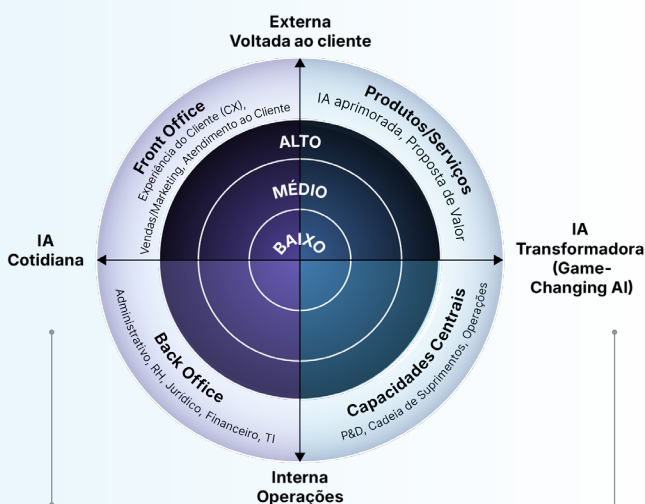
Depois de definir o nível de ambição, você deve identificar de forma sistemática as áreas de valor que se alinham aos seus objetivos e capacidades. Comece explorando aplicações de IA tanto transformadoras quanto disruptivas:

- **Aplicações transformadoras** aprimoram e otimizam estruturas, processos ou produtos existentes. O objetivo é aumentar a eficiência e reduzir custos.
- **Aplicações disruptivas** introduzem mudanças fundamentais ao possibilitar produtos, mercados ou formas de operação totalmente novos. Essas inovações podem desafiar ou substituir modelos de negócio existentes ou transformar setores inteiros.

O Radar de Oportunidades de IA

A **viabilidade** é uma combinação de:

- Viabilidade técnica
- Prontidão interna
- Prontidão externa



A **IA Cotidiana** consiste em aplicações transformadoras, enquanto a **IA Transformadora (Game-Changing AI)** consiste em aplicações disruptivas.

Outra distinção importante é se a IA é utilizada internamente para melhorar processos de negócio ou externamente para criar novos produtos e serviços:

- **Aplicações internas** focam na eficiência operacional, redução de custos ou melhoria da qualidade de processos existentes.
- **Aplicações externas** buscam utilizar a IA para desenvolver novas ofertas que proporcionem vantagem competitiva.

Por exemplo, uma aplicação transformadora externa de IA pode ser o desenvolvimento de sistemas de recomendação personalizados em uma plataforma de e-commerce já existente. Isso influencia a forma como os produtos são apresentados aos clientes, permanecendo dentro de um modelo de negócio estabelecido.

Uma aplicação disruptiva interna de IA pode ser a automação completa de fluxos de trabalho por meio de inovações em logística e produção, alterando radicalmente a gestão de recursos. Nesse caso, a organização deve estar preparada para uma transformação profunda, tanto internamente quanto na colaboração com parceiros.

A empresa de pesquisa [Gartner](#) desenvolveu o **AI Opportunity Radar (Radar de Oportunidades de IA)**, que categoriza aplicações de IA com base em duas dimensões: o nível de impacto (transformador vs. disruptivo) e se a aplicação é interna ou externa. Além disso, o radar avalia a dificuldade de implementação de cada aplicação, considerando complexidade técnica, prontidão interna e maturidade de mercado.

Aplicações posicionadas no centro do círculo são mais fáceis de implementar, enquanto aquelas mais distantes são mais desafiadoras. Por exemplo, a automação de tarefas administrativas manuais, como faturamento ou elaboração de relatórios, pode ser relativamente simples, gerando benefícios como economia de tempo e redução do risco de erros. No entanto, isso oferece valor estratégico limitado, pois se concentra principalmente na otimização de processos existentes.

A personalização da experiência do cliente baseada em IA em todos os canais digitais é uma aplicação mais complexa. Ela exige grandes volumes de dados de alta qualidade, modelos avançados de IA e um profundo entendimento das necessidades dos clientes. Essas soluções podem proporcionar vantagem competitiva significativa e gerar novas fontes de receita. Ao mesmo tempo, demandam um horizonte de planejamento mais longo e recursos substanciais para ter sucesso, pois impactam múltiplos processos de negócio. A sua organização deve estar preparada para investir tempo e recursos significativos, mantendo-se comprometida mesmo diante de desafios e contratempos.

Utilizar o modelo de radar para posicionar aplicações de IA oferece uma estrutura clara para avaliar onde e como a IA cria mais valor, orientando decisões estratégicas sobre implementação.

Experimente e aprenda!

Ao esclarecer o nível de ambição e priorizar áreas de criação de valor, você estabelece o enquadramento e a direção adequados para a geração de valor com IA. Dentro desses limites, é necessário explorar, desenvolver, testar e aprender.

Tendo em mente a ilusão do laboratório — o fenômeno em que bons resultados em projetos-piloto frequentemente falham na produção — é fundamental evitar ciclos excessivamente longos de iteração. É preciso identificar complexidades inesperadas e problemas relacionados à baixa qualidade dos dados o mais cedo possível.

Isso significa testar novas abordagens de IA por meio de projetos-piloto, adotar uma mentalidade de fail fast, que permita aprendizado rápido, entregar funcionalidades em pequenos incrementos — Produtos Mínimos Viáveis (MVPs) — e automatizar todo o pipeline, do desenvolvimento à implantação.

Por fim, é essencial fechar o ciclo, garantindo que as experiências em produção retroalimentem as fases anteriores: ideia, conceito, design, desenvolvimento, testes e lançamento.



Uma forma eficaz de começar é estabelecer um centro de competência em IA como núcleo das iniciativas de IA e nomear um coordenador de IA responsável por liderar e apoiar projetos em toda a organização. Isso fornece estrutura e direção nas fases iniciais, ao mesmo tempo em que assegura o alinhamento com a estratégia geral da empresa.

Profissionalize e amplie!

Sua organização estabeleceu suas primeiras soluções baseadas em IA. Você adquiriu conhecimento sobre os pontos fortes e fracos dos diferentes tipos de IA, sobre a qualidade dos dados da organização e sobre o que é necessário para gerenciar e operar soluções de IA de forma eficaz. **Mais importante ainda, você descobriu o iceberg — tudo o que está oculto abaixo da superfície ao implementar IA em um processo de negócio e garantir sua manutenção e desenvolvimento no longo prazo.** Soluções de IA normalmente apresentam uma proporção significativamente maior de custos de ciclo de vida após a implantação em comparação com outras soluções de TI.



Para continuar evoluindo, é necessário profissionalizar e escalar:



Desenvolva um roadmap de IA – Garanta que o uso de IA esteja alinhado aos objetivos e valores da sua organização por meio de um plano estratégico ágil.



Estabeleça uma governança sólida de IA – Diante do ritmo acelerado das mudanças tecnológicas, ancore a governança de IA na alta gestão para apoiar a estratégia.



Impulsione a inovação em IA de forma sistemática – Explore, avalie e priorize oportunidades de negócio baseadas em IA por meio de processos estruturados de inovação.



Construa uma infraestrutura de IA escalável – A IA exige grandes volumes de dados e elevado poder computacional, o que demanda uma infraestrutura técnica que ofereça suporte ao treinamento, à avaliação e à implantação de modelos.



Garanta dados de alta qualidade e bem governados – Os dados devem ser de alta qualidade, bem documentados, interoperáveis e tecnicamente acessíveis. Aborde questões éticas, legais e de segurança por meio de uma governança de dados abrangente, envolvendo TI, jurídico, especialistas de domínio e áreas de negócio.



Implemente AI Ops para a gestão contínua da IA – Mantenha os modelos de IA atualizados por meio de processos sistemáticos de integração de dados, treinamento e retreinamento de modelos, implantação de modelos, avaliação de desempenho e monitoramento de segurança.



Desenvolva competências em IA em toda a organização – Recrute especialistas em IA e, ao mesmo tempo, assegure treinamento amplo em IA para os colaboradores, possivelmente por meio de um centro de competências em IA.

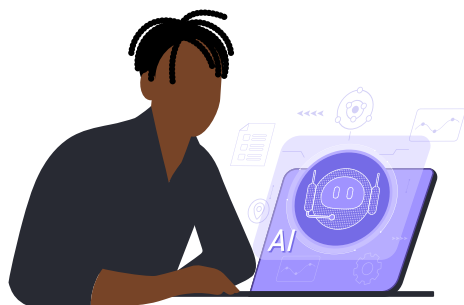
Os próximos capítulos abordarão **considerações éticas, de governança, risco, qualidade e aspectos jurídicos**.



Considerações éticas



A IA oferece oportunidades significativas, mas também apresenta desafios éticos. Sistemas de IA não são inerentemente éticos nem antiéticos; eles refletem as escolhas feitas por quem os projeta, treina e implementa. Sua organização deve garantir que a IA seja utilizada de forma responsável, transparente e justa, a fim de promover confiança, conformidade e criação de valor sustentável.

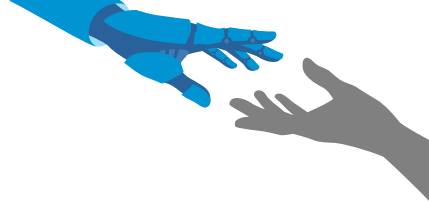


A ética trata de compreender e lidar com as implicações morais de nossas ações. Ao implementar IA em sua organização, é necessário avaliar as consequências éticas: os sistemas de IA estão sendo utilizados de acordo com os valores centrais e princípios morais da organização?

Mas de quais valores e princípios estamos falando? Eles incluem os valores de todas as pessoas que trabalham na organização e daquelas que são afetadas por ela. Estendem-se também à sociedade, ao ecossistema, ao setor ou ao mercado em que a organização atua. Alguns princípios éticos estão explicitamente incorporados em leis, regulamentos e requisitos concretos que devem ser cumpridos; outros funcionam como objetivos subjacentes refletidos em normas regulatórias, padrões do setor ou convenções não escritas.

Este capítulo oferece uma visão geral dos desafios éticos mais relevantes relacionados à IA. Ele ajuda a identificar e gerenciar sistematicamente preocupações éticas, permitindo que a IA seja utilizada para criar valor em alinhamento com os valores da organização e com o respeito aos direitos e à integridade individuais.

O campo da ética em IA evolui rapidamente, e novas questões e desafios continuarão surgindo. É essencial acompanhar esses desenvolvimentos e atualizar as diretrizes éticas da organização à medida que novos conhecimentos se tornem disponíveis.



IA centrada no ser humano e *accountability*

Se houver um princípio ético a ser priorizado — e continuamente revisitado — é o uso da IA de forma centrada no ser humano. A IA deve apoiar, e não substituir, o julgamento humano e a tomada de decisões. Ferramentas de IA devem ampliar o conhecimento e a expertise humanos. Esse princípio é particularmente crítico em processos decisórios complexos. Os seres humanos devem sempre ter a palavra final em decisões críticas, especialmente quando a IA influencia indivíduos de maneiras que podem ter consequências sociais ou econômicas significativas.

A *accountability* exige a definição clara de quem é responsável pelo uso da IA e quem toma decisões com base nos sistemas de IA. A sua organização deve estabelecer papéis bem definidos e garantir que profissionais qualificados validem e aproveem soluções de IA antes de sua implantação. Também deve ficar claro quem assume a responsabilidade legal caso algo dê errado. Mecanismos de monitoramento contínuo devem estar em vigor para assegurar que os sistemas de IA funcionem conforme o esperado e sigam as diretrizes éticas estabelecidas. À medida que a regulamentação relacionada à IA evolui, essa exigência se tornará ainda mais relevante.

Transparência e explicabilidade

Para construir confiança nos sistemas de IA, todas as partes interessadas — incluindo colaboradores, clientes e órgãos reguladores — precisam compreender como a IA é utilizada na organização e quais decisões ela apoia. Isso é conhecido como transparência e se aplica tanto ao desenvolvimento quanto à operação das soluções de IA. Transparência também significa ser aberto quanto às medidas adotadas para garantir que decisões baseadas em IA sejam confiáveis. Se a organização não conseguir alcançar transparência suficiente sobre como e quando a IA é utilizada, deve considerar ferramentas ou métodos alternativos. Para alcançar a transparência, você deve ser capaz de explicar como os algoritmos chegam às suas conclusões.

Explicabilidade significa que você deve ser capaz de explicar os resultados gerados pela IA de uma forma que os humanos possam compreender. Por exemplo, se a IA for usada para otimizar a experiência do cliente, deve ser possível explicar por que determinados segmentos de clientes recebem recomendações ou soluções específicas.

Se um algoritmo sugere uma determinada estratégia ou decisão, deve estar claro quais informações foram utilizadas e como essa conclusão foi alcançada. No entanto, se a explicação for excessivamente complexa para ser compreendida, ela perde seu propósito. Mesmo que cada etapa do cálculo seja simples, isso não garante compreensão se houver etapas demais. Uma explicação longa ou intrincada pode ser tão opaca quanto uma “caixa-preta”.

A explicabilidade permite que decisores humanos avaliem recomendações geradas por IA e as substituam quando necessário. Ela deve combinar lógica, ciência cognitiva e compreensão de psicologia para garantir que a IA forneça explicações tecnicamente corretas e, ao mesmo tempo, compreensíveis. Em última análise, transparência e explicabilidade são fundamentais para construir confiança entre aqueles que desenvolvem, utilizam ou são impactados por sistemas de IA.

Equidade e vieses

A equidade é uma das questões éticas mais fundamentais relacionadas à IA. Sistemas de IA podem, de forma não intencional, reforçar vieses sociais existentes, pois frequentemente são treinados com dados que refletem esses vieses. Por exemplo, um sistema de IA que avalia pedidos de crédito pode discriminar com base em gênero ou etnia se os dados de treinamento contiverem tais distorções.

Portanto, é necessário avaliar e ajustar os sistemas de IA para remover vieses indesejados. Observe o termo “indesejados”: todos os conjuntos de dados contêm vieses — esses padrões permitem que os algoritmos funcionem ao fornecer sinais significativos. O desafio é utilizar esses sinais de forma construtiva, evitando que resultem em decisões injustas. Alcançar isso requer definir critérios de equidade, utilizar conjuntos de dados diversos, ajustar algoritmos durante a implantação e estabelecer mecanismos para detectar e corrigir resultados enviesados.

