A inteligência artificial e a potencialização das fraudes em geral

O uso da inteligência artificial (IA) tem se expandido rapidamente em diversos setores da sociedade, promovendo inovações e otimizando processos em áreas que vão desde a saúde até a exploração espacial. Existem muitos potenciais positivos da IA para os direitos humanos, especialmente das IAs generativas, que fazem cada vez mais parte da vida cotidiana.

Para Volker Türk, Alto Comissário das Nações Unidas para os Direitos Humanos, "a IA tem potencial para proporcionar enormes benefícios à humanidade", pois é capaz de "melhorar as previsões estratégicas, democratizar o acesso ao conhecimento, aumentar o ritmo dos avanços científicos e incrementar a capacidade de processar enormes quantidades de informação." Türk tem razão quando afirma ser necessário integrar "os direitos humanos ao longo de todo o ciclo de vida da IA" para que seus riscos sejam minimizados.

A utilização correta da IA pode contribuir para o desenvolvimento socioeconômico, a prevenção da criminalidade, a gestão de inteligência de segurança pública e de provas criminais, a redução das desigualdades sociais, a preparação da defesa civil para catástrofes naturais e a prevenção de fraudes.

Podemos fazer uma breve lista de usos positivos neste campo, começando pelo monitoramento dos direitos humanos, uma vez que a IA pode detectar, acompanhar e notificar violações dos direitos humanos em grande escala ou perceber movimentações fraudulentas.

No campo do acesso à justiça, sistemas de IA auxiliam a identificação e processamento de casos de violações de direitos humanos ou de condutas ilícitas. Quando levamos em conta a educação em direitos humanos, as plataformas de IA podem divulgar conhecimento sobre direitos fundamentais a populações vulneráveis e podem ajudar as pessoas a prevenir sua própria vitimização.

No quesito acesso à informação, as IA auxiliam o trabalho dos órgãos de defesa dos direitos humanos, das agências de defesa do consumidor e dos órgãos de proteção ao crédito. Pode-se empregar estas tecnologias para aumentar a eficiência e a produtividade dos sistemas nacionais e regionais de proteção à pessoa humana, tornando mais rápida e mais precisa a coleta, o processamento e a análise de dados, eliminando e dando sentido a enormes quantidades de informações num breve instante.

Spacca

Não se pode esquecer da capacidade preditiva das IA, qualidade que pode ajudar governos e empresas a prever potenciais violações dos direitos humanos, práticas anticoncorrenciais e outras condutas ilícitas através da análise de padrões e tendências. No tópico mais sensível dos direitos humanos, a capacidade preditiva das IA pode ser especialmente útil em zonas de conflito ou em situações em que existe risco de genocídio ou violência étnica.

Foro antifraude

Muitos destes temas foram discutidos no *I Foro Internacional Antifraude*, que o *Ties Group* promoveu nos dias 20 e 21 de março de 2024 em Brasília. Esta parceria público-privada reuniu autoridades federais, estaduais e distritais, representantes de entidades internacionais, profissionais da advocacia e do setor empresarial, além de acadêmicos e organizações não governamentais. Na condição de coordenador científico do Foro, ao lado do advogado Antenor Madruga, me coube presidir o painel de diálogo intersetorial dedicado justamente às fraudes por meio de IAs. Dividi esta tarefa com o consultor legislativo e advogado Marcelo Cavali.

Partimos da premissa de que, apesar de seus inúmeros proveitos, a IA apresenta severos riscos para os direitos humanos, para a integridade da Administração Pública e para um ambiente seguro de negócios. Por exemplo, sistemas de IA mal concebidos ou mal utilizados podem levar à discriminação, à invasão de privacidade, a violações dos direitos humanos, à exploração de posições anticoncorrenciais, à sonegação fiscal e à supressão de posições de trabalho.

A implementação de sistemas de IA sem as devidas salvaguardas e considerações éticas tem o potencial de causar consequências indesejadas de maneira pervasiva, por todos os ambientes do mercado e da gestão pública, exacerbando as desigualdades sociais, violando os direitos humanos e atravancando o desenvolvimento econômico sustentável.

De fato, como acontece com qualquer tecnologia poderosa, a IA também pode ser utilizada para fins nefastos, incluindo a prática de fraudes de toda ordem. A capacidade da IA de aprender, adaptar-se e executar tarefas com eficiência sobre-humana torna-a uma ferramenta valiosa para os fraudadores, que buscam explorar vulnerabilidades do sistema financeiro, de plataformas de *e-commerce* e do setor industrial.

Fraudes assistidas por IA podem assumir diversas formas, incluindo a criação de *e-mails* e mensagens de *phishing* mais convincentes, utilizando processamento de linguagem natural para imitar o estilo de escrita de indivíduos específicos e conduzir *BEC scams (Business Email Compromise)* bem-sucedidos. Além disso, a IA pode ser usada para gerar *deepfakes* — vídeos e áudios falsificados extremamente realistas — para manipular a opinião pública e os consumidores, extorquir pessoas ou realizar qualquer

outra fraude que depende de identificação pessoal positiva.

