

A experiência virou o verdadeiro luxo

O conceito de luxo sempre esteve associado à exclusividade. Produtos raros, marcas de prestígio, objetos difíceis de conquistar e bens que simbolizavam status eram vistos como as maiores aspirações de consumo. Hoje, essa lógica começa a dar lugar a uma nova percepção de valor

Glaucia Fernandes (*)

Em um mundo onde praticamente tudo está a poucos cliques de distância, o verdadeiro luxo vem deixando de ser apenas aquilo que possuímos e está se tornando aquilo que vivemos. Essa mudança é especialmente evidente entre as novas gerações de consumidores. Inclusive, pesquisas conduzidas pela Mastercard mostram que a maioria dos brasileiros prefere investir em experiências a adquirir bens materiais. Isso significa que, mais do que comprar, as pessoas querem sentir, querem compartilhar momentos, construir memórias e viver histórias que permaneçam muito além do instante do consumo.

Essa transformação representa uma grande oportunidade para empresas de diferentes setores. Afinal, quando falamos em experiência, não estamos nos referindo apenas a entretenimento ou turismo, mas a toda interação entre pessoas e marcas. A experiência começa antes mesmo da compra e continua depois que ela termina. Na gastronomia essa realidade se torna ainda mais evidente.

Durante a pandemia, aprendemos o valor da conveniência. O delivery aproximou os restaurantes dos consumidores e mostrou que tecnologia e eficiência podem caminhar juntas. Porém, aprendemos uma outra importante lição: uma refeição pode ser entregue em casa, a experiência não. Isso, porque nenhuma embalagem consegue transportar o olhar acolhedor de quem recebe o cliente, o ambiente cuidadosamente preparado, a conversa ao redor da mesa, o tempo desacelerado,



Vista Separada, CANVA

o aroma que antecede o primeiro prato e pode despertar memórias afetivas, a surpresa da sobremesa, a celebração de uma conquista, o reencontro entre amigos, aquele jantar que, anos depois, continua sendo lembrado.

É justamente nesse conjunto de detalhes que nasce aquilo que considero o verdadeiro luxo contemporâneo. O mais curioso de tudo é que ele é acessível. Não depende de ostentação, não exige formalidades, tampouco está necessariamente relacionado ao preço da conta. Esse luxo está na capacidade de uma marca fazer alguém sentir que aquele momento foi especial.

É interessante, que esse movimento também muda a forma como as empresas precisam construir seus negócios. Durante muitos anos, a qualidade do produto foi suficiente para gerar diferenciação. Depois, vieram preço e conveniência. Hoje, esses fatores continuam importantes, mas deixaram de ser exclusivos. A tecnologia democratizou processos, que a inteligência artificial tende a democratizar ainda mais.

Produtos podem ser copiados, cardápios podem ser semelhantes, processos podem ser automatizados, mas as experiências continuarão sendo únicas. É por isso que tantas empresas passaram a investir em hospitalidade, atendimento, personalização e cultura organizacional.

A experiência não acontece por acaso. Ela nasce da forma como uma equipe é treinada, da autonomia concedida aos colaboradores, da cultura construída diariamente dentro da empresa, da atenção aos pequenos detalhes, do propósito compartilhado entre todas as pessoas envolvidas naquela operação. No setor de alimentação, por exemplo, isso significa compreender que servir um prato é apenas parte da entrega.

O cliente não escolhe um restaurante exclusivamente pela comida, mas pelo ambiente onde deseja comemorar um aniversário, pelo local onde fará um pedido de casamento, pela mesa em que reunirá a família depois de muito tempo, pelo espaço no qual fechará um importante negócio ou simples-

mente pelo desejo de transformar uma noite comum em uma lembrança especial. Em outras palavras, restaurantes deixaram de vender apenas refeições e passaram a entregar cenários onde histórias acontecem.

Esse entendimento também traz benefícios concretos para os negócios. Afinal, marcas que constroem experiências memoráveis tendem a aumentar a fidelização dos clientes, fortalecer sua reputação, gerar recomendações espontâneas, reduzir a dependência de promoções baseadas exclusivamente em preço e desenvolver conexões emocionais muito mais duradouras. Além disso, os colaboradores costumam se sentir mais engajados quando entendem que seu trabalho vai além da execução operacional e participam diretamente da construção dessas experiências.

Em um mercado cada vez mais competitivo, essa percepção faz diferença. Acredito que quanto mais automatizado se torna o mundo, maior passa a ser o valor das experiências genuinamente humanas. E, talvez, este seja o maior desafio - e também a maior oportunidade - para as empresas nos próximos anos: utilizar toda a eficiência proporcionada pela tecnologia para dedicar ainda mais tempo ao que nenhuma inovação será capaz de substituir, que é fazer as pessoas se sentirem acolhidas, valorizadas e felizes.

(*) **Diretora executiva do L'Entrecôte de Paris, rede de restaurantes fine dining que faz parte do Grupo SMZTO, é reconhecida por inovar no Brasil com o conceito de prato único e proporcionar a verdadeira experiência vivida nos mais tradicionais bistrôs parisienses - www.lentrecotedeparis.com.br/ @lentrecotedeparis.**

O vínculo de emprego e a uberização na mira do STF

Matheus Krizanowski (*)

empresa.