Padrões obscuros e manipulação

Padrões obscuros manipulam usuários para que façam escolhas que talvez não fizessem se tivessem informações completas. A IA pode amplificar essas práticas quando utilizada para maximizar ganhos de curto prazo em detrimento dos interesses de longo prazo dos usuários. Por exemplo, a precificação dinâmica baseada em IA pode explorar vieses psicológicos para induzir consumidores a pagar mais.

Sua organização deve assegurar que soluções de IA não manipulem nem explorem usuários, especialmente grupos vulneráveis. Priorizar transparência e explicabilidade ajuda a mitigar o risco de padrões obscuros.

Padrões obscuros são ilegais de acordo com o AI Act da União Europeia e o Digital Services Act (DSA).



Dependência da IA

A IA pode se tornar um passivo se for integrada a processos centrais de negócio sem uma avaliação de riscos holística que considere perspectivas de longo prazo. Embora a IA seja uma ferramenta valiosa — ou talvez justamente por isso — é essencial garantir que a expertise humana e o pensamento crítico permaneçam centrais. A dependência excessiva de IA, especialmente em decisões críticas, pode enfraquecer competências organizacionais e aumentar a dependência de fornecedores de tecnologia. Por exemplo, se uma empresa automatiza o atendimento ao cliente com IA, deve garantir que a interação humana continue disponível para casos complexos ou sensíveis.

Há também o risco de a IA se tornar tão integrada às operações essenciais que a organização não consiga funcionar sem ela. Caso os sistemas de IA se tornem indisponíveis — por mudanças no modelo de preços do fornecedor, descontinuação do serviço, falência ou mudanças tecnológicas significativas — isso pode causar interrupções operacionais graves.

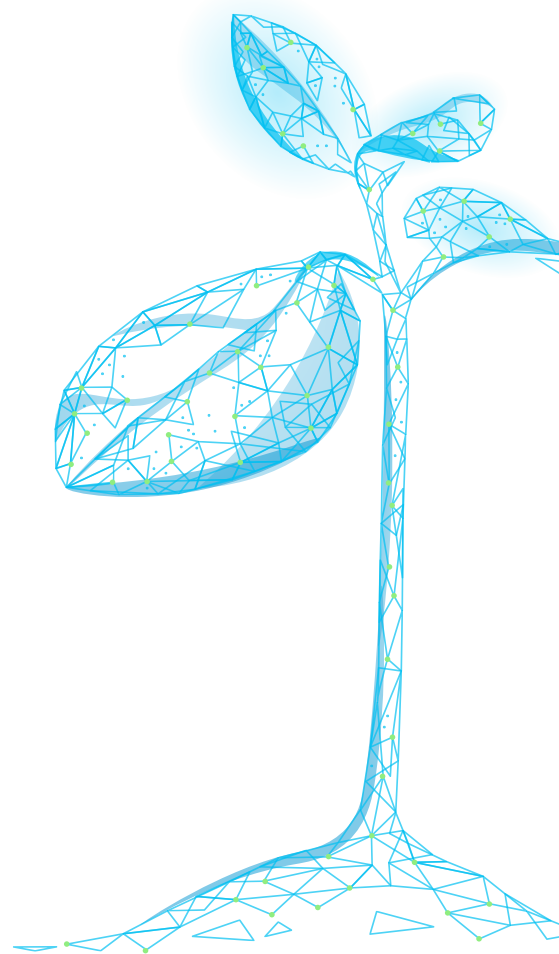
Atualizações frequentes e mudanças tecnológicas também podem exigir ajustes organizacionais significativos, aumentando custos e demandas por recursos. Para mitigar esse risco, é necessário avaliar a estabilidade de longo prazo de toda a cadeia tecnológica e desenvolver planos de contingência com soluções alternativas.

Impacto ambiental e climático

O treinamento de grandes modelos de IA requer quantidades significativas de energia, aumentando a pegada de carbono da sua organização. Isso é especialmente relevante para *machine learning* e *deep learning*, nos quais grandes volumes de dados demandam elevado poder computacional.

Para reduzir o impacto ambiental da IA, devem ser utilizados algoritmos e infraestruturas energeticamente eficientes. A otimização de modelos para consumir menos energia e o uso de provedores de nuvem comprometidos com fontes renováveis podem reduzir emissões. Essas iniciativas devem estar alinhadas a uma estratégia mais ampla de digitalização sustentável, equilibrando avanço tecnológico e responsabilidade ambiental.

Embora o maior impacto ambiental dos modelos de IA ocorra durante o desenvolvimento, treinamento e início da produção, a pegada continua ao longo de todo o ciclo de vida. A atualização e a ampliação dos modelos, à medida que os conjuntos de dados crescem, frequentemente exigem mais energia. O planejamento de longo prazo do consumo energético pode ajudar a reduzir a pegada ambiental total da IA.



Hierarquias intencionais e dilemas éticos

A adoção da IA frequentemente apresenta dilemas éticos, exigindo um equilíbrio entre oportunidades tecnológicas e considerações éticas. Uma hierarquia intencional é um framework valioso para avaliar esses desafios, posicionando decisões éticas em um espectro — desde a conformidade regulatória básica até compromissos mais profundos com valores e princípios éticos.

No nível mais baixo, as organizações concentram-se em evitar erros, cumprir leis e minimizar riscos reputacionais. Em níveis mais elevados, as decisões refletem um compromisso consciente com valores e responsabilidade social. A aplicação de hierarquias intencionais ajuda sua organização a avaliar desafios éticos sob múltiplas perspectivas e a identificar soluções sustentáveis de longo prazo. Uma abordagem baseada apenas em conformidade frequentemente leva a uma mentalidade reativa, tratando a ética como uma obrigação, e não como uma oportunidade. Em contraste, o trabalho ético sistemático fortalece a cultura interna e melhora a reputação externa.

Ao enfrentar dilemas que envolvem valores conflitantes, diferentes abordagens podem ajudar a encontrar soluções. Um exemplo típico é a tensão entre a privacidade e a necessidade de grandes conjuntos de dados para treinar modelos de IA. **Uma hierarquia intencional pode orientar a tomada de decisão ao delinear diferentes níveis de resposta:**



Priorização – A solução mais simples, mas frequentemente a menos ideal, consiste em favorecer um valor em detrimento do outro, por exemplo, priorizando a privacidade em detrimento da disponibilidade de dados, ou vice-versa.



Compromisso – Uma abordagem intermediária busca equilibrar valores conflitantes, embora possa resultar em desfechos subótimos que não satisfazem plenamente nenhuma das partes.



Reconciliação – Uma abordagem mais ambiciosa procura reduzir ou eliminar a contradição entre valores. Por exemplo, por meio do desenvolvimento de tecnologias que minimizem a dependência de dados pessoalmente identificáveis.



Benefício mútuo – O resultado ideal ocorre quando ambos os lados se beneficiam. No caso da privacidade e do acesso a dados, dados sintéticos podem viabilizar o treinamento de IA ao mesmo tempo em que protegem a privacidade.

Nem todos os dilemas podem ser totalmente resolvidos, mas uma abordagem estruturada para a tomada de decisões éticas e o uso consciente de hierarquias intencionais podem ajudar sua organização a desenvolver soluções eticamente sólidas e tecnologicamente robustas. Isso, por sua vez, permite manter a reputação da organização enquanto se aproveita todo o potencial da inteligência artificial.



Governança, qualidade e risco

A IA impacta a qualidade e o risco de novas maneiras. Sua organização deve adaptar seus processos de governança para considerar as características específicas da IA em comparação com tecnologias tradicionais.

Neste capítulo, descrevemos como a IA afeta qualidade e risco e apresentamos orientações sobre o que considerar ao planejar a implementação de IA em sua organização. Para estruturar essa discussão, ela foi integrada a um framework de GRC (Governança, Gestão de Riscos e Conformidade), abordando especificamente como a IA impacta os processos de governança, a gestão de riscos e a conformidade com leis, regulamentos e políticas.

Governança

A IA desafia os processos tradicionais de governança de diversas formas. Um dos principais desafios é que muitos sistemas de IA operam como “caixas-pretas”, dificultando explicar como os algoritmos chegam às suas decisões. Isso frequentemente gera incertezas quanto à responsabilização e ao suporte à tomada de decisões quando soluções de IA são utilizadas em decisões críticas de negócio.

Governar a IA de forma eficaz exige uma abordagem estruturada que esclareça responsabilidades, estabeleça mecanismos de supervisão e assegure o alinhamento com objetivos éticos e organizacionais. Isso começa com uma estratégia de governança que defina quem é responsável pelos sistemas de IA, como eles são monitorados e quais processos garantem qualidade, conformidade e melhoria contínua. Essa estratégia deve integrar a governança de IA às estruturas mais amplas e aos processos decisórios da organização, garantindo que as soluções de IA sejam desenvolvidas, implementadas e utilizadas de forma responsável e transparente.

Accountability e transparência



Se um banco utiliza IA para avaliação de crédito, deve ficar claramente indicado que a IA está sendo utilizada e quem é responsável por monitorar o desempenho do algoritmo, lidar com erros e garantir que as decisões estejam alinhadas às diretrizes estabelecidas.

Caso o sistema de IA tome uma decisão injusta ou discriminatória, devem existir mecanismos para detectar e corrigir esse problema.

Diretrizes éticas e vieses



Um modelo de recrutamento pode favorecer indiretamente um determinado grupo demográfico devido a dados

historicamente desequilibrados, mesmo que o modelo não tenha acesso direto a dados que distinguem esses grupos. Isso é conhecido como efeito proxy.

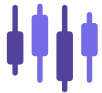
Vieses podem gerar desafios éticos, e as organizações devem monitorar esses riscos por meio de auditorias regulares para prevenir vieses ilegais ou indesejáveis.

Para implementar a estratégia de governança de IA, é necessário estabelecer estruturas específicas de governança.

Além de procedimentos claros, papéis e responsabilidades, isso pode incluir um comitê de ética em IA ou um conselho de governança responsável por supervisionar iniciativas de IA em toda a organização. Esses órgãos devem garantir que o uso da IA esteja em conformidade com políticas internas, padrões éticos e requisitos regulatórios.

A governança eficaz depende da definição clara de responsabilidades em toda a organização. Quem é responsável pela estratégia geral de IA? Quem monitora as soluções tecnológicas? Quem garante que as soluções de IA estejam alinhadas aos objetivos éticos e estratégicos da organização? Uma divisão clara de responsabilidades assegura que todas as partes relevantes — equipes técnicas, liderança e áreas de negócio — compreendam seus papéis na governança dos sistemas de IA.

Monitoramento contínuo e auditorias



Uma seguradora que utiliza IA para avaliação de riscos pode perceber que o algoritmo se torna menos preciso ao longo do tempo, à medida que condições de mercado ou comportamentos dos clientes se afastam dos dados nos quais o modelo foi treinado.

Portanto, a empresa deve dispor de sistemas para auditorias regulares e ajustes nos modelos, a fim de manter alto desempenho.

A governança eficaz de IA inclui uma gestão de qualidade estruturada, com diretrizes e procedimentos internos claros.

Outro aspecto da gestão da qualidade em IA é o estabelecimento de métodos para validar e testar modelos de IA antes da implantação, durante atualizações e por meio de avaliações contínuas de qualidade na operação diária.

Garantir dados de treinamento de alta qualidade é essencial, tanto no desenvolvimento inicial quanto em ciclos posteriores de retreinamento. A governança de IA também deve incluir medidas para manter a qualidade dos dados de entrada utilizados em produção. As organizações podem fortalecer a governança de IA utilizando ambientes de simulação, validação cruzada e projetos-piloto para testar modelos antes da implantação em larga escala.

Gestão de risco

Diferentemente dos sistemas tradicionais de TI, soluções de IA são mais dinâmicas e frequentemente difíceis de prever, o que torna a gestão de riscos mais complexa. Esses riscos incluem ameaças tecnológicas, como ataques cibernéticos a sistemas de IA, bem como riscos de negócio e éticos decorrentes de decisões incorretas tomadas por sistemas de IA.

Antes de implantar soluções de IA em produção, as organizações devem conduzir avaliações de risco, examinando superfícies de ataque, erros algorítmicos imprevistos e questões relacionadas ao uso de dados e à tomada de decisões.

Também é necessário avaliar a robustez, ou seja, como a solução de IA lida com eventos inesperados. Isso inclui influências externas, como falhas tecnológicas ou mudanças nas condições dos dados. Uma solução de IA robusta deve ser capaz de se adaptar a essas situações ou, no mínimo, garantir um desligamento controlado de funções em eventos críticos, como desastres naturais ou incêndios.

Você também deve estar ciente de que, como Inga Strümke aponta em seu livro *Maskiner som tenker* (Máquinas Pensantes), os fornecedores de soluções de IA podem inserir um número ilimitado de *backdoors* que os clientes não conseguem detectar. Portanto, você deve avaliar cuidadosamente os riscos associados aos dados antes de adicionar informações confidenciais a uma solução de IA.

Os **riscos operacionais** são uma parte central dessa avaliação. Sistemas de IA podem falhar de forma inesperada, e falhas de modelo podem ter consequências graves, especialmente quando utilizados em processos críticos. Recomenda-se a criação de cenários para explorar como modelos de IA podem se comportar sob diferentes condições e planejar possíveis cenários de falha.

Risco operacional decorrente da dependência de IA



Uma solução de IA que monitora riscos financeiros em tempo real pode começar a fazer avaliações incorretas se encontrar novos padrões fora dos dados de treinamento. Se a organização não dispuser de controles manuais ou processos alternativos de tomada de decisão, isso pode gerar consequências significativas.

Para gerenciar riscos operacionais no uso da IA, **você deve implementar mecanismos de controle para detectar erros e medidas de contingência** — como redundância ou procedimentos alternativos — garantindo que os processos de negócio não sejam interrompidos.

