Aula 40 – Ética em Visão Computacional: Vieses, Privacidade e Responsabilidade

A Visão Computacional (VC) tem se tornado uma das tecnologias mais transformadoras do nosso tempo, redefinindo a forma como interagimos com o mundo digital e físico. Desde o desbloqueio do seu smartphone com o rosto até sistemas complexos de diagnóstico médico e veículos autônomos, a capacidade das máquinas de "ver" e interpretar imagens e vídeos está em constante evolução. No entanto, com grande poder vem grande responsabilidade. À medida que esses sistemas se tornam mais sofisticados e onipresentes, emergem questões éticas complexas que não podem ser ignoradas.

Nesta aula, não vamos apenas explorar os aspectos técnicos da Visão Computacional, mas mergulhar nas suas implicações mais profundas. Você já parou para pensar como um algoritmo de reconhecimento facial pode ser injusto? Ou como a vigilância por câmeras pode impactar sua privacidade? Nosso objetivo é que, ao final desta jornada, você seja capaz de identificar e analisar os vieses presentes em dados e sistemas de VC, compreender os desafios de privacidade inerentes a essas tecnologias e reconhecer a urgência de desenvolver e implementar soluções de forma ética e responsável.

Este conhecimento é crucial não apenas para o desenvolvimento de sistemas mais justos e seguros, mas também para a sua atuação profissional em um mercado que exige cada vez mais uma consciência ética robusta. Prepare-se para conectar o que você já sabe sobre redes neurais e processamento de imagens com um novo olhar sobre o impacto social e moral da tecnologia.

O Poder da Visão Computacional e Seus Dilemas Inerentes

Imagine um mundo onde as máquinas não apenas veem, mas também interpretam, categorizam e até preveem eventos a partir de imagens. Esse mundo já é a nossa realidade, impulsionado pela Visão Computacional. Desde a otimização de linhas de produção industrial até a assistência em cirurgias complexas, a VC está em todo lugar, prometendo eficiência e inovação. Contudo, essa capacidade extraordinária de processar informações visuais em escala massiva traz consigo uma série de dilemas éticos que exigem nossa atenção e reflexão.

A tecnologia, por si só, é uma ferramenta neutra. É a forma como a projetamos, implementamos e utilizamos que define seu impacto. No caso da Visão Computacional, o potencial para o bem é imenso, mas o risco de perpetuar ou até amplificar desigualdades e injustiças também é real. Precisamos entender que cada linha de código, cada dataset de treinamento e cada decisão de design carrega consigo valores e pressupostos que podem ter consequências profundas na vida das pessoas.

> Pense na Visão Computacional como uma **faca de dois gumes**: ela pode cortar o caminho para avanços incríveis, mas também pode ferir se usada sem cuidado. É essa dualidade que nos convida a explorar as áreas críticas de vieses, privacidade e responsabilidade, garantindo que o progresso tecnológico seja acompanhado por um compromisso ético inabalável.

Vieses em Dados: O Espelho Distorcido da Realidade

Para que um sistema de Visão Computacional "aprenda" a reconhecer objetos, pessoas ou padrões, ele precisa ser alimentado com uma vasta quantidade de dados visuais. Esses dados, geralmente imagens e vídeos, são a base sobre a qual os modelos de Deep Learning, como as Redes Neurais Convolucionais (CNNs) e os Vision Transformers (ViT), constroem seu conhecimento. No entanto, a qualidade e a representatividade desses datasets são absolutamente cruciais, pois qualquer distorção presente neles será inevitavelmente refletida e amplificada pelo sistema.

O problema surge quando esses conjuntos de dados não são um espelho fiel da diversidade do mundo real. Se um dataset de treinamento é predominantemente composto por imagens de um determinado grupo demográfico, etnia ou gênero, o modelo resultante terá dificuldades em reconhecer ou processar com precisão indivíduos que não se encaixam nesse perfil majoritário. Essa falta de representatividade não é um erro técnico, mas sim um reflexo de vieses sociais e históricos que são inadvertidamente incorporados ao processo de coleta e anotação dos dados.