A automatização e massificação dessas atividades fraudulentas com o uso de IA permite a realização de ataques em larga escala e com uma precisão que seria impossível para fraudadores humanos em sua faina criminosa artesanal.

Os novos sistemas de IA também servem a outros objetivos nefastos, na criação de material sintético retratando abuso sexual infantil, destinado a alimentar redes de pedófilos em todo o mundo. Prestam-se também a produzir conteúdo fraudulento sobre candidatos, autoridades estatais e o sistema eleitoral, com o fim de desestabilizar democracias e influir negativamente sobre a vontade dos eleitores.

Desafios significativos

A complexidade e a adaptabilidade das ferramentas de IA também representam desafios significativos para a detecção e a prevenção de fraudes. Sistemas de segurança cibernética tradicionais muitas vezes não são capazes de identificar ou bloquear ataques orquestrados com o auxílio de IA, uma vez que essas ferramentas podem aprender e se ajustar para contornar barreiras tecnológicas.

Isso exige um contínuo aprimoramento das tecnologias de detecção de fraudes e da presença de outras IAs, muitas das quais também precisarão utilizar IAs avançadas para identificar padrões suspeitos de comportamento e neutralizar tentativas de fraude em tempo real.

Como disse a Vice-Procuradora-Geral Lisa Monaco, do Departamento de Justiça dos Estados Unidos, "fraude mediante o uso de IA ainda assim é fraude; formar carteis mediante IAs ainda assim é formação de cartel; manipulação de mercados mediante IAs ainda assim é manipulação de mercados." Essas condutas podem ser atribuídas a pessoas em particular e, nos casos permitidos em lei, a pessoas jurídicas.

Crimes corporativos, crimes tributários, delitos contra o sistema financeiro, delinquência industrial, violações de direitos de autor, infrações contra consumidores e contra o mercado de capitais podem ser amplificados com o uso de IA. É preciso o quanto antes que existam medidas regulatórias para prevenir danos vultosos e prejuízos astronômicos à sociedade, inclusive com a responsabilidade penal de pessoas jurídicas.

É preciso, também, que as agências estatais de fiscalização e controle comecem a verificar se os programas de *compliance* das entidades que atuam nos setores por elas regulados abordam os riscos das IAs em suas atividades. A introdução de uma abordagem das IA baseada em risco (*risk-based approach*) deve ser levada em conta na aferição da responsabilidade administrativa e civil de empresas que as utilizem em sua atividade econômica.

Legislação penal

Por outro lado, em uma futura legislação penal, o emprego de IAs para a prática de criminalidade de massa deve ativar causas específicas de aumento de pena para seus artífices, sejam eles pessoas físicasou jurídicas. Não discutiremos a personalidade jurídica (e a responsabilidade) de robôs; ao fim do diaquem responde pelos danos são as empresas e as pessoas naturais, e não inteligências artificiais.

A disseminação dos sistemas de IA já é enorme. Como será o mundo quando tais tecnologias estiverem espalhadas por todos os cantos do mundo, em todas as atividades humanas? Este dia é inevitável e, com seus bônus e ônus, ocorrerá por volta de 2040, o que nos faz pensar no risco da existência de uma sociedade de pleno controle e vigilância, uma sociedade orwelliana, e num mundo de muitos delitos potencializados por IA, no qual será muito fácil ver a supressão de direitos fundamentais e a causação de prejuízos econômicos e muito difícil escapar da opressão tecnológica e dos custos dessas atividades criminosas facilitadas por tecnologia.

Diante de tais riscos, não há como não lembrar de Chaplin, em sua crítica social ao império das máquinas, ao graal da produtividade e à desumanização do homem em *Tempos Modernos.* Para que não cheguemos a cenários de apocalipse tecnológico, como os descritos em *Terminator,* ou de totalitarismo digital, como o retratado em *1984*, ou num governo por máquinas, precisamos garantir uma abordagem humano-cêntrica em todo o ciclo das IAs. Para isso, é necessário regulação.

Normas setoriais e confinadas no tempo, como a resolução do TSE sobre o emprego de IA na propaganda eleitoral, ou o ato do CNJ sobre a utilização de IAs no Poder Judiciário não são suficientes para lidar com os imensos desafios que se apresentam. A União Europeia já deflagrou sua jurisdição prescritiva e aprovou a versão final do que virá a ser a primeira Lei de Inteligência Artificial do mundo, com um escopo realmente abrangente, para além do que se vê na China ou noutras iniciativas domésticas mais limitadas.

Desde o Marco Civil da Internet (MCI), o Congresso deve um tratamento conglobante do impacto penal e civil das novas tecnologias. O projeto de lei apresentado na Câmara Alta pelo senador Rodrigo Pacheco é uma boa oportunidade de debate, tendo como norte o direito de Bruxelas e a principiologia e os padrões éticos no manejo de IA já instituídos pela OCDE, pela Unesco e os propostos por organizações não governamentais. Se a IA pode ser um veneno para importantes valores da pós-modernidade, ela também é o antídoto para os grandes desafios do presente e do porvir.

Date Created
27/03/2024