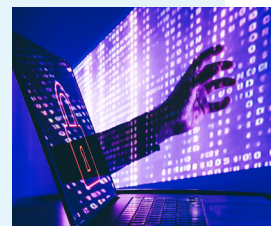
Primeiramente, é necessário avaliar os riscos associados ao modelo de IA, incluindo a segurança dos dados de treinamento e a resiliência contra ataques como inversão de modelo e envenenamento de dados. Isso exige uma compreensão sólida do funcionamento dos modelos de IA e a capacidade de identificar vulnerabilidades potenciais. Além disso, **é essencial monitorar continuamente o desempenho do modelo para manter sua funcionalidade, mesmo à medida que novos padrões de dados ou tendências de mercado surgem.**

Para mitigar esses riscos, implemente mecanismos de controle que monitorem os sistemas de IA em tempo real e detectem desvios no desempenho do modelo ou nos dados de entrada. Tais mecanismos podem incluir alertas automatizados caso um modelo produza resultados inesperados ou irracionais. Isso reduz o risco de decisões equivocadas afetarem as operações ou a reputação da organização. O monitoramento também garante que seres humanos possam revisar decisões críticas quando necessário.

Ataques de inversão de modelo

Através de ataques de inversão de modelos, **os atacantes podem reconstruir informações confidenciais fazendo consultas a um modelo de IA treinado**. Isso é

particularmente perigoso para soluções de IA que lidam com dados pessoais, como informações de saúde ou financeiras.

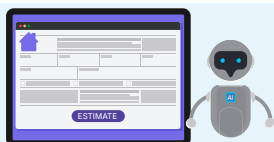


A **dependência** de fornecedores terceirizados de tecnologia de IA também introduz riscos. Ao utilizar serviços ou modelos de IA externos, as empresas devem avaliar a segurança, a confiabilidade e a conformidade desses fornecedores com as regulamentações aplicáveis. Avaliações criteriosas de fornecedores terceiros e acordos claros que protejam os interesses e os dados da organização são essenciais.

As organizações devem estabelecer processos de monitoramento específicos para fornecedores a fim de lidar com esses desafios, acompanhar o desempenho de modelos de IA externos e garantir o alinhamento com os requisitos operacionais. Isso ajuda a detectar possíveis falhas precocemente e a mitigar a dependência de fornecedores terceirizados sem salvaguardas adequadas.

Os **riscos jurídicos** também devem ser considerados. O uso extensivo e irresponsável da IA pode levar à violação de leis e regulamentos, como infrações à legislação de proteção de dados e privacidade, violação de direitos de propriedade intelectual ou discriminação. Além disso, as regulamentações sobre IA exigem cada vez mais que as empresas avaliem, gerenciem e mitiguem de forma sistemática os riscos relacionados à tecnologia. Portanto, é necessário garantir que seus sistemas de IA estejam em conformidade com as leis aplicáveis e que existam procedimentos estabelecidos para lidar com possíveis desafios jurídicos. Abordaremos esse tema com mais detalhes em um capítulo posterior.

Sistema automatizado de compra de imóveis da Zillow



[A Zillow desenvolveu um sistema automatizado para a compra de casas com base no seu modelo Zestimate, que utilizava IA para estimar o valor dos imóveis.](#)

Quando a pandemia da COVID-19 causou flutuações significativas no mercado imobiliário, ocorreu um evento imprevisível — algo para o qual o modelo não estava preparado. O sistema não possuía mecanismos para detectar anomalias, fazendo com que a Zillow continuasse a comprar casas a preços inflacionados. Isso resultou em perdas financeiras substanciais e, por fim, levou à decisão de descontinuar o programa.



Além dos controles técnicos, as organizações devem desenvolver um plano de contingência para gerenciar riscos operacionais associados à dependência de IA. Esse plano pode incluir o estabelecimento de procedimentos manuais e sistemas redundantes que assumam as operações caso a solução de IA falhe, como a implementação de processos alternativos de tomada de decisão quando o modelo encontrar dados imprevistos. As organizações devem estar preparadas para que modelos de IA percam precisão ao longo do tempo e exijam atualizações frequentes, especialmente em ambientes dinâmicos, como a previsão de comportamento do usuário ou de tendências de mercado.

Conforme mencionado anteriormente, também é crucial abordar riscos relacionados à qualidade dos dados. Sistemas de IA dependem de grandes volumes de dados para funcionar de forma eficaz, e dados de baixa qualidade podem levar a resultados imprecisos ou enviesados. As organizações devem implementar práticas eficazes de gestão de dados para garantir que os dados de treinamento sejam representativos, precisos e livres de vieses. Auditorias regulares de dados e modelos ajudam a manter alta qualidade e confiabilidade nos sistemas de IA.

Sistemas de IA também podem introduzir riscos reputacionais significativos. Decisões incorretas ou discriminatórias tomadas por um modelo de IA podem rapidamente atrair atenção negativa da mídia e prejudicar a confiança de clientes e parceiros. Portanto, o risco reputacional deve ser integrado à estratégia geral de gestão de riscos da organização. Isso inclui estratégias claras de comunicação para responder a eventuais erros ou resultados controversos gerados por sistemas de IA.

Resultados algorítmicos imprevisíveis e risco de reputação

Sistemas de IA são complexos, o que pode levar a situações em que algoritmos tomam decisões que parecem imprevisíveis ou irrazoáveis para os usuários finais. Mesmo que essas decisões sejam baseadas em padrões presentes nos dados, tais resultados podem representar um risco reputacional para a organização, especialmente se forem percebidos como discriminatórios.

Para lidar com isso, é necessário implementar testes automatizados extensivos e salvaguardas — *guardrails* — para detectar e corrigir situações anômalas.

Compliance

A IA introduz novos desafios de conformidade à medida que as organizações adotam esses sistemas. Garantir que a IA opere dentro dos marcos legais exige uma estratégia de conformidade que integre tecnologia, governança e aspectos jurídicos.

Desenvolva procedimentos robustos para monitorar, documentar e avaliar decisões de IA e o uso de dados. Auditorias e relatórios regulares ajudam a demonstrar conformidade e a mitigar riscos legais.

A tecnologia também pode ser utilizada para fortalecer a conformidade, por exemplo, por meio de ferramentas que monitoram decisões de IA, anonimização de dados ou automação de auditorias, mantendo a supervisão sobre sistemas de IA complexos.

A colaboração com especialistas jurídicos e autoridades regulatórias ajuda as organizações a se manterem atualizadas sobre desenvolvimentos legais e fornece orientação sobre boas práticas para atender aos requisitos de conformidade. Isso pode incluir a participação em fóruns do setor, grupos de trabalho ou programas de certificação sobre o uso responsável da IA.

A conformidade não se trata apenas de evitar multas e sanções — ela também é fundamental para construir confiança com clientes, parceiros e reguladores. Regulamentações tecnológicas frequentemente se baseiam em princípios éticos fundamentais, como transparência e responsabilidade. A conformidade torna-se mais gerenciável quando está alinhada a esses princípios e sustentada por sistemas eficazes de supervisão e melhoria contínua. O objetivo deve ser garantir que a organização utilize IA de forma segura e responsável, com processos sustentáveis alinhados a valores internos e exigências externas.

Uso de dados pessoais no treinamento de IA

Se um modelo de IA for treinado com dados pessoais sem consentimento ou se esses dados não puderem ser excluídos mediante solicitação do titular, isso pode configurar violação do GDPR. Portanto, sistemas de IA devem ser desenvolvidos e implementados com mecanismos integrados que permitam aos usuários exercer seus direitos, como o direito de acesso e o direito ao esquecimento.



Para cumprir o GDPR, as organizações devem adotar processos transparentes sobre como modelos de IA tratam dados pessoais, incluindo como os dados são anonimizados e protegidos — tema que será aprofundado em capítulos posteriores.



Compreensão das obrigações legais para a utilização da IA na Europa

A regulamentação da IA, como o AI Act, sinaliza uma mudança fundamental na governança da inteligência artificial. No entanto, as organizações devem lembrar que os marcos legais existentes que regulam a implementação de IA continuam plenamente aplicáveis. Estruturas legais relacionadas à proteção de dados, administração pública, antidiscriminação, direitos do consumidor e responsabilidade civil permanecem igualmente relevantes, pois já se aplicam à IA.

Compreender a legislação de IA na Europa não é uma tarefa simples, mas é possível identificar princípios gerais comuns, apesar das diferenças entre legislações nacionais. Embora os regulamentos da União Europeia sejam implementados com variações nacionais — e apesar do Brexit e da existência de países fora da UE — a Europa compartilha uma tradição jurídica comum baseada em princípios semelhantes em diversas áreas.

Esses princípios gerais e similaridades serão explorados nos próximos capítulos deste guia. Além disso, deve-se observar que os capítulos anteriores descreveram abordagens para o uso responsável, seguro e ético da

IA que também se alinham bem com os fundamentos gerais para a implementação legal da IA na Europa.

Como ponto de partida geral, as organizações devem aderir às mesmas normas regulatórias e requisitos de conformidade que regem o trabalho manual tradicional e a TI. As leis e regulamentos existentes continuam a ser plenamente aplicáveis, mas introduzem desafios jurídicos na adaptação às capacidades tecnológicas emergentes.

Orientação do documento



Este guia aborda os marcos legais gerais da União Europeia relacionados à IA. Implementações nacionais podem variar, portanto as organizações devem consultar profissionais jurídicos qualificados e familiarizados com as regulamentações específicas aplicáveis em sua jurisdição antes de implementar e utilizar sistemas de IA. As informações fornecidas neste guia destinam-se apenas a orientação geral e não constituem aconselhamento jurídico.

Embora as aplicações possam variar, diversos marcos regulatórios merecem atenção especial devido a riscos específicos relacionados à IA. **Os direitos humanos continuam a formar a base de muitas diretrizes que regem o uso da IA, assim como em outros contextos. As leis de sigilo profissional e confidencialidade são particularmente críticas, pois sistemas de IA podem expor inadvertidamente informações sensíveis por meio de reconhecimento de padrões ou de resultados não intencionais.** No setor público, os princípios do direito administrativo que regem a tomada de decisões justas enfrentam novos desafios quando algoritmos realizam ou apoiam decisões que afetam direitos individuais. A legislação antidiscriminatória torna-se cada vez mais relevante, uma vez que sistemas de IA podem perpetuar ou amplificar vieses presentes nos dados de treinamento, potencialmente gerando impactos discriminatórios ilícitos sem justificativa transparente.



As iniciativas regulatórias digitais da UE

Nos últimos anos, a União Europeia introduziu importantes regulamentações tecnológicas, incluindo o GDPR e o AI Act, estabelecendo padrões para proteção de dados, transparência da IA e responsabilização.

Atualmente, a agenda regulatória da UE continua a evoluir, com a Comissão Europeia avançando iniciativas nas áreas de sustentabilidade, finanças, cibersegurança e regulação digital, muitas das quais se concentram no fortalecimento da governança tecnológica, da segurança e dos marcos dos mercados digitais.

É importante destacar que algumas propostas anteriores foram retiradas ou reconsideradas. A Diretiva de Responsabilidade em IA (AI Liability Directive) foi abandonada devido à “ausência de um acordo previsível” sobre a regulamentação. De forma semelhante, propostas de atualização das regras de privacidade online para serviços de mensagens ficaram estagnadas. Em vez disso, a prioridade parece ter se deslocado para a implementação das regulamentações existentes e para o refinamento de marcos mais antigos voltados a tecnologias emergentes, cibersegurança e governança da IA. As áreas de foco atuais incluem a elaboração de guias de apoio ao AI Act, a atualização do Cyber Resilience Act e a implementação de salvaguardas financeiras por meio do Digital Operational Resilience Act (DORA).

Embora o processo regulatório da UE permaneça metódico, os próximos meses trarão desenvolvimentos contínuos na governança digital, juntamente com esforços para simplificar a conformidade entre diferentes marcos regulatórios. As partes interessadas devem se preparar tanto para novos requisitos específicos por setor quanto para a implementação de legislações já adotadas, à medida que os mecanismos de fiscalização forem sendo desenvolvidos.

As regras de responsabilidade civil em toda a Europa também seguem princípios semelhantes. As empresas que utilizam IA assumem a responsabilidade primária por prevenir esses danos por meio de procedimentos abrangentes de avaliação de riscos e protocolos rigorosos de testes. No entanto, isso passará por algumas mudanças à medida que o AI Act for plenamente implementado nos países da UE, uma vez que o regulamento estabelece responsabilidades graduadas com base nos níveis de risco.

Essa mudança provavelmente significará que as empresas deverão esperar requisitos de certificação semelhantes à marcação CE antes de implantar sistemas de IA de alto risco. Esse cenário em transformação exige uma abordagem proativa tanto em relação à conformidade atual quanto à antecipação de requisitos emergentes.

Para navegar nesse ambiente em evolução, tanto no que diz respeito à responsabilidade civil quanto a outras áreas jurídicas, as empresas devem:



Integrar a supervisão jurídica ao desenvolvimento de IA desde o início.



Garantir conformidade com as regulamentações existentes, ao mesmo tempo em que se prepara para regulamentações futuras.



Estabelecer frameworks de governança para acompanhar mudanças regulatórias.



Adotar modelos de IA transparentes e explicáveis para alinhar-se a princípios de equidade e *accountability*.



Documentar avaliações de risco e estratégias de mitigação tanto para cenários de responsabilidade geral quanto de responsabilidade por produto.



Manter-se informadas sobre regulamentações específicas de setores que possam se aplicar às aplicações de IA.

Uma empresa que aborda esses desafios de forma proativa não apenas reduz riscos, como também fortalece sua posição como líder responsável e inovador em mercados impulsionados por IA.