> **Imagine que você está ensinando uma criança a reconhecer animais, mas só mostra fotos de cachorros de uma única raça.** Quando ela encontrar um cachorro de outra raça ou um gato, sua capacidade de identificação será limitada. Da mesma forma, os sistemas de VC aprendem com o que lhes é mostrado, e se o "mundo" que lhes apresentamos é incompleto ou distorcido, suas "percepções" também serão.

Impactos dos Vieses em Sistemas de Reconhecimento Facial

Os vieses em datasets não são meras curiosidades acadêmicas; eles têm consequências tangíveis e muitas vezes graves, especialmente em aplicações críticas como o reconhecimento facial. Sistemas de reconhecimento facial são utilizados em diversas áreas, desde o desbloqueio de celulares e controle de acesso até a identificação de suspeitos em investigações criminais e a vigilância em espaços públicos. Quando esses sistemas são treinados com dados enviesados, sua precisão pode variar drasticamente entre diferentes grupos demográficos.

Taxas de Erro Desiguais

Estudos demonstram que algoritmos de reconhecimento facial apresentam taxas de erro significativamente mais altas para mulheres e pessoas de pele escura em comparação com homens e pessoas de pele clara.

Falsos Positivos e Negativos

Um sistema enviesado pode falhar em identificar corretamente uma pessoa de um grupo minoritário, levando a identificações erradas ou falhas na identificação.

Discriminação Algorítmica

O viés algorítmico pode se tornar uma ferramenta de discriminação e injustiça social, perpetuando preconceitos existentes na sociedade.

Pense em um sistema de segurança aeroportuária que falha em identificar um passageiro legítimo devido à sua etnia, causando atrasos e constrangimentos injustos. Ou, ainda mais grave, um sistema de vigilância que erroneamente identifica um indivíduo como suspeito de um crime, resultando em uma investigação equivocada ou até mesmo em uma prisão injusta. Esses exemplos ilustram como o viés algorítmico pode se tornar uma ferramenta de discriminação e injustiça social, perpetuando preconceitos existentes na sociedade. É como usar **óculos com lentes coloridas**: o mundo que o sistema "vê" é filtrado e distorcido, e as decisões tomadas com base nessa visão podem ser profundamente falhas.

Mitigando Vieses: Estratégias e Desafios na Construção de Sistemas Justos

Reconhecer a existência de vieses é o primeiro passo, mas a verdadeira questão é: como podemos construir sistemas de Visão Computacional mais justos e equitativos? A mitigação de vieses é um campo de pesquisa ativo e complexo, envolvendo abordagens que vão desde a coleta de dados até o design do algoritmo e a avaliação pós-implementação. Não existe uma solução única, mas sim um conjunto de estratégias que, quando aplicadas em conjunto, podem reduzir significativamente a probabilidade de um sistema perpetuar injustiças.

01

Diversificação dos Datasets

Garantir que os dados reflitam a verdadeira diversidade da população que o sistema irá atender, incluindo diferentes etnias, gêneros, idades e condições de iluminação.

02

Aumentação de Dados

Gerar novas amostras a partir das existentes, com pequenas variações, para enriquecer o dataset de treinamento.

03

Coleta Direcionada

Focar na obtenção de dados de grupos sub-representados para equilibrar o conjunto de treinamento.

04

Adversarial Debiasing

Desenvolver algoritmos que podem identificar e corrigir vieses durante o processo de aprendizado.

No entanto, a mitigação de vieses não é um processo simples. Definir o que é "justiça" em um contexto algorítmico pode ser um desafio, pois diferentes métricas de justiça podem entrar em conflito. Além disso, a coleta de dados diversificados pode ser cara e demorada, e a implementação de técnicas avançadas de debiasing pode adicionar complexidade ao modelo. É como tentar **ajustar uma balança** com muitos pesos diferentes: é preciso cuidado, conhecimento e um compromisso contínuo para alcançar o equilíbrio.