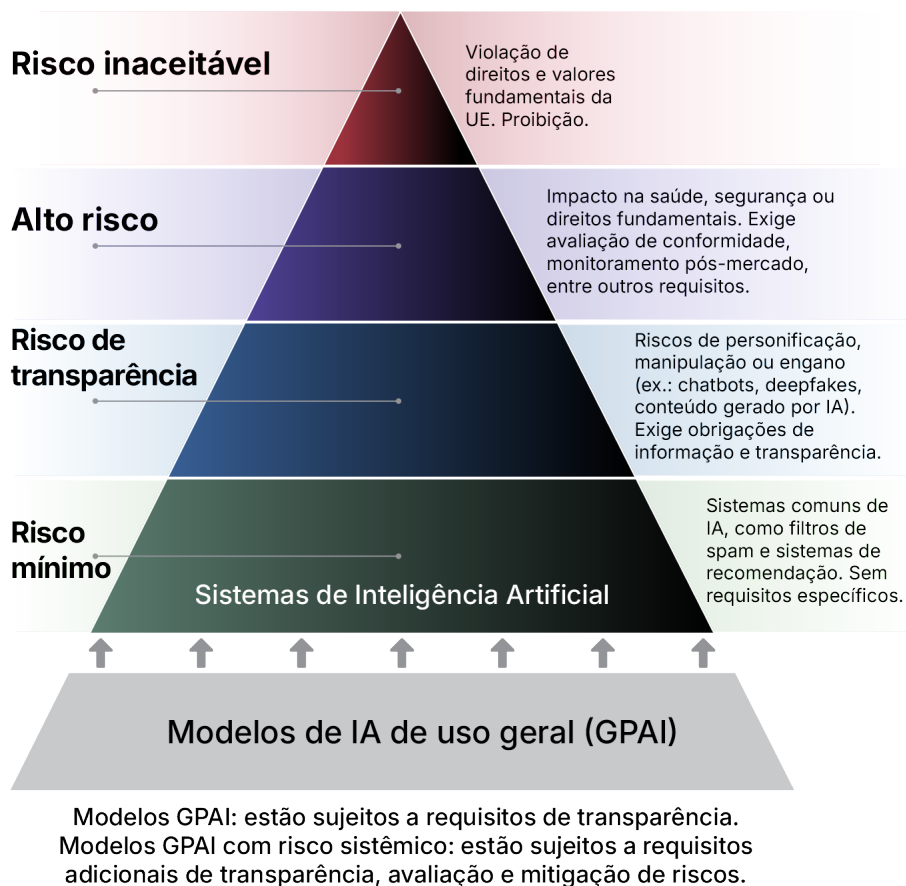


IA Act

O AI Act é o novo marco legal da União Europeia para promover o uso seguro e responsável da inteligência artificial. O regulamento busca equilibrar a necessidade de inovação com a necessidade de proteção contra usos nocivos da IA. Isso é feito por meio de duas abordagens principais: risco e papéis.

O AI Act é uma regulamentação baseada em risco. Isso significa, entre outras coisas, que as regras aplicáveis variam conforme a classificação de risco do sistema de IA.

O AI Act proíbe sistemas de IA considerados de risco inaceitável. Isso inclui, por exemplo, IA utilizada para manipular ou enganar deliberadamente pessoas, sistemas de "pontuação social" (*social scoring*) ou sistemas usados para avaliar a probabilidade de uma pessoa cometer um crime com base exclusivamente em perfilamento. A grande maioria dos sistemas de IA não será proibida pelo regulamento. Muitos sistemas apresentam risco mínimo e não possuem requisitos específicos sob o AI Act, como filtros de spam e sistemas de recomendação.



As regras aplicáveis aos sistemas de IA de alto risco são particularmente relevantes. Esses sistemas são permitidos, mas devem cumprir requisitos específicos de conformidade e segurança. As obrigações aplicáveis dependem do papel desempenhado pela organização em relação ao sistema.

O Artigo 6 do AI Act define o que constitui um sistema de alto risco. Existem duas formas principais pelas quais um sistema de IA pode ser classificado como de alto risco:

- **A primeira ocorre quando o sistema de IA é, ou está integrado a, um produto que já está sujeito à legislação europeia de segurança de produtos.** Isso se aplica a produtos nos quais a segurança é crítica, como brinquedos infantis, elevadores e equipamentos de proteção — ver [Anexo I](#) do AI Act.
- **A segunda ocorre quando o sistema de IA é utilizado para finalidades listadas no [Anexo III](#) do AI Act.** Se um sistema for utilizado para uma dessas finalidades, ele será, em regra, considerado de alto risco. O elemento comum entre esses sistemas é o fato de poderem impactar diretamente a vida e a segurança das pessoas, e de erros ou vieses poderem afetar significativamente direitos fundamentais, segurança pública ou tratamento justo.

Exemplos de sistemas de alto risco no AI Act



Biometria – Sistemas para identificação biométrica remota, categorização biométrica baseada em características sensíveis e reconhecimento de emoções.



Infraestrutura crítica – Sistemas utilizados como componentes de segurança em infraestruturas digitais críticas e no fornecimento de água, eletricidade, gás e aquecimento.



Educação – Sistemas utilizados para processos de admissão, avaliação de resultados de aprendizagem, níveis educacionais e monitoramento durante provas e exames.



Emprego e recrutamento – Sistemas utilizados para recrutamento, decisões de contratação e avaliação de desempenho e comportamento de colaboradores.



Serviços sociais – Sistemas utilizados para avaliar elegibilidade a serviços públicos, solvência creditícia e seguros de saúde.



Aplicação da lei – Sistemas utilizados para avaliação de risco criminal, detecção de mentiras e avaliação de provas em investigações.



Imigração e controle de fronteiras – Sistemas utilizados para avaliações de segurança, análise de pedidos de asilo e identificação em controles fronteiriços.



Justiça e democracia – Sistemas utilizados para processamento de processos judiciais e para influenciar resultados eleitorais e votações.

Atualmente, já existem diversos sistemas de IA de alto risco em uso. **Alguns exemplos incluem:**

Uso da IA para avaliar alunos nas escolas

Turnitin Gradescope:

Ferramenta baseada em IA para avaliar e fornecer feedback sobre trabalhos acadêmicos. O sistema utiliza machine learning para analisar respostas, detectar possíveis plágios e auxiliar na correção com base em critérios predefinidos. Embora tenha sido desenvolvido para otimizar o processo de correção, levanta questionamentos sobre justiça e precisão na avaliação automatizada de estudantes.



Uso de IA para policiamento direcionado

Palantir Gotham: A Palantir fornece uma plataforma baseada em IA utilizada por agências de segurança pública para análise preditiva de dados e inteligência. O sistema integra grandes volumes de dados de diversas fontes para identificar padrões relacionados a atividades criminosas. Embora possa aumentar a eficiência policial, o sistema tem sido alvo de críticas devido a possíveis violações de privacidade e ao risco de reforçar vieses existentes no sistema de justiça. As autoridades alfandegárias da Noruega utilizam a Palantir para identificar potenciais contrabandistas, empregando métodos que vão desde reconhecimento de placas até análise de redes sociais. Em 2016, a polícia norueguesa firmou contrato com a Palantir, mas o projeto foi interrompido em 2020 antes de sua implementação. Em ambos os casos, a Autoridade Norueguesa de Proteção de Dados expressou preocupações. De forma semelhante, a polícia alemã também enfrentou críticas pelo uso do sistema, principalmente devido ao risco de envolver pessoas inocentes em investigações.



Uso de IA como componente de segurança na gestão de infraestrutura crítica

Gestão de tráfego com IA em Verona: Na região de Porta Nuova, um importante cruzamento da cidade de Verona, está sendo testado um sistema inteligente de sensores que utiliza inteligência artificial para analisar dados de tráfego em tempo real. O sistema combina radar e câmeras para classificar veículos, medir velocidade e detectar infrações de trânsito. Os dados auxiliam a gestão do tráfego, como o ajuste de semáforos. Embora isso possa melhorar o fluxo viário e reduzir emissões, surgem preocupações relacionadas à segurança dos dados e ao possível uso indevido das informações coletadas.

Para determinar se um sistema de IA se enquadra como de alto risco, é necessário verificar se o uso pretendido corresponde a alguma das descrições do Anexo III. Contudo, mesmo que o sistema seja utilizado para uma finalidade listada no Anexo III, ele não é automaticamente classificado como de alto risco. **Existem exceções a essa regra geral. O seu sistema não será considerado de alto risco se for possível documentar que ele:**

- Executa tarefas simples e repetitivas, com margem de erro muito baixa;
- Realiza controle de qualidade de trabalho já executado por humanos;
- Identifica padrões sem substituir ou influenciar o julgamento humano;
- Apenas prepara a base para uma avaliação listada no Anexo III.

Funções dos operadores no AI Act

O AI Act atribui responsabilidades e obrigações com base no papel específico que uma organização desempenha em relação a um sistema de IA. Esses papéis — como provedor, implantador, distribuidor, entre outros — determinam quais medidas devem ser implementadas para garantir conformidade com o regulamento. Por exemplo:

- Você é considerado **provedor** se desenvolveu uma ferramenta de recrutamento baseada em IA e a colocou no mercado ou a colocou em uso sob seu próprio nome. Nesse caso, você é responsável pela classificação de risco e pela documentação técnica.
- Você é considerado **implantador** (*deployer*) se utiliza uma ferramenta de IA para analisar dados de clientes. Nesse caso, você possui obrigações específicas de supervisão, deve implementar medidas de gestão de riscos e garantir que colaboradores ou usuários finais recebam as informações necessárias sobre o sistema.

Papéis do operador definidos





Modelos gerais – GPAI

Conforme mencionado anteriormente, surgiram diversos modelos de IA capazes de executar uma ampla gama de tarefas. Esses modelos são conhecidos como IA de uso geral (GPAI). Soluções GPAI são treinadas com grandes volumes de dados diversos e podem executar múltiplas tarefas. Elas podem ser utilizadas diretamente ou integradas a outros sistemas de IA. Exemplos conhecidos incluem grandes modelos de linguagem, como o ChatGPT da OpenAI. Outros modelos GPAI podem processar imagens, áudios ou dados científicos.

O AI Act inclui um capítulo específico com regras próprias para GPAI. De acordo com o regulamento, um modelo GPAI é definido como um modelo de IA treinado com grandes volumes de dados, utilizando auto-supervisão em larga escala, capaz de desempenhar competentemente uma ampla variedade de tarefas distintas e de ser integrado a diversos sistemas ou aplicações posteriores. Modelos com pelo menos um bilhão de parâmetros, treinados com grandes conjuntos de dados, geralmente se enquadram nessa definição.

Se você for um implantador de um modelo GPAI, deverá seguir as regras gerais do AI Act conforme o uso do modelo e o nível de risco envolvido. No entanto, requisitos específicos se aplicam caso você coloque no mercado ou desenvolva um modelo GPAI.

Modelos GPAI estão sujeitos a uma abordagem baseada em risco. Modelos particularmente poderosos ou com impacto social significativo podem ser classificados como de risco sistêmico. O risco sistêmico em modelos GPAI surge quando um modelo está entre os mais avançados — por exemplo, aqueles que exigem pelo menos 10^{25} FLOPs (operações de ponto flutuante) para treinamento, um processo que atualmente custa dezenas de milhões de euros — ou quando apresenta impacto social equivalente devido à sua escalabilidade, alcance ou potencial de causar danos significativos. Esses modelos estão sujeitos a requisitos mais rigorosos, incluindo:

- **Documentar o funcionamento do modelo e suas limitações;**
- **Divulgar os dados utilizados para treinamento;**
- **Garantir conformidade com a legislação de direitos autorais.**

Até 9 de abril de 2025, o Código de Conduta Europeu para IA de Uso Geral fornecerá orientações detalhadas para auxiliar provedores de modelos GPAI a cumprir suas obrigações sob o AI Act, especialmente no que se refere a transparência, direitos autorais e mitigação de riscos.

Aprovação do IA Act

O Parlamento Europeu adotou formalmente o AI Act em meados de 2024, e o regulamento entrou em vigor em 1º de agosto de 2024. **Nos Estados-Membros da UE, suas disposições passam a ser aplicadas de forma gradual ao longo de vários anos:**

- **2 de fevereiro de 2025** – Entra em vigor a proibição de práticas de IA proibidas, incluindo social *scoring*, técnicas de manipulação, determinados sistemas de identificação biométrica e requisitos de alfabetização em IA.
- **2 de agosto de 2025** – Tornam-se aplicáveis os frameworks de governança e supervisão, incluindo a designação, pelos Estados-Membros, de Escritórios de IA, bem como as obrigações para provedores de modelos de IA de Uso Geral (GPAI) e as disposições relativas a penalidades.
- **2 de agosto de 2026** – Data principal de aplicação, quando a maior parte das disposições do AI Act entra em vigor, especialmente aquelas que regem sistemas de IA de alto risco. Até essa data, os Estados-Membros devem ter pelo menos um *sandbox* regulatório de IA em funcionamento.
- **2 de agosto de 2027** – Prazo final para a implementação completa dos requisitos aplicáveis a sistemas de IA de alto risco incorporados a produtos regulados por outros atos da UE, como dispositivos médicos, brinquedos e máquinas.

O AI Act também será incorporado ao Acordo do Espaço Econômico Europeu (EEE), garantindo sua aplicação na Noruega, Islândia e Liechtenstein. O cronograma para essa incorporação depende do processo decisório do Comitê Conjunto do EEE e da implementação nacional subsequente.

Cada país do EEE deve estabelecer as estruturas administrativas necessárias para se alinhar às disposições do AI Act. O intervalo de tempo entre a aplicação do regulamento na UE e sua incorporação ao EEE significa que a implementação nos países do EEE ocorrerá com atraso em relação ao cronograma da União Europeia.

Sandbox regulatório



Um *sandbox* regulatório é um ambiente controlado no qual empresas podem desenvolver, testar e validar sistemas inovadores de IA sob a supervisão das autoridades competentes. Essa abordagem busca fomentar a inovação ao mesmo tempo em que garante a conformidade com as leis e regulamentos aplicáveis.

De acordo com o Artigo 57 do Artificial Intelligence Act (AI Act) da União Europeia, os Estados-Membros são obrigados a estabelecer pelo menos um *sandbox* regulatório de IA, que deverá estar operacional até agosto de 2026. Esses sandboxes fornecem uma estrutura para a colaboração entre desenvolvedores de IA e reguladores, facilitando a implantação segura e ética de tecnologias de IA.

Alguns países já iniciaram programas desse tipo. **Por exemplo, a Autoridade Norueguesa de Proteção de Dados (Datatilsynet) opera um *sandbox* regulatório desde 2020, com foco em soluções de IA que aprimoram a proteção da privacidade.** Essa iniciativa oferece orientação gratuita a empresas selecionadas, promovendo o desenvolvimento de sistemas de IA responsáveis e em conformidade.

Embora iniciativas semelhantes estejam surgindo em outros Estados-Membros da UE, a implementação e o escopo dos *sandboxes* regulatórios de IA variam de país para país.

Impacto no Reino Unido e na Suíça

Após deixar a União Europeia, o Reino Unido optou por uma abordagem diferente para a regulamentação da IA. O governo britânico decidiu não introduzir uma regulamentação abrangente como o AI Act, adotando em vez disso um modelo setorial, com diretrizes específicas por domínio. No entanto, empresas britânicas que colocam sistemas de IA no mercado da UE ou utilizam sistemas de IA dentro da UE devem cumprir os requisitos do AI Act.

Além disso, em virtude do Windsor Framework, a Irlanda do Norte permanece alinhada a parte das regulamentações do mercado único europeu, o que pode resultar em uma divisão regulatória em relação à governança da IA entre a Irlanda do Norte e o restante do Reino Unido.

A Suíça, que não é membro da União Europeia nem do Espaço Econômico Europeu, não está diretamente sujeita ao AI Act. Ainda assim, empresas suíças que colocam sistemas de IA no mercado da UE devem cumprir o regulamento. Atualmente, a Suíça está avaliando sua própria abordagem regulatória para a inteligência artificial.



Privacidade e o GDPR

Quando sua empresa adota IA, é fundamental avaliar cuidadosamente se, e em que medida, o sistema processa dados pessoais. Sistemas de IA frequentemente trabalham com grandes volumes de dados, que podem conter informações sobre indivíduos. Para estar em conformidade com as regulamentações de privacidade previstas no GDPR, é necessário implementar medidas que garantam que os dados pessoais sejam tratados de forma lícita, justa e segura.

Lembre-se de que o GDPR se aplica sem exceções quando você implementa IA da mesma forma que se aplica quando não há uso de IA. É necessário realizar a mesma rotina de conformidade que em qualquer outro tratamento de dados pessoais — se não de forma ainda mais metódica. Os requisitos gerais de avaliação de riscos, de estabelecimento de uma base legal para o tratamento e de proteção dos direitos dos titulares dos dados — como acesso, retificação e eliminação — continuam plenamente aplicáveis. Considerando que o GDPR abrange uma ampla gama de medidas detalhadas de conformidade, este capítulo abordará apenas os princípios gerais do framework.



Cumprir com o GDPR pode ser desafiador ao utilizar IA. Muitas vezes, é difícil compreender plenamente como um sistema de IA funciona e quais dados estão sendo processados. Por exemplo, explicar como o sistema chega às suas decisões pode ser complexo, o que torna mais exigente o cumprimento dos deveres de transparência e o fornecimento de informações significativas sobre a lógica envolvida na tomada de decisões automatizadas. Seguir as medidas técnicas e éticas descritas nos capítulos anteriores é especialmente importante para lidar com esses desafios.

Avaliação de riscos e Avaliação do impacto à proteção de dados (DPIA)

O GDPR baseia-se nos princípios de proteção de dados desde a concepção (*data protection by design*) e por padrão (*by default*) e fundamenta muitos de seus requisitos de conformidade na possibilidade de risco. **Ao abordar esses padrões, é necessário proteger ativamente os dados pessoais ao longo de todo o seu tratamento, por meio da implementação de medidas técnicas e organizacionais que minimizem riscos à privacidade. Isso inclui a realização de avaliações de risco e a incorporação de salvaguardas de privacidade às soluções desde o início.**

Para conduzir uma avaliação de risco abrangente, você deve, por exemplo:

- **Identificar** quais dados pessoais são tratados e onde estão armazenados
- **Reconhecer** ameaças externas e internas aos dados pessoais
- **Detectar** fragilidades em seus sistemas e procedimentos
- **Avaliar** as possíveis consequências de violações ou do uso indevido dos dados

O principal exemplo de gestão de riscos no GDPR é a exigência da Avaliação de Impacto à Proteção de Dados (DPIA). Uma DPIA deve ser realizada quando o tratamento puder representar um alto risco aos direitos e às liberdades das pessoas naturais. Uma DPIA é particularmente importante se você utilizar novas tecnologias, processar dados pessoais em larga escala, monitorar sistematicamente indivíduos, combinar dados pessoais de múltiplas fontes ou

processar dados relativos a pessoas em situação de vulnerabilidade. Nesse contexto, recomendamos sempre a realização de uma DPIA ao implantar um novo serviço de IA.

Ao conduzir uma DPIA, é necessário avaliar regularmente os dados pessoais que estão sendo processados e o fluxo subsequente desses dados. Além disso, deve-se avaliar a probabilidade de ocorrência de incidentes, o impacto potencial das consequências e as salvaguardas adequadas para mitigar os riscos. Isso pode incluir criptografia, pseudonimização ou outras formas de proteger seus sistemas, como procedimentos abrangentes de treinamento de usuários.

É necessário manter uma gestão contínua de riscos e realizar uma DPIA sempre que o sistema de IA for submetido a mudanças significativas. Também é importante lembrar de envolver o Encarregado de Proteção de Dados (DPO), caso a organização possua um.

Exigência de DPIA

Observe que até mesmo ferramentas simples de IA, como copilots, exigem a realização de uma DPIA. Não é o nível de sofisticação da ferramenta que determina essa exigência, mas a forma como ela é utilizada e a extensão de seu uso. Um desafio associado às ferramentas de IA é que os fornecedores frequentemente não fornecem total transparência sobre o funcionamento das ferramentas, o que pode dificultar o cumprimento dos requisitos relativos aos direitos de acesso e eliminação de dados.



Documentação

Uma documentação adequada é crucial para a conformidade com o GDPR — se não está documentado, não aconteceu. Você deve documentar a análise de aquisição antes de obter uma ferramenta de IA, as avaliações de risco, a justificativa para a escolha de soluções específicas, o processo de implementação e modificações posteriores. Após selecionar uma solução, certifique-se de atualizar o registro de atividades de tratamento (RoPA), a política de privacidade, o registro de consentimentos e demais documentações relevantes.

Quando esses processos são documentados de forma consciente, a realização de uma DPIA torna-se muito mais simples. Considere o seguinte exemplo: ao documentar a justificativa para a implementação de uma ferramenta de IA — incluindo uma descrição do serviço ou ferramenta de IA, o que a aquisição pretende aprimorar ou tornar mais eficiente, os prós e contras da ferramenta — e ao atualizar o RoPA, você já terá concluído vários aspectos de uma DPIA.

Um processo de documentação abrangente atende a propósitos de negócio que vão além da conformidade regulatória. Integrar considerações de privacidade à documentação geral de aquisições reforça os princípios de transparência, responsabilização e justiça, com esforço adicional mínimo. Do ponto de vista da conformidade, a documentação demonstra a abordagem proativa da organização na gestão dos riscos à privacidade associados à implementação de IA.



Categorias especiais de dados pessoais

Você deve estar ciente dos requisitos legais específicos ao processar dados de saúde, etnia, opiniões políticas ou crenças religiosas — as chamadas categorias especiais de dados pessoais. Regulamentações mais rigorosas se aplicam a esses tipos de dados, tanto para a coleta quanto para o uso em sistemas de IA. Existem bases legais limitadas para o tratamento desses dados em comparação com dados pessoais comuns.

Portanto, é necessário avaliar cuidadosamente se o uso de categorias especiais de dados pessoais é necessário e proporcional para a finalidade do sistema de IA. Sempre que possível, devem ser exploradas soluções alternativas que não envolvam categorias especiais. Caso esse tratamento ainda seja necessário, é importante estabelecer mecanismos de minimização de dados, controle de acesso e revisões regulares do tratamento de dados.

É especialmente importante reconhecer que sistemas de IA podem compilar dados pessoais comuns para inferir categorias especiais de dados pessoais. Um exemplo disso ocorreu quando [pesquisadores, em colaboração com o Facebook, analisaram postagens de texto de usuários para prever depressão](#). Com base em postagens e comentários ordinários, o sistema de IA foi capaz de detectar o risco de depressão meses antes de tanto um médico quanto a própria pessoa terem consciência disso. Embora esse uso da IA possa ser benéfico para prevenção e intervenção precoce, ele também levanta preocupações significativas em relação à privacidade.



Preparação dos colaboradores

Ter medidas técnicas e jurídicas em vigor não é suficiente — **é necessário implementar ações concretas para garantir que a documentação reflita os processos e decisões reais. O treinamento eficaz dos colaboradores é essencial para assegurar a conformidade com as regulamentações de privacidade. A privacidade deve ser integrada aos programas de treinamento existentes, abordando desafios práticos relacionados à IA, como equidade e como identificar e mitigar vieses nos sistemas.**

Para garantir a conformidade contínua, a organização deve revisar e atualizar regularmente os procedimentos de privacidade como parte de seu framework de governança.

Privacidade e inovação

A implementação de novas ferramentas de IA introduz novos desafios relacionados à privacidade. A IA pode processar grandes volumes de dados de maneiras que podem ser difíceis de auditar ou interpretar — fenômeno conhecido como “caixa-preta”. Por exemplo, um desafio pode surgir quando um sistema de IA processa dados pessoais para finalidades além daquelas definidas pela base legal original. Nesses casos, pode ser necessário obter novo consentimento ou identificar uma base legal alternativa para o tratamento. No entanto, o fenômeno da caixa-preta também pode gerar outros desafios no cumprimento dos direitos dos titulares dos dados. Pode ser difícil fornecer a eles informações claras sobre como seus dados são utilizados ou cumprir a obrigação de eliminação. Esses desafios serão explorados com mais profundidade neste capítulo.

É importante lembrar que as regulamentações de privacidade existem para proteger os direitos dos indivíduos, e não para impedir a inovação razoável. Embora o uso de IA possa introduzir novos tipos de riscos à privacidade, isso não significa necessariamente que seu uso seja ilícito. Alguns riscos podem ser aceitáveis e proporcionais, desde que salvaguardas adequadas estejam em vigor para minimizá-los ao máximo possível e que os benefícios do uso da IA sejam cuidadosamente ponderados em relação aos riscos. De fato, as regulamentações de privacidade oferecem considerável flexibilidade quando compreendidas e aplicadas corretamente. Na maioria dos casos, é possível desenvolver abordagens que protejam os dados pessoais e permitam que a organização continue inovando.

IA e os princípios fundamentais do GDPR

Ao desenvolver e utilizar soluções de IA em sua organização, você deve aplicar os sete princípios fundamentais do GDPR ao longo de todo o processo.

A incorporação desses princípios às práticas de IA permite desenvolver soluções que estejam em conformidade com os requisitos regulatórios, ao mesmo tempo em que promovem a inovação responsável. Essa abordagem não apenas fortalece a proteção da privacidade — ela também constrói confiança junto aos seus clientes e à sociedade em geral.

Nas páginas a seguir, examinaremos alguns desafios comuns que podem surgir ao utilizar IA, bem como exemplos de estratégias eficazes para enfrentá-los.



Limitação da finalidade



Minimização de dados



Exatidão



Limitação do armazenamento



Licitude, lealdade e transparência



Integridade e confidencialidade



Accountability



Limitação da finalidade

Os dados pessoais devem ser coletados apenas para finalidades específicas, explícitas e legítimas e não podem ser posteriormente tratados de maneira incompatível com essas finalidades.

Desafios potenciais:

A limitação da finalidade é desafiadora no contexto da IA porque modelos de IA frequentemente exigem grandes volumes de dados coletados ao longo de longos períodos. Isso significa que os dados podem ter sido coletados em um momento em que o uso de IA não foi planejado nem comunicado aos titulares dos dados. Se as organizações posteriormente desejarem utilizar esses dados para treinar modelos de IA, isso pode entrar em conflito com o princípio da limitação da finalidade, uma vez que a finalidade original não abrange esse novo uso.

Além disso, sistemas de IA podem identificar padrões nos dados que as organizações desejam explorar para novas finalidades, o que pode ser ilícito e contradizer o princípio da limitação da finalidade.

Nossa recomendação:

Para lidar com esses desafios, sua organização deve considerar usos futuros ao selecionar a base legal para o tratamento de dados. O treinamento e o uso de IA frequentemente exigem uma base legal atualizada ou nova, o que pode envolver a obtenção de novo consentimento ou o estabelecimento de outra base legal legítima para o tratamento de dados.

Lembre-se de que o consentimento é apenas uma das possíveis bases legais. Dependendo da aplicação de IA, outras bases podem ser mais adequadas.

Ao desenvolver frameworks claros e previamente definidos para o uso de IA, a organização pode antecipar melhor e navegar de forma mais eficaz pela eventual necessidade de uma nova base legal para o tratamento.



Minimização de dados

O tratamento de dados pessoais deve ser adequado, relevante e limitado ao que é necessário em relação às finalidades para as quais é realizado, e somente quando a finalidade do tratamento não puder ser razoavelmente alcançada por outros meios.

Desafios potenciais:

A minimização de dados mostra-se particularmente difícil no contexto da IA, pois modelos de *machine learning* frequentemente exigem grandes volumes de dados para treinamento e desenvolvimento.

Determinar quais dados específicos são necessários antes de avaliar o desempenho do modelo pode ser desafiador. Como resultado, pode-se coletar mais dados do que o necessário para melhorar a precisão do modelo, o que pode não estar alinhado com o princípio da minimização de dados.

Além disso, sistemas de IA podem gerar novas necessidades de dados à medida que evoluem.

Nossa recomendação:

Comece definindo claramente a finalidade e os dados necessários para alcançá-la. O primeiro passo é eliminar dados de entrada desnecessários (*feature selection*) durante o processo de desenvolvimento. Isso geralmente é benéfico para a qualidade do modelo, a estabilidade, o tempo de resposta, os custos operacionais e o impacto ambiental.

Métodos como dados sintéticos podem reduzir a necessidade de dados pessoais em conjuntos de treinamento. Outra abordagem que pode ajudar a limitar o uso de dados pessoais é o aprendizado federado (*federated learning*), que treina modelos localmente nos dispositivos dos usuários sem exigir que os dados brutos sejam coletados em um banco de dados centralizado.