Estratégia de Mitigação	Âmbito/Aplicação	Base/Origem	Exemplo
Diversificação de Dados	Pré-treinamento	Coleta de dados	Incluir mais imagens de grupos sub-representados
Aumentação de Dados	Pré-treinamento	Processamento de dados	Rotacionar, espelhar ou alterar brilho de imagens existentes
Adversarial Debiasing	Durante treinamento	Algoritmo	Usar uma rede adversária para "ensinar" o modelo a ser imparcial
Auditoria Algorítmica	Pós-treinamento	Avaliação	Testar o modelo em diferentes grupos demográficos para identificar vieses

Privacidade na Era da Visão Computacional: Uma Nova Fronteira

Se os vieses representam uma distorção na forma como a Visão Computacional "vê" o mundo, a privacidade aborda o que acontece com as imagens e vídeos que ela processa. Em um cenário onde câmeras estão em quase todos os lugares – ruas, lojas, residências, veículos – a coleta de dados visuais se tornou massiva e, muitas vezes, invisível para o indivíduo. Essa onipresença levanta questões fundamentais sobre quem tem acesso a essas informações, como elas são armazenadas, por quanto tempo e para quais finalidades.

A Visão Computacional pode extrair uma quantidade surpreendente de informações de uma imagem: não apenas a identidade de uma pessoa, mas também suas emoções, seu comportamento, seus hábitos e até mesmo sua saúde. Quando esses dados são coletados sem consentimento explícito ou sem um propósito claro e limitado, a linha entre a conveniência tecnológica e a invasão da privacidade se torna tênue. A preocupação não é apenas com a vigilância governamental, mas também com o uso comercial desses dados, que podem ser usados para publicidade direcionada, precificação discriminatória ou até mesmo para influenciar decisões pessoais.

> Imagine que cada vez que você sai de casa, um diário detalhado de seus movimentos, interações e até mesmo expressões faciais está sendo secretamente preenchido. Essa é a analogia de um **diário aberto em praça pública** que a falta de privacidade na Visão Computacional pode representar.

Sistemas de Vigilância e a Invasão da Privacidade

Os sistemas de vigilância baseados em Visão Computacional são talvez o exemplo mais palpável e controverso do conflito entre segurança e privacidade. Câmeras de segurança, antes estáticas e passivas, agora são equipadas com IA capaz de realizar detecção de objetos em tempo real, reconhecimento facial, análise de comportamento e até mesmo predição de eventos. Em cidades inteligentes, aeroportos, shoppings e até mesmo em condomínios residenciais, a promessa é de maior segurança e eficiência.

No entanto, essa promessa vem acompanhada de um custo potencial para a liberdade individual. A capacidade de rastrear os movimentos de uma pessoa, identificar sua presença em múltiplos locais e cruzar essas informações com outros bancos de dados levanta sérias preocupações sobre a criação de uma sociedade de vigilância em massa. O uso indiscriminado ou sem supervisão desses sistemas pode levar à erosão da privacidade, à supressão da dissidência e à criação de perfis detalhados de cidadãos sem seu conhecimento ou consentimento.

Rastreamento de Movimentos

Identificação da presença em múltiplos locais e cruzamento de informações

Análise Comportamental

Predição de eventos e criação de perfis detalhados

Erosão da Liberdade

Supressão da dissidência e monitoramento sem consentimento

Considere o uso de reconhecimento facial em protestos públicos. Embora possa ser justificado pela segurança, também pode ser usado para identificar e monitorar ativistas, inibindo o direito à livre expressão. A questão central é encontrar um equilíbrio: como podemos aproveitar os benefícios da Visão Computacional para a segurança sem transformar nossos espaços públicos em zonas de vigilância constante, onde cada passo é monitorado e cada rosto é escaneado?

Tecnologias para Preservação da Privacidade

Diante dos desafios impostos pela Visão Computacional à privacidade, a boa notícia é que a inovação tecnológica também oferece soluções. A área de "Privacy-Preserving AI" (IA que Preserva a Privacidade) está em constante evolução, desenvolvendo métodos para permitir que os sistemas de VC funcionem eficazmente sem comprometer a identidade ou os dados sensíveis dos indivíduos. O objetivo é criar um **escudo invisível** para as informações pessoais, permitindo a análise de dados sem a necessidade de expô-los diretamente.

Privacidade Diferencial

Adiciona "ruído" matemático aos dados de forma controlada, tornando impossível identificar um indivíduo específico em um grande conjunto de dados, enquanto ainda permite análises estatísticas precisas.