Embora dados sintéticos e aprendizado federado possam reduzir a necessidade de processar dados pessoais, eles ainda apresentam desafios em relação ao princípio da minimização de dados. Dados sintéticos frequentemente exigem um conjunto inicial de dados reais, e o aprendizado federado ainda envolve a coleta de dados, mesmo que esses dados não sejam transmitidos a terceiros.



Exatidão

Os controladores devem assegurar que os dados pessoais sejam exatos e, quando necessário, mantidos atualizados. Devem adotar todas as medidas razoáveis para eliminar ou retificar, sem demora, dados pessoais inexatos, levando em consideração as finalidades para as quais os dados são tratados.

Desafios potenciais:

Garantir a exatidão em soluções baseadas em IA pode ser complexo, pois modelos de IA aprendem a partir de dados do mundo real, que podem ser imprecisos ou desatualizados. Erros nos dados podem ser amplificados durante o processo de treinamento, levando a decisões incorretas ou a vieses nos resultados do modelo.

Isso pode resultar no tratamento e no armazenamento de dados pessoais incorretos, violando o requisito de exatidão e de manutenção de dados pessoais atualizados.

Outro desafio é que muitos modelos de IA operam como “caixas-pretas”, o que dificulta compreender como as decisões são tomadas e, conseqüentemente, torna mais difícil identificar e corrigir erros.

Nossa recomendação:

Implemente monitoramento contínuo e validação das fontes de dados e do desempenho dos modelos de IA.

Utilize algoritmos de IA explicável (XAI) que forneçam visibilidade sobre como as decisões são tomadas, facilitando a detecção e a correção de erros.

Estabeleça procedimentos robustos e monitoramento automatizado para garantir que os dados de treinamento permaneçam atualizados e reflitam com precisão as condições relevantes, ao mesmo tempo em que se avalia se os resultados do modelo atendem aos requisitos de exatidão no tratamento de dados pessoais.



Limitação do armazenamento

Os dados pessoais devem ser mantidos em forma que permita a identificação dos titulares dos dados apenas pelo tempo necessário às finalidades para as quais os dados pessoais são tratados.

Desafios potenciais:

No contexto da IA, a limitação do armazenamento vai além da simples eliminação de dados pessoais, pois também se aplica à forma como os dados de treinamento influenciam modelos totalmente treinados.

Mesmo após os dados terem sido apagados, informações sobre indivíduos incluídos no conjunto de dados de treinamento ainda podem estar indiretamente presentes no modelo. Isso cria o risco de “ataques de inversão”, nos quais atacantes conseguem reconstruir dados pessoais a partir do modelo com base em suas saídas.

Isso representa um desafio significativo para o cumprimento do direito à eliminação previsto no GDPR e do princípio da limitação do armazenamento, uma vez que pode ser difícil garantir que os dados sejam verdadeiramente “esquecidos”.

Nossa recomendação:

As organizações devem utilizar técnicas que garantam que dados pessoais individuais não possam ser identificados nem reconstruídos a partir das saídas de modelos de IA. Uma abordagem consiste em introduzir ruído controlado nos dados: variações leves e controladas nos dados utilizados pelo modelo de IA, tornando difícil ou impossível vincular a saída do modelo a um indivíduo específico. Isso ajuda a proteger os dados pessoais mesmo quando eles foram utilizados no treinamento.

No entanto, o GDPR exige que os dados sejam totalmente eliminados ou anonimizados quando não forem mais necessários para a finalidade declarada. O método acima, por si só, não é suficiente para cumprir os requisitos de eliminação do GDPR. Portanto, devem ser implementados procedimentos claros de eliminação de dados — não apenas para os dados brutos, mas também para o tratamento de dados de treinamento e das saídas dos modelos.



Licitude, lealdade e transparência

Todo tratamento de dados pessoais deve ser lícito e leal. Deve ser transparente para os indivíduos que dados pessoais a seu respeito são coletados, utilizados, consultados ou de outra forma tratados, bem como em que medida esses dados pessoais são ou serão tratados.

Desafios potenciais:

Um desafio jurídico surge quando modelos de IA identificam padrões em dados pessoais sem que o tratamento esteja amparado por uma base legal clara e explícita.

Modelos que funcionam como uma “caixa-preta” também podem dificultar a garantia de que as decisões sejam justas. Vieses nos dados de treinamento podem comprometer o princípio da lealdade, ao criar de forma não intencional resultados discriminatórios com base em gênero, etnia ou idade.

Além disso, a natureza complexa e frequentemente imprevisível dos sistemas de IA dificulta a explicação de como as decisões são tomadas. Isso pode desafiar os requisitos de transparência do GDPR, uma vez que os indivíduos têm o direito de compreender como seus dados pessoais são tratados.

Quando a IA é utilizada para tomada de decisões automatizadas com efeitos significativos sobre os indivíduos, proteções adicionais se aplicam, incluindo o direito à revisão humana.

Nossa recomendação:

Para garantir a licitude, é necessário dispor de uma base legal para todo o tratamento de dados, como consentimento ou interesse legítimo, e as organizações devem manter registros dessa base legal. Auditorias regulares e mecanismos de supervisão devem ser realizados para assegurar que o modelo permaneça justo e transparente em suas decisões.

Os sistemas de IA e seus conjuntos de dados devem ser avaliados quanto a vieses para garantir que as decisões não resultem em discriminação com base em categorias especiais de dados pessoais, como estado de saúde ou origem étnica. Devem ser utilizados métodos de teste de viés, como a verificação de resultados entre diferentes grupos demográficos, para identificar possíveis problemas de discriminação.

As organizações devem implementar modelos de IA explicável (XAI) que forneçam explicações claras sobre os processos de tomada de decisão.



Integridade e confidencialidade

Os dados pessoais devem ser tratados de forma a garantir segurança e confidencialidade adequadas, incluindo a proteção contra acesso não autorizado ou ilícito, bem como contra perda acidental, destruição ou danos, por meio da adoção de medidas técnicas ou organizacionais apropriadas.

Desafios potenciais:

A IA frequentemente processa grandes volumes de dados, o que aumenta o risco de incidentes de segurança, como ataques cibernéticos, vazamentos ou acessos não autorizados. Isso pode resultar na exposição de dados pessoais.

Se os modelos não forem corretamente projetados ou treinados com salvaguardas de anonimização, podem expor inadvertidamente dados pessoais em suas saídas. Isso cria um conflito entre a necessidade de acessibilidade dos dados para o desempenho do modelo e a exigência de proteger a confidencialidade dos indivíduos.

O uso de fornecedores terceiros para serviços de IA também introduz riscos consideráveis. A organização pode ser responsabilizada por violações de confidencialidade caso não implemente medidas de segurança adequadas. As organizações devem garantir que todos os operadores de dados estejam em conformidade com os requisitos do GDPR.

O controle de acesso pode ser desafiador quando vários departamentos ou colaboradores utilizam sistemas de IA. O acesso não autorizado pode comprometer tanto a integridade quanto a confidencialidade dos dados.

Nossa recomendação:

Para garantir a integridade e a confidencialidade em soluções de IA, sua organização deve estabelecer protocolos de segurança, como criptografia de dados, controle de acesso e monitoramento regular, a fim de reduzir o risco de acessos não autorizados e vazamentos de dados.

Priorize o treinamento de modelos de IA com dados anonimizados, sempre que possível. Implemente restrições de acesso estritamente necessárias e desenvolva salvaguardas que impeçam os modelos de revelar informações pessoais.

Ao utilizar fornecedores terceiros, estabeleça acordos seguros de tratamento de dados (DPAs) ou limite o uso de serviços que não possam garantir segurança adequada para os dados pessoais.

Desenvolva políticas internas claras de controle de acesso. Conceda aos colaboradores acesso com base no princípio do menor privilégio e assegure treinamento em privacidade e segurança de dados. Trate erros e dados corrompidos rapidamente para manter a integridade dos dados.



Accountability

O controlador deve assumir a responsabilidade pelo tratamento de dados pessoais e pela conformidade com os demais princípios, implementando medidas apropriadas e registros que demonstrem essa conformidade.

Desafios potenciais:

A complexidade dos sistemas de IA, especialmente daqueles suscetíveis ao fenômeno da “caixa-preta”, cria obstáculos significativos aos requisitos de documentação e proteção de dados.

Sua organização deve demonstrar que adotou as precauções necessárias e implementou medidas de segurança adequadas. Isso exige documentação abrangente do design do sistema de IA, dos dados de treinamento e do raciocínio por trás das decisões do sistema.

O princípio da *accountability* exige que as organizações mantenham controle completo sobre todo o ciclo de vida do sistema de IA, incluindo a realização de Avaliações de Impacto à Proteção de Dados (DPIA).

Nossa recomendação:

Para assegurar a responsabilização, as organizações devem projetar e implementar frameworks de governança que documentem a conformidade com as regulamentações de proteção de dados ao longo de todo o ciclo de vida do sistema de IA. Para sistemas de IA de alto risco, devem ser realizadas avaliações de impacto a fim de identificar e mitigar potenciais riscos à privacidade antes da implementação. Isso inclui a criação e a manutenção de documentação técnica detalhada sobre o design do sistema de IA, os dados de treinamento e os processos de tomada de decisão, garantindo transparência para as autoridades de supervisão e para os titulares dos dados.

Os sistemas de IA devem passar por auditorias sistemáticas para assegurar a conformidade com o GDPR, incluindo testes de viés e atualizações de segurança conforme necessário.

Também é fundamental dispor de diretrizes claras e de uma atribuição definida de responsabilidades em matéria de privacidade de dados. O treinamento dos colaboradores relevantes é necessário para garantir o acompanhamento adequado. Medidas de segurança, como criptografia, controles de acesso e registro (*logging*) das atividades de dados, também devem ser implementadas para proteger os dados pessoais de forma eficaz.



Legislação Trabalhista

A IA está transformando o ambiente de trabalho e desafiando os frameworks jurídicos tradicionais. Ao mesmo tempo em que aumenta a eficiência e cria novas oportunidades, também levanta questões importantes e considerações éticas relacionadas aos direitos dos colaboradores e à privacidade.

Conforme mencionado anteriormente, a IA pode melhorar substancialmente a eficiência dos negócios. A abordagem mais direta consiste em equipar os colaboradores com ferramentas de IA que aumentem sua produtividade. Como empregador, você pode determinar a organização e os métodos de trabalho no âmbito do seu poder diretivo. No entanto, dentro da UE e do EEE, o poder diretivo é limitado pelos direitos dos trabalhadores à informação, consulta e participação, conforme definidos pela legislação nacional. Embora os requisitos de consulta variem em detalhes entre os Estados-Membros, eles compartilham princípios subjacentes comuns.

A legislação trabalhista em toda a Europa exige que os empregadores abordem fatores como treinamento, desenvolvimento de competências e participação dos colaboradores, embora os requisitos específicos variem conforme a jurisdição. Em alguns países, conselhos de trabalhadores ou representantes dos empregados devem ser consultados antes da implementação de mudanças significativas nos processos de trabalho. Os empregadores devem consultar a legislação trabalhista nacional e os acordos coletivos aplicáveis para compreender as obrigações exatas em sua jurisdição antes de implementar sistemas de IA.

Quando os colaboradores precisam se adaptar a fluxos de trabalho integrados com IA, isso exige treinamento especializado. Como empregador, é necessário garantir que os colaboradores recebam treinamento adequado e contínuo, bem como suporte, para incorporar essas ferramentas de forma eficaz às suas atividades diárias. Também é importante promover o uso responsável da IA, levando em consideração os diferentes níveis de proficiência existentes na força de trabalho.



Alguns colaboradores podem demonstrar incerteza, ceticismo ou resistência em relação a mudanças tecnológicas. Abordar essas preocupações é essencial para uma implementação bem-sucedida.



Treinamento e competência

Antes de exigir que os colaboradores utilizem IA, é necessário garantir que recebam treinamento adequado e direcionado. Eles precisam desenvolver proficiência no uso das ferramentas de IA e compreender as implicações éticas e jurídicas que regem o uso da IA.

Justificativa e responsabilidade



Como empregador, você deve estabelecer um caso de negócio claro para a implementação de IA. Deve haver uma necessidade operacional legítima para melhorar a eficiência ou aprimorar a qualidade do trabalho, por exemplo, para manter a competitividade no mercado. Também é necessário avaliar como o uso da IA afetará o ambiente de trabalho. Caso sejam identificados impactos negativos potenciais, devem ser implementadas salvaguardas apropriadas para mitigá-los. Isso é conhecido como o requisito de implementação responsável.



Participação e envolvimento dos colaboradores

Se a implementação de IA alterar a forma como os colaboradores trabalham, pode ser necessário, conforme a legislação nacional, envolver os colaboradores e seus representantes antes de finalizar a mudança. Quando essa obrigação se aplica e como ela deve ser cumprida pode variar de país para país. Os colaboradores devem ter oportunidades significativas de contribuir com sugestões sobre como as ferramentas de IA serão integradas às operações diárias.

GDPR: Requisitos no ambiente de trabalho

Ferramentas de IA também podem ser aplicadas às áreas de RH, administração e gestão. Ao longo da última década, ferramentas voltadas a processos de recrutamento, monitoramento, avaliação e feedback passaram a ser oferecidas no mercado. Antes de implementar esse tipo de ferramenta, você, como empregador, deve avaliar cuidadosamente sua funcionalidade, aplicação e resultados, à luz das regulamentações aplicáveis.

É importante observar que o GDPR também se aplica ao tratamento de dados de colaboradores. Para garantir a conformidade, você deve:

- Informar os colaboradores sobre como a IA é utilizada e como os dados pessoais são tratados nesse contexto.
- Permitir que os colaboradores acessem as informações que o sistema de IA processa a seu respeito.
- Retificar informações incorretas quando solicitado pelos colaboradores ou quando forem identificados erros.