Criptografia Homomórfica

Permite realizar cálculos sobre dados criptografados sem a necessidade de descriptografá-los. Um modelo de VC pode processar imagens sem nunca "ver" o conteúdo original em texto claro.

Aprendizado Federado

Permite que modelos de IA sejam treinados em dados descentralizados. Os dados permanecem nos dispositivos dos usuários, e apenas as atualizações do modelo são compartilhadas.

Essas tecnologias são cruciais para construir sistemas de Visão Computacional que sejam poderosos e, ao mesmo tempo, respeitem a privacidade dos usuários, pavimentando o caminho para uma IA mais ética e confiável.

A Responsabilidade do Desenvolvedor e da Empresa

Quando um sistema de Visão Computacional falha eticamente – seja por vieses que levam à discriminação ou por falhas na proteção da privacidade – surge a pergunta crucial: de quem é a responsabilidade? A resposta não é simples, pois envolve uma cadeia complexa de atores, desde os pesquisadores que desenvolvem os algoritmos, passando pelos engenheiros que os implementam, até as empresas que os comercializam e os governos que os regulam. No entanto, o desenvolvedor e a empresa que constroem e implantam esses sistemas carregam um peso significativo nessa equação.

Design Ético

Considerar proativamente os potenciais impactos sociais e éticos desde a concepção

Validação Rigorosa

Testar modelos em diversos grupos demográficos e implementar mecanismos de transparência

Políticas Corporativas

Estabelecer diretrizes claras de uso ético e investir em auditorias independentes

> Pense no desenvolvedor como o **arquiteto de uma ponte**: ele não é apenas responsável por sua solidez estrutural, mas também por garantir que ela seja segura para todos que a atravessam e que não cause danos ao ambiente ao redor. A negligência em qualquer etapa pode ter consequências desastrosas.

A construção de uma cultura de responsabilidade ética dentro das equipes de desenvolvimento e nas empresas é fundamental para garantir que a Visão Computacional seja uma força para o bem.

Regulamentação e Governança da Visão Computacional

A velocidade com que a Visão Computacional e a Inteligência Artificial avançam muitas vezes supera a capacidade das leis e regulamentações de acompanhá-las. No entanto, a necessidade de um arcabouço legal robusto para governar o uso dessas tecnologias é inegável. A regulamentação não visa frear a inovação, mas sim garantir que ela ocorra de forma segura, justa e respeitosa aos direitos humanos. Sem diretrizes claras, o risco de abusos e de um desenvolvimento irresponsável aumenta exponencialmente.

Iniciativas globais, como o Ato de IA da União Europeia (EU AI Act), são exemplos de esforços para criar um quadro regulatório abrangente. Essas leis buscam classificar os sistemas de IA com base em seu nível de risco (de risco mínimo a inaceitável) e impor obrigações correspondentes, como a necessidade de avaliação de conformidade, supervisão humana e transparência. No Brasil, a Lei Geral de Proteção de Dados (LGPD) já estabelece princípios importantes para o tratamento de dados pessoais, incluindo aqueles coletados por sistemas de VC.

1

Classificação de Risco

Sistemas categorizados de risco mínimo a inaceitável

2

Avaliação de Conformidade

Obrigações de auditoria e certificação

3

Supervisão Humana

Garantia de controle e intervenção humana

4

Transparência

Direito à explicabilidade das decisões

A regulamentação atua como as **regras do jogo**: ela define os limites, estabelece as expectativas e impõe consequências para o descumprimento. Para a Visão Computacional, isso significa estabelecer padrões para a coleta e uso de dados, exigir auditorias de vieses, garantir o direito à explicabilidade das decisões algorítmicas e proteger a privacidade dos cidadãos.