Também é importante destacar que decisões orientadas por IA no ambiente de trabalho podem ter consequências significativas para colaboradores individuais. O GDPR inclui requisitos específicos para a tomada de decisões automatizadas e o perfilhamento de titulares de dados. Esses requisitos se aplicam quando a IA é utilizada para tomar decisões que afetam as condições de trabalho, como promoções ou avaliações de desempenho.

A regra geral é que os titulares dos dados — e, portanto, os colaboradores — têm o

direito de solicitar que um ser humano, e não apenas uma máquina, esteja envolvido em decisões que produzam efeitos jurídicos ou que, de outra forma, os afetem de maneira significativa. No GDPR, isso é denominado o direito de não estar sujeito a decisões exclusivamente automatizadas.

Base legal para o tratamento

Se você pretende utilizar sistemas de IA que tratem dados pessoais de colaboradores, o GDPR determina que é necessário assegurar uma base legal para esse tratamento de dados.

Para essa base legal, pode ser tentador solicitar o consentimento dos colaboradores, mas essa frequentemente não é uma solução apropriada ou lícita. Considerando a relação de poder entre empregador e empregado, o colaborador pode sentir-se pressionado a conceder consentimento. Para que o consentimento seja válido, ele deve ser dado livremente, sem qualquer elemento de coação, pressão ou impossibilidade de recusa.

Recomenda-se considerar bases legais alternativas para o tratamento. Se o sistema de IA for necessário para as operações do negócio, o tratamento de dados poderá, muitas vezes, fundamentar-se em interesses legítimos ou na necessidade para a execução do contrato de trabalho, em vez de no consentimento. A base legal apropriada dependerá da aplicação específica da IA e da finalidade do tratamento.





AI Act: Requisitos e restrições no ambiente de trabalho

O AI Act da UE impacta a forma como ferramentas de IA podem ser implantadas no ambiente de trabalho. O regulamento classifica aplicações específicas — como aquelas utilizadas em recrutamento, monitoramento de colaboradores e tomada de decisões no local de trabalho — como de alto risco. Para aplicações de alto risco, não apenas os desenvolvedores ou aqueles que colocam o sistema no mercado europeu são afetados; os implementadores (deployers) também estão sujeitos a requisitos de conformidade. **As seguintes aplicações de IA são categorizadas como de alto risco no AI Act:**

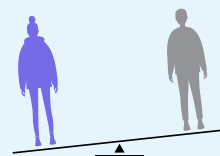
- Sistemas de IA para recrutamento e triagem/seleção de currículos (CVs). Isso inclui sistemas que posicionam e direcionam anúncios de vagas, analisam e classificam candidaturas ou avaliam candidatos a emprego.
- Sistemas de IA que influenciam condições de emprego. Isso inclui sistemas que tomam decisões sobre condições de trabalho, promoções ou desligamentos. Também abrange sistemas que alocam tarefas de trabalho com base no comportamento ou nas características dos colaboradores, bem como sistemas que monitoram e avaliam o desempenho e a conduta dos colaboradores no ambiente de trabalho.

Como empregador que utiliza um sistema de IA de alto risco, você deve cumprir diversos requisitos. É necessário implementar medidas técnicas e organizacionais para garantir que o sistema seja utilizado de acordo com sua finalidade pretendida. Há a obrigação de monitorar o desempenho, assegurar supervisão humana, garantir transparência e realizar uma avaliação de riscos. De forma especialmente relevante, é necessário garantir que o sistema não discrimine.

Por exemplo, se você utilizar IA para triagem de currículos, o sistema deve ser capaz de explicar a fundamentação por trás de suas avaliações das candidaturas. Também é essencial estar ciente e mitigar de forma eficaz o risco de que sistemas de IA amplifiquem vieses existentes no processo de recrutamento.

Ferramenta de recrutamento baseada em IA da Amazon

A ferramenta de recrutamento baseada em IA da Amazon foi descontinuada em 2018 porque discriminava mulheres no processo de seleção de currículos. O sistema de IA havia sido treinado com candidaturas a vagas ao longo de um período de dez anos, a maioria das quais provenientes de homens. Como resultado, o sistema aprendeu a despriorizar candidaturas que continham a palavra “mulher” ou que provinham de universidades tipicamente femininas. Mesmo após tentativas de corrigir esses vieses, a Amazon considerou a ferramenta não confiável e, por fim, interrompeu seu uso, citando preocupações de que o sistema não poderia ser ajustado de forma adequada para garantir resultados justos e imparciais no processo de recrutamento.



O AI Act também proíbe certos tipos de sistemas de IA no ambiente de trabalho, pois estes são classificados como representando um risco inaceitável. É proibida a implantação de sistemas de IA que tentem interpretar emoções por meio da análise de dados biométricos (dados sobre características físicas). Um exemplo disso são sistemas de IA projetados para avaliar se um candidato a emprego está dizendo a verdade em uma entrevista por meio da análise de expressões faciais ou da voz. A União Europeia determinou que tais sistemas representam um risco tão significativo aos direitos humanos fundamentais que não podem ser permitidos em nenhuma circunstância.

Guia de IA no ambiente de trabalho

À medida que a IA se torna uma parte mais significativa da força de trabalho, torna-se cada vez mais importante implementar diretrizes claras sobre como essas ferramentas devem ser utilizadas. Diretrizes internas de IA oferecem diversos benefícios nesse sentido:

Para os colaboradores, elas fornecem respostas claras sobre como as ferramentas de IA devem ser operadas de forma correta e responsável. Isso facilita a compreensão do que constitui uso proibido, bem como do uso pretendido das ferramentas. Dessa forma, podem ser evitados mal-entendidos e incertezas entre os colaboradores.

Para os empregadores, um guia é essencial para estabelecer limites claros. Ao explicar o que é permitido e o que não é no uso da IA, reduz-se o risco de não conformidade não intencional — seja em relação aos direitos dos colaboradores ou aos requisitos regulatórios. Limites claros também fornecem a melhor base para lidar com uso inadequado recorrente de ferramentas de IA.

Mais importante ainda, um guia bem elaborado pode ajudar a construir confiança entre empregadores e colaboradores ao demonstrar uma abordagem proativa em relação ao uso ético da IA. A criação de um guia abrangente também demonstra que a organização leva a implementação da IA a sério.

Metáfora do semáforo

A metáfora do semáforo pode ser uma forma prática e simples de estruturar diretrizes de uso de IA:



Vermelho – Uso proibido. Não é permitido em nenhuma circunstância. Exemplo: IA de reconhecimento de emoções em entrevistas (proibida pelo AI Act).

Amarelo – Uso que requer avaliação adicional. É necessário consultar as equipes de proteção de dados ou de TI antes de prosseguir. Exemplo: IA para triagem de currículos (alto risco, requer DPIA, transparência e supervisão humana).

Verde – Uso autorizado e lícito de ferramentas de IA. Trata-se de um uso seguro, alinhado às diretrizes da empresa. Exemplo: IA para tradução automática para uso interno, sem tratamento de dados pessoais.

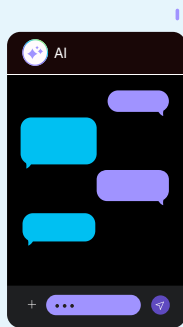
Caso: Monitoramento no local de trabalho sob uma nova perspectiva

À medida que o ambiente de trabalho se torna mais digital, os empregadores passam a dispor de maiores capacidades técnicas para monitorar as atividades dos colaboradores.

O monitoramento no local de trabalho está, de uma forma ou de outra, sujeito a regulamentações em toda a Europa, seja por meio do GDPR ou da legislação nacional. Enquanto alguns países impõem restrições rigorosas ao monitoramento de colaboradores, outros o permitem sob determinadas condições, como quando é necessário para fins de segurança ou conformidade.

Ao implementar ferramentas de IA no ambiente de trabalho, é necessário estar atento ao que constitui monitoramento e em quais condições ele é legalmente permitido. Tome como exemplo os assistentes de IA (copilots). Essas ferramentas têm acesso a e-mails, arquivos e pastas compartilhadas e podem realizar análises que anteriormente eram difíceis ou impraticáveis para indivíduos. Tecnicamente, um gestor poderia revisar tudo o que um colaborador escreveu e avaliar seu desempenho com base nisso. Sem o uso de IA, isso raramente seria um meio prático de monitoramento ou sequer possível de ser realizado manualmente, pois demandaria recursos excessivos.

Com assistentes de IA, os empregadores agora podem analisar facilmente grandes volumes de conteúdo para avaliar colaboradores. Sistemas de IA podem revisar arquivos e



documentos, e-mails, o uso de emojis de reação, declarações feitas em reuniões, entre outros elementos. No entanto, é importante lembrar: o fato de a tecnologia tornar isso possível não significa que seja legal. Esse tipo de monitoramento exige uma finalidade legítima que atenda aos requisitos da legislação de proteção de dados e do direito do trabalho.



Direitos de Propriedade Intelectual



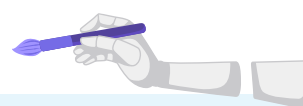
A propriedade intelectual concede o uso exclusivo, por exemplo, de invenções técnicas, marcas e obras criativas. A IA apresenta novos desafios para esses direitos, especialmente no que diz respeito ao uso de dados de entrada, dados de saída e dados de treinamento. Embora existam soluções práticas, é essencial compreender como a IA impacta tanto os seus próprios direitos de propriedade intelectual quanto os de terceiros.

O termo “propriedade intelectual” abrange, de forma ampla, diversos direitos que indivíduos ou empresas podem obter por meio da criação de obras originais. Esses direitos incluem direitos autorais, patentes, marcas registradas, direitos de design e segredos comerciais. Os direitos de propriedade intelectual concedem ao titular controle exclusivo sobre ativos intangíveis protegidos, que vão desde obras literárias e artísticas até invenções técnicas, identidades de marca e designs distintivos. O surgimento da IA desafia interpretações consolidadas do direito da propriedade intelectual em diversas áreas.

Direitos autorais sobre conteúdo gerado por IA

Conteúdo criado por IA pode receber proteção por direitos autorais? Para que uma obra seja protegida por direitos autorais, ela deve ser o resultado de uma expressão criativa original de um autor humano. Consequentemente, sistemas de IA não podem, de forma independente, deter direitos autorais.

Quem é o proprietário da arte criada por IA?



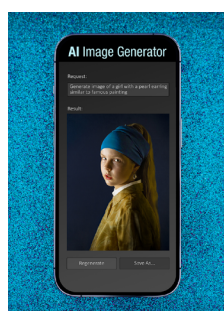
[Um artista apresentou um questionamento jurídico contra o Escritório de Direitos Autorais dos Estados Unidos \(U.S. Copyright Office\)](#) após o órgão se recusar a conceder direitos autorais à imagem *Theatre D'opera Spatial*, que ele criou utilizando a ferramenta de IA Midjourney.

A imagem, que venceu uma competição de arte, foi produzida por meio do teste de diversos *prompts* diferentes na ferramenta de IA e posteriormente refinada no Photoshop. **O Escritório de Direitos Autorais rejeitou o pedido porque a imagem continha conteúdo gerado por IA em excesso para se qualificar para proteção por direitos autorais.**

Mas e quanto ao usuário do sistema de IA? A visão predominante é que obras criadas com auxílio de IA podem ser elegíveis à proteção por direitos autorais, desde que o resultado reflita a contribuição intelectual e criativa original do usuário humano. O fator decisivo é o grau de controle criativo humano e de tomada de decisões exercido ao longo de todo o processo.

O nível de envolvimento humano necessário para que haja proteção por direitos autorais ainda não está totalmente definido. Nos Estados Unidos, indivíduos tiveram pedidos de direitos autorais negados para imagens geradas por IA quando sua contribuição se limitou ao fornecimento de *prompts* textuais. No entanto, o exercício de controle criativo substancial, como fornecer instruções detalhadas ao sistema de IA e editar a obra resultante, pode ser suficiente para estabelecer a proteção por direitos autorais no contexto da União Europeia. O fator decisivo é se o indivíduo demonstrou originalidade suficiente e controle criativo sobre o produto final.

Jogo limpo no uso de material de origem



A Getty Images entrou com uma ação judicial contra a empresa de IA

Stability AI por utilizar suas imagens sem permissão para treinar um sistema de IA capaz de gerar novas imagens. **A Getty alega que isso viola direitos autorais e infringe os direitos dos fotógrafos. A Stability AI argumenta que o uso das imagens é legal, pois se enquadra como "uso justo" (*fair use*) de acordo com a doutrina de direitos autorais.**

Risco de violação de direitos de propriedade intelectual de terceiros

O uso de ferramentas de IA, especialmente aquelas que geram texto, imagens ou código, envolve o risco de violação de direitos de propriedade intelectual de terceiros.

Como empresa, é importante reconhecer que conteúdos gerados por IA podem assemelhar-se inadvertidamente a obras existentes protegidas por direitos de propriedade intelectual. Mesmo sem a intenção de copiar, sistemas de IA podem produzir conteúdos que infrinjam tais direitos. Caso isso ocorra, os titulares dos direitos podem buscar indenização ou iniciar processos judiciais, independentemente de a infração ter sido intencional. É importante destacar que empresas que utilizam IA frequentemente são submetidas a padrões mais rigorosos do que indivíduos particulares.

Para mitigar esse risco, empresas de IA estão implementando salvaguardas para impedir que sistemas de IA gerem conteúdos protegidos por direitos autorais. O AI Act da União Europeia também exigirá que ferramentas de IA incluam medidas técnicas adequadas para evitar a criação de conteúdos que violem as regulamentações da UE, incluindo as leis de direitos autorais.

Dados de treinamento

Ao utilizar modelos de IA fornecidos por desenvolvedores terceiros, é essencial que as empresas compreendam quais materiais foram utilizados no processo de treinamento. **O treinamento de modelos de IA normalmente envolve o armazenamento temporário de grandes conjuntos de dados, o que pode constituir violação de direitos autorais se realizado sem o consentimento dos titulares dos direitos.**

Diversas grandes empresas de IA já enfrentaram processos judiciais pelo uso não autorizado de materiais protegidos por direitos autorais durante a fase de treinamento. Por exemplo, a Getty Images entrou com uma ação judicial contra a Stability AI, alegando o uso de milhões de imagens protegidas por direitos autorais sem permissão. De forma semelhante, vários autores iniciaram processos judiciais contra a OpenAI pelo uso de seus livros como dados de treinamento para o ChatGPT.