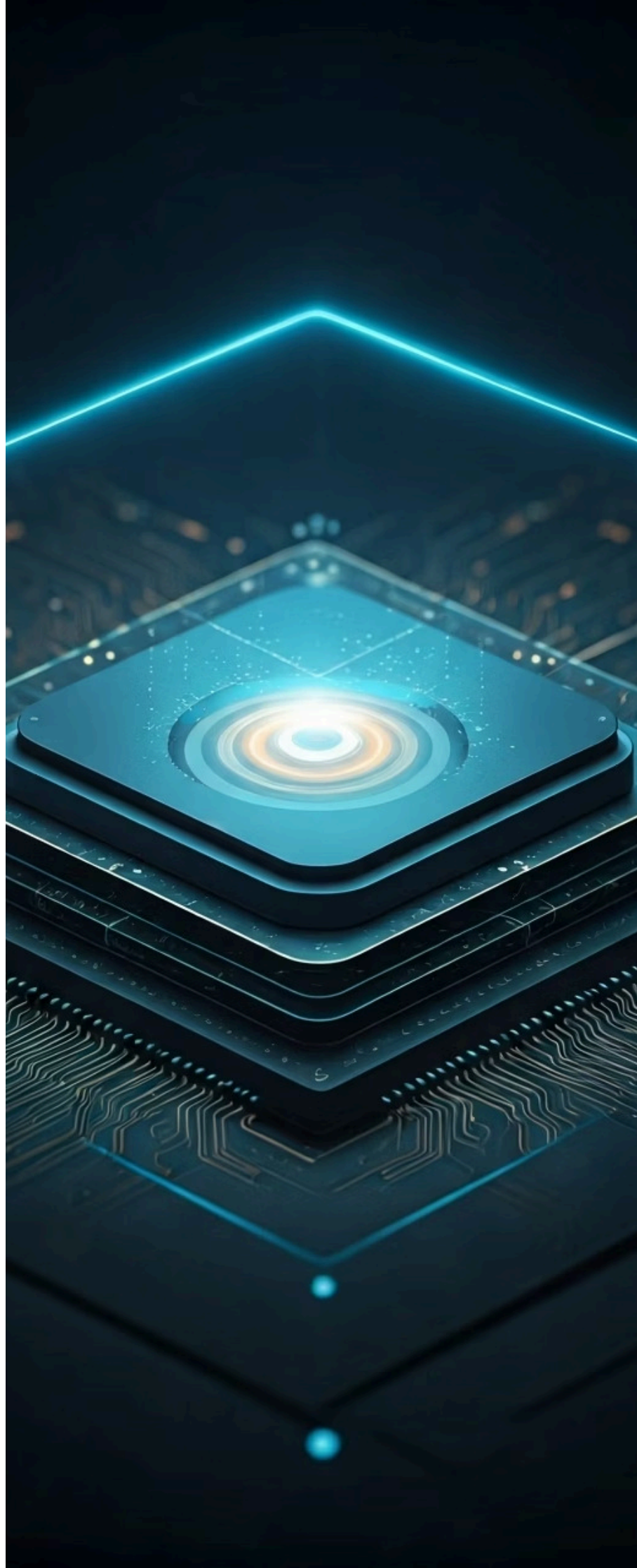
O Papel dos Vision Transformers (ViT) e a Ética

A evolução dos modelos de Deep Learning trouxe novas arquiteturas, e os Vision Transformers (ViT) representam uma das mais recentes e impactantes inovações. Diferentemente das CNNs tradicionais, que processam imagens por meio de filtros locais, os ViTs utilizam mecanismos de "atenção" para analisar a imagem de forma global, capturando relações de longo alcance entre diferentes partes da imagem. Essa capacidade de contextualização global, embora poderosa, também introduz novas considerações éticas.

A complexidade inerente aos ViTs e a outros modelos de IA de última geração, como ResNet e EfficientNet, pode tornar ainda mais desafiador identificar e mitigar vieses. Se um viés se manifesta de forma sutil em padrões de atenção distribuídos por toda a imagem, sua detecção e correção exigem ferramentas de explicabilidade mais sofisticadas. Além disso, a capacidade desses modelos de aprender representações altamente abstratas pode dificultar a compreensão de como eles chegam a determinadas decisões, criando o que é conhecido como o problema da "caixa preta".

> Pense nos ViTs como um **novo par de olhos** que veem a imagem de uma maneira completamente diferente. Embora esses olhos possam ser mais perspicazes em alguns aspectos, também podem ter seus próprios pontos cegos ou formas de interpretar o mundo que são difíceis de decifrar.

A pesquisa em **IA Explicável (XAI)** é fundamental para desvendar o funcionamento interno desses modelos complexos, permitindo que desenvolvedores e usuários compreendam por que uma decisão foi tomada e, assim, identifiquem e corrijam potenciais vieses ou falhas éticas.



IA Generativa e os Desafios Éticos na Criação de Imagens

A ascensão da IA Generativa, com modelos como as GANs (Generative Adversarial Networks) e os Modelos de Difusão, revolucionou a criação e edição de imagens. Essas tecnologias são capazes de gerar conteúdo visual ultrarrealista, desde rostos de pessoas que nunca existiram até paisagens fantásticas e obras de arte. Embora o potencial criativo seja imenso, essa capacidade também abre portas para desafios éticos significativos, especialmente no que tange à autenticidade e à disseminação de informações falsas.

Deepfakes

Rostos e vozes sintetizados para criar vídeos ou áudios falsos convincentes, usados para desinformação, manipulação política, fraude ou difamação.

Autenticidade

A linha entre o real e o sintético torna-se cada vez mais indistinguível, levantando questões sobre a confiança na mídia.

Direitos Autorais

Quem é o "autor" de uma imagem gerada por IA? O modelo, o desenvolvedor, ou o artista que forneceu os dados de treinamento?

É como ter um **artista capaz de criar falsificações perfeitas**: a habilidade é impressionante, mas o uso indevido pode ser devastador. A pesquisa em **detecção de deepfakes** e em **marca d'água digital** para conteúdo gerado por IA é crucial para combater o uso malicioso e garantir a integridade do ambiente digital.

Aplicações em Tempo Real e a Urgência Ética

A Visão Computacional não se limita a análises pós-evento; ela está cada vez mais presente em aplicações que exigem decisões em tempo real. Algoritmos otimizados para detecção de objetos, rastreamento de movimento e análise de cenas em milissegundos são a espinha dorsal de sistemas de veículos autônomos, robótica industrial, drones de entrega e até mesmo assistentes de segurança pessoal. A capacidade de reagir instantaneamente a estímulos visuais é um avanço tecnológico notável, mas também amplifica a urgência das considerações éticas.

Veículos Autônomos

Decisões de vida ou morte em frações de segundo

Robótica Industrial

Segurança e colaboração humano-máquina

Vigilância em Tempo Real

Privacidade e proteção de dados instantânea

> Em sistemas de tempo real, as decisões algorítmicas têm consequências imediatas e, muitas vezes, irreversíveis. Um viés em um algoritmo de detecção de pedestres em um carro autônomo, por exemplo, pode ter resultados fatais. Uma falha de privacidade em um sistema de vigilância em tempo real pode expor dados sensíveis no exato momento em que são coletados. A margem para erro é mínima, e a necessidade de robustez, confiabilidade e justiça algorítmica é máxima.

Pense em um **carro autônomo em alta velocidade**: cada decisão que ele toma, baseada em sua "visão" computacional, deve ser impecável. Não há tempo para reflexão ou correção manual. Isso exige que os algoritmos sejam não apenas precisos, mas também transparentes em suas limitações e capazes de operar de forma ética mesmo em cenários ambíguos.

Construindo um Futuro Ético para a Visão Computacional

A jornada pela ética em Visão Computacional nos mostrou que a tecnologia é um reflexo de quem a cria e como ela é utilizada. Os vieses nos dados, as preocupações com a privacidade e a necessidade de responsabilidade não são obstáculos intransponíveis, mas sim convites para um desenvolvimento mais consciente e humano. Construir um futuro ético para a Visão Computacional exige uma abordagem multidisciplinar, que combine a excelência técnica com a sensibilidade social e a compreensão dos direitos humanos.

Questionar

Sempre avaliar criticamente os sistemas e seus impactos

Auditar

Implementar verificações rigorosas de vieses e privacidade

Projetar com Empatia

Considerar o impacto humano em cada decisão de design

Advogar

Promover regulamentações justas e práticas éticas

Isso significa que, como futuros profissionais da área, vocês não são apenas programadores ou engenheiros; são também arquitetos de um futuro. A responsabilidade de questionar, de auditar, de projetar com empatia e de advogar por regulamentações justas recai sobre cada um de vocês. A ética não é um adendo, mas um pilar fundamental em todas as etapas do ciclo de vida de um sistema de Visão Computacional, desde a concepção até a implementação e o descarte.