A União Europeia buscou abordar essa questão por meio da exceção de direitos autorais para mineração de texto e dados (*Text and Data Mining – TDM*), prevista na Diretiva de Direitos Autorais no Mercado Único Digital (DSM). Além disso, o AI Act introduz requisitos mais rigorosos de transparência em relação aos dados de treinamento, determinando que os desenvolvedores de IA documentem quais obras protegidas por direitos autorais foram utilizadas.



Mudanças nas leis de dados com a IA

A Diretiva de Direitos Autorais no Mercado Único Digital (DSM) introduz novas regras de direitos autorais para o mundo digital. **Uma mudança significativa é que passa a ser legal analisar grandes volumes de texto e dados (mineração de texto e dados — *Text and Data Mining, TDM*) sem a necessidade de obter previamente autorização dos titulares dos direitos.**

Isso significa que, ao realizar pesquisas ou conduzir atividades empresariais, é possível analisar qualquer material ao qual se tenha acesso legal. Isso inclui conteúdos disponibilizados online com a aprovação do titular dos direitos e, provavelmente, também conteúdos acessados por meio de serviços por assinatura.

Os titulares de direitos podem optar por impedir que seu conteúdo seja utilizado para mineração de texto e dados, mas a diretiva não especifica como essa opção deve ser exercida. Uma solução prática para sites pode ser a implementação de um sinal legível por máquina que indique que o conteúdo não pode ser utilizado para esse tipo de análise.

Proteção contra ações judiciais ao utilizar modelos de IA pré-treinados

Muitos fornecedores de IA renunciam aos direitos sobre os resultados gerados por seus modelos. Como usuário, isso geralmente significa que você pode ter confiança de que o fornecedor de IA não reivindicará direitos sobre o conteúdo que você cria utilizando o serviço. No entanto, continua sendo fundamental garantir que os dados de treinamento utilizados nesses modelos não infrinjam os direitos de propriedade intelectual de terceiros. A falta de licenciamento adequado dos dados de treinamento pode expor sua empresa a reivindicações legais ou litígios.

Alguns grandes fornecedores de IA oferecem medidas de proteção para proporcionar maior segurança aos usuários. Essas medidas podem incluir:



Acordos de indenização

O fornecedor pode assumir a responsabilidade pelos custos legais e por eventuais indenizações caso o sistema de IA seja considerado infrator de direitos de propriedade intelectual.

Garantias sobre dados de treinamento



Alguns fornecedores garantem que seus dados de treinamento sejam devidamente licenciados, proporcionando maior segurança de que você não será responsabilizado por violações.



Suporte jurídico

O fornecedor pode oferecer assistência jurídica ou representação legal caso surjam reivindicações relacionadas à violação de direitos de propriedade intelectual decorrentes do uso de seu sistema de IA.

Essas medidas de proteção podem oferecer algum grau de segurança, mas é necessário revisar cuidadosamente os termos de serviço do fornecedor e as limitações de responsabilidade para garantir que sua empresa esteja adequadamente coberta.



Termos e condições de licença

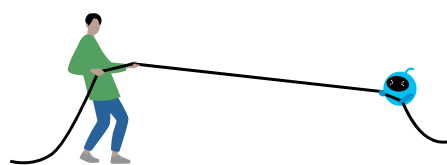
O mercado atual de IA é dominado por poucas grandes corporações norte-americanas, o que limita o poder de negociação na adoção de ferramentas de IA. Mesmo quando as condições contratuais não são negociáveis, compreender os termos aos quais se está aderindo continua sendo essencial.

Os contratos padrão dessas empresas geralmente são moldados por tradições jurídicas norte-americanas, consistindo frequentemente em múltiplos documentos extensos, com linguagem complexa e atualizações frequentes. Embora os termos gerais costumem ser semelhantes entre os fornecedores, identificar diferenças pequenas, porém críticas, pode ser desafiador.

Se a sua organização pretende utilizar serviços de IA, você deve:

- **Realizar uma análise minuciosa dos termos e condições antes de iniciar o uso.**
- **Monitorar continuamente as atualizações desses termos.**

Dada a natureza não negociável desses contratos, a escolha do fornecedor de IA adequado é fundamental. O fornecedor deve apoiar a inovação ao mesmo tempo em que garante a conformidade com os requisitos de privacidade e segurança de dados. Um ponto central de avaliação é equilibrar os custos em relação às medidas de segurança oferecidas pelo fornecedor.



Serviços gratuitos de IA

Ferramentas de IA gratuitas podem parecer economicamente vantajosas, mas frequentemente envolvem compensações ocultas. Muitos fornecedores monetizam essas ferramentas utilizando dados pessoais e entradas dos usuários, o que pode resultar em publicidade direcionada, segurança de dados mais fraca e menor controle sobre as informações compartilhadas. Em modelos gratuitos, os fornecedores costumam usar dados dos usuários para aprimorar e refinar seus sistemas de IA. Essa prática levanta preocupações para as empresas no que diz respeito à privacidade de dados, às obrigações de confidencialidade e à proteção de segredos comerciais. Ela pode levar à não conformidade com o GDPR (como a ausência de um acordo de tratamento de dados ou a transferência de dados para fora da UE) e a consequentes violações de obrigações contratuais para empresas que atuam como operadores de dados. Para organizações que lidam com dados pessoais sensíveis ou informações proprietárias, é fortemente recomendável investir em uma solução de IA paga que ofereça garantias robustas de segurança.

Em modelos gratuitos, os fornecedores frequentemente utilizam dados dos usuários para aprimorar e refinar seus sistemas de IA. Essa prática levanta preocupações para as empresas no que se refere à privacidade de dados, às obrigações de confidencialidade e à proteção de segredos comerciais. **Para organizações que lidam com dados pessoais sensíveis ou informações proprietárias, é fortemente recomendável investir em uma solução de IA paga que ofereça garantias robustas de segurança.**

Ao revisar acordos de prestação de serviços de grandes fornecedores de IA, é comum encontrar extensas limitações de responsabilidade e restrições detalhadas de uso. Os fornecedores reconhecem explicitamente que seus sistemas de IA podem produzir erros, apesar do uso de tecnologia avançada. Muitos acordos proíbem expressamente o uso de sistemas de IA em setores de alto risco, como serviços jurídicos, assessoria financeira e saúde. Essas restrições funcionam tanto como mecanismos de limitação de responsabilidade quanto como reconhecimento das limitações atuais da IA. Em tais setores, nos quais erros podem ter consequências significativas, o comprador e o implementador dos sistemas de IA assumem responsabilidade substancial pelos resultados.

Antes de celebrar acordos para serviços de IA, analise cuidadosamente os termos e as condições de licenciamento. Os principais aspectos a considerar incluem como o acordo regula:



Tratamento de dados e direitos: Determine quem mantém a titularidade dos seus dados de entrada e como o fornecedor pode utilizá-los. Dê atenção especial a saber se o fornecedor está autorizado a usar seus dados para treinar seus modelos de IA.



Limitações de responsabilidade: Esclareça a responsabilidade do fornecedor por erros ou resultados imprecisos. Revise quaisquer níveis de serviço garantidos relacionados à confiabilidade do sistema e ao tempo de disponibilidade (uptime).



Restrições de uso: Identifique quaisquer limitações sobre como você pode utilizar o modelo, incluindo restrições ao tratamento de dados ou áreas de aplicação proibidas.



Privacidade e segurança da informação: Avalie os períodos de retenção de dados, os tipos de dados armazenados, as medidas de segurança aplicáveis e as finalidades para as quais os dados são mantidos.

IA personalizada – Uso de APIs



Para muitas empresas, aproveitar a IA de forma eficaz envolverá o desenvolvimento de modelos personalizados por meio do uso de APIs (Application Programming Interfaces) de modelos de linguagem de grande escala (LLMs). Essa abordagem permite que as organizações personalizem soluções de IA às suas necessidades específicas, ao mesmo tempo em que se beneficiam de modelos pré-treinados poderosos.

O uso de APIs oferece flexibilidade significativa na definição de um serviço. No entanto, no que diz respeito aos termos de uso das APIs de grandes fornecedores, o poder de negociação costuma ser mínimo. Na prática, as condições fundamentais aplicáveis aos LLMs são em grande parte semelhantes entre os diferentes fornecedores.

Ao utilizar APIs, é especialmente importante estar atento ao direito do fornecedor de modificar a API ou seus termos e a como essas alterações podem impactar a solução personalizada.

Histórico do documento e agradecimentos

Fontes e colaboradores

Da Experis, as seguintes pessoas participaram de sessões de trabalho ou forneceram outras contribuições valiosas:

- Jørgen Longva, Director Competencies
- Ekaterina Kuzmina, Subject Matter Expert Data & ML
- Robert Grønås, Subject Matter Expert Digital Security
- Rune Aasgaard, Community Lead Strategy and Transformation

Da Vaar Law, as seguintes pessoas participaram:

- Thor Beke, Managing Partner
- Johanne Mustad, Associate Lawyer

Documentos e Fontes

- AT&T. Autonomous Assistants: The Next Step of the GenAI Revolution to Empower Employees and Serve Customers. Retrieved October 2024. <https://about.att.com/blogs/2024/autonomous-assistants.html>
- Bastigkeit Ericstam, Sonia. AI in the Workplace: Regulating Explainability and Consent in Algorithmic Management. Faculty of Law, Stockholm University Research Paper No. 135, March 4, 2024.
- CNN Business. Zillow's home-buying debacle shows how hard it is to use AI to value real estate. Retrieved October 2024. <https://edition.cnn.com/2021/11/09/tech/zillow-ibuying-home-zestimate/index.html>
- Digital Norway. Vaktplaner, ruteoptimalisering og prognoser: Derfor er data en nøkkel til Odas suksess, Retrieved October 2024, <https://digitalnorway.com/ruteoptimalisering-vaktplaner-prognoser-derfor-er-data-en-nokkel-til-odas-suksess/>
- EU AI Act. Annex I: List of Union Harmonisation Legislation. Retrieved October 2024. <https://artificialintelligenceact.eu/annex/1/>

- EU AI Act. Annex II: List of Criminal Offences Referred to in Article 5(1), First Subparagraph, Point (h)(iii). Retrieved October 2024. <https://artificialintelligenceact.eu/annex/2/>
- EU AI Act. Annex III: High-Risk AI Systems Referred to in Article 6(2). Retrieved October 2024. <https://artificialintelligenceact.eu/annex/3/>
- EU Joint Research Centre Data Catalogue. Selected AI cases in the public sector (JRC129301). Retrieved October 2024. <https://data.jrc.ec.europa.eu/dataset/7342ea15-fd4f-4184-9603-98bd87d8239a>
- Futurity.org. Facebook posts with these words can predict depression. Retrieved September 2024. <https://www.futurity.org/depression-facebook-prediction-1893812>
- Gartner. AI and Generative AI Case Study Snapshots. Retrieved October 2024. <https://www.gartner.com/document-reader/document/5191663>
- Gartner. Gartner AI Opportunity Radar: Set Your Enterprise's AI Ambition. Retrieved October 2024. <https://www.gartner.com/document-reader/document/4836831>
- INRIX. INRIX Announces Compass, a New Mobility Intelligence Technology Powered by 20+ Years of Proprietary Data and Amazon Bedrock Generative AI». Retrieved October 2024. <https://inrix.com/press-releases/bedrock-compass-gen-ai/>
- Microsoft and LinkedIn, 2024. Work Trend Index Annual Report - AI at Work Is Here—Now Comes the Hard Part. Microsoft WorkLab. Retrieved August 2024. <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>
- Reuter. Artist sues after US rejects copyright for AI-generated image. Retrieved October 2024. <https://www.reuters.com/legal/litigation/artist-sues-after-us-rejects-copyright-ai-generated-image-2024-09-26/>
- Section. The AI Proficiency Report. Section School, 2024. Retrieved September 2024. <https://www.sectionschool.com>
- Strümke, Inga. Maskiner som tenker. Kagge forlag, 2023.
- Toyota Research Institute. Toyota Research Institute Unveils New Generative AI Technique for Vehicle Design. Retrieved October 2024. <https://pressroom.toyota.com/toyota-research-institute-unveils-new-generative-ai-technique-for-vehicle-design/>

O ChatGPT, o Perplexity.ai e o Claude. ai receberam perguntas formuladas da seguinte maneira: “Você pode fornecer alguns exemplos de [tópico]?”. As respostas foram avaliadas à luz da experiência e do conhecimento pessoal, adaptadas a contextos específicos, utilizadas para pesquisa adicional e incorporadas à expansão de ideias originais.

Histórico de revisões

Versão	Data	Descrição	Pessoas responsáveis
1.0	2024-11-25	Primeira edição	Director Competencies at Experis Norway, Jørgen Longva, and Managing Partner at Vaar Law, Thor Beke
1.0.1	2025-02-18	Corrigiu um erro na pirâmide de risco do AI Act	Director Competencies at Experis Norway, Jørgen Longva
1.0.1	2025-03-16	Tradução para o inglês	Director Competencies, Jørgen Longva, and Rune Aasgaard, Community Lead Strategy and Transformation, both at Experis Norway. Johanne Mustad, Associate Lawyer at Vaar Advokat.
1.0.2	2025-10-21	Globalização do relatório	Head of Legal at ManpowerGroup Norway, Emil Skjærvø Sætereng

SOBRE A EXPERIS

A Experis® é líder global em alocação de profissionais de TI e serviços de tecnologia da informação. A Experis acelera o crescimento das organizações ao atrair, avaliar e alocar talentos tecnológicos especializados em funções de alta demanda, entregando projetos críticos para o negócio que aumentam a competitividade das organizações e das pessoas que atendemos. Por meio da Experis Academy, oferecemos treinamentos intensivos e programas de capacitação para recém-formados, além de desenvolvimento de competências personalizadas para preparar colaboradores atuais para funções tecnológicas de alta demanda. A Experis faz parte da família de marcas do ManpowerGroup® (NYSE: MAN), que também inclui Manpower e Talent Solutions.

Para mais informações, visite nosso site.