> Pense na Visão Computacional como um **jardim que precisa de cuidado constante**: ele pode florescer com inovações incríveis, mas também pode ser invadido por ervas daninhas se não for cultivado com atenção e propósito. Ao abraçar os princípios da ética, da justiça e da privacidade, podemos garantir que a Visão Computacional seja uma ferramenta poderosa para o progresso, beneficiando a todos e construindo um mundo mais equitativo e seguro.

Consolidação e Próximos Passos

Nesta aula, exploramos as complexas interseções entre a Visão Computacional e a ética, focando nos vieses algorítmicos, nas questões de privacidade e na responsabilidade inerente ao desenvolvimento e uso dessas tecnologias. Vimos como os dados enviesados podem levar a discriminação, como a vigilância pode erodir a privacidade e a importância da regulamentação e das tecnologias de preservação da privacidade. Discutimos também como as tendências atuais, como ViTs e IA Generativa, trazem novos desafios éticos.

Em prática

Ao desenvolver ou avaliar um sistema de Visão Computacional, sempre questione a origem e a diversidade dos dados de treinamento. Considere as implicações de privacidade para os usuários e busque implementar tecnologias de proteção. Lembre-se de que a responsabilidade ética é compartilhada e deve ser integrada desde o design até a implantação.

Autoavaliação

1. **Qual das seguintes opções melhor descreve a principal causa de vieses em sistemas de Visão Computacional?**
   - a) Falhas de hardware nos servidores de treinamento.
   - b) A falta de diversidade e representatividade nos datasets de treinamento.
   - c) Erros de sintaxe na linguagem de programação utilizada.
   - d) A complexidade excessiva dos modelos de Deep Learning.
2. **Um sistema de reconhecimento facial apresenta uma taxa de erro significativamente maior para mulheres e pessoas de pele escura. Este cenário é um exemplo direto de:**
   - a) Superajuste (overfitting) do modelo.
   - b) Um ataque de envenenamento de dados.
   - c) Viés algorítmico e suas consequências sociais.
   - d) Uma falha na otimização da rede neural.
3. **Qual tecnologia visa permitir que modelos de IA sejam treinados em dados descentralizados, sem a necessidade de centralizar informações sensíveis?**
   - a) Criptografia de chave pública.
   - b) Aprendizado federado.
   - c) Blockchain.
   - d) Realidade aumentada.
4. **A principal preocupação ética associada à IA Generativa (como GANs e Modelos de Difusão) na criação de imagens é:**
   - a) O alto custo computacional para gerar imagens.
   - b) A dificuldade em obter direitos autorais para as imagens geradas.
   - c) O potencial para criação e disseminação de deepfakes e desinformação.
   - d) A limitação da criatividade humana por máquinas.

Gabarito

1. b) | **2.** c) | **3.** b) | **4.** c)

Questão Discursiva

> Discuta como a necessidade de regulamentação e a implementação de tecnologias de preservação da privacidade podem coexistir com o avanço da inovação em Visão Computacional, utilizando exemplos práticos de como esses elementos se complementam para construir um futuro tecnológico mais ético.

Próxima Aula

O Futuro da Visão Computacional e Próximos Passos

Na Aula 41, exploraremos as tendências emergentes, as inovações que moldarão a próxima década da área e como você pode continuar aprimorando suas habilidades e conhecimentos neste campo dinâmico.

Recursos Adicionais

📚 Artigos de Pesquisa sobre Fairness em AI

Para aprofundar nos métodos de mitigação de vieses

⚖️ Documentação da LGPD/GDPR

Para entender os aspectos legais da privacidade de dados

🌍 Relatórios sobre Ética em IA da UNESCO

Para uma perspectiva global e filosófica

NOTA IMPORTANTE: As informações regulatórias/legais/técnicas desta aula estão atualizadas até 2025. Consulte sempre fontes oficiais para verificar alterações.