Uma decisão que reconheça automaticamente o vínculo em todos os casos parece pouco compatível com a diversidade dos modelos de plataforma. Ao mesmo tempo, a ausência de parâmetros uniformes mantém empresas e trabalhadores expostos a interpretações divergentes. A solução mais prudente tende a estar na fixação de critérios objetivos, capazes de orientar a análise de cada caso concreto.

A escala do mercado brasileiro aumenta o peso da decisão. Segundo dados atribuídos à fintech GigU, o Brasil concentra 1,4 milhão de motoristas cadastrados na Uber, o maior volume entre os países em que a plataforma atua. Em uma estimativa global de 7,8 milhões de condutores inscritos, quase 18% estariam no mercado brasileiro.

O caso será analisado no Tema 1291, a partir do Recurso Extraordinário 1.446.336, sob relatoria do ministro Edson Fachin. A Corte deverá definir se existe, ou em quais condições pode existir, relação de emprego entre trabalhadores de aplicativo e empresas administradoras de plataformas digitais. Como a matéria tem repercussão geral, a tese deverá orientar processos semelhantes em todo o país e reduzir a dispersão de entendimentos sobre essas relações.

O processo chegou a ser incluído na pauta do plenário em junho de 2026, mas foi retirado após a aprovação da Convenção nº 193 da Organização Internacional do Trabalho, voltada ao trabalho em plataformas digitais. O STF considerou a norma internacional como fato superveniente relevante e determinou a manifestação das partes e dos amici curiae antes da retomada do julgamento, atualmente previsto para 27 de agosto de 2026.

A análise jurídica deverá partir dos elementos clássicos da relação de emprego, especialmente subordinação, pessoalidade, habitualidade e onerosidade. A dificuldade está em aplicar esses critérios a modelos nos quais o comando empresarial nem sempre ocorre por ordens diretas, chefias presenciais ou controle tradicional de jornada.

Nas plataformas digitais, parte da organização do trabalho pode ocorrer por sistemas automatizados de ranqueamento, distribuição de chamadas, avaliações, bloqueios, precificação dinâmica e definição indireta das condições de prestação do serviço. Por isso, a chamada subordinação algorítmica tende a ganhar relevância no julgamento, pois o STF deverá avaliar se esses mecanismos, quando verificados em determinado grau, podem caracterizar poder diretivo empresarial.

A liberdade formal para aceitar ou recusar corridas, escolher horários e permanecer conectado à plataforma também deverá ser examinada com cautela. Esses elementos podem indicar autonomia, mas não encerram a análise jurídica quando há outros fatores capazes de revelar controle, dependência econômica ou organização do trabalho pela

Caso o STF reconheça a possibilidade de vínculo empregatício em determinadas situações, as plataformas poderão enfrentar aumento relevante de custos, com obrigações relacionadas a férias, décimo terceiro salário, FGTS, contribuições previdenciárias, jornada, descanso e demais encargos previstos na Consolidação das Leis Trabalhistas. Também poderá haver repercussão sobre passivos retroativos em ações individuais e coletivas que discutem a natureza da relação mantida com motoristas e entregadores.

Em razão do volume de profissionais cadastrados, uma mudança de entendimento poderá pressionar a sustentabilidade financeira de alguns modelos de negócio. A depender do alcance da tese, da eventual modulação de efeitos e do número de litígios, empresas poderão ter de rever preços, regras de operação, políticas de permanência na plataforma e estruturas internas de gestão. Em hipóteses mais graves, o impacto acumulado pode gerar risco de reorganização empresarial, inclusive com discussões sobre recuperação judicial.

Para os trabalhadores, eventual reconhecimento de vínculo poderá assegurar direitos típicos da relação de emprego, como férias, décimo terceiro salário, proteção previdenciária e maior previsibilidade remuneratória. A formalização, contudo, também tende a trazer maior controle da prestação dos serviços, com regras de jornada, fiscalização, deveres disciplinares e obrigações compatíveis com o regime celetista.

Os efeitos da decisão não devem ficar restritos às grandes plataformas de mobilidade e entrega. A tese poderá influenciar outras empresas que utilizam tecnologia para intermediar serviços e organizar trabalho, ainda que atuem em setores distintos. Por isso, negócios inseridos na economia de plataformas devem revisar contratos, políticas internas, sistemas de avaliação, critérios de bloqueio, distribuição de demandas e comunicações dirigidas aos trabalhadores cadastrados.

A preparação jurídica deve envolver compliance trabalhista, gestão de riscos e documentação consistente sobre o funcionamento da plataforma. Independentemente do resultado, o julgamento mostra que novos modelos de negócio precisam operar com regras previsíveis, capazes de reduzir conflitos, proteger direitos e oferecer maior segurança para empresas e trabalhadores.

(*) **Advogado da área trabalhista do Cisco Advogados Associados.**

Segurança em ambientes de IA: quem protege a IA que protege a sua empresa?

Thiago R. de Souza (*)

A Inteligência Artificial não é mais uma tecnologia experimental, hoje ela ocupa um papel estratégico dentro das organizações. Assistentes corporativos, copilotos de desenvolvimento, agentes autônomos e chatbots já participam de atividades críticas, acessando bancos de dados, documentos internos, APIs e sistemas corporativos para apoiar decisões, automatizar processos e aumentar a produtividade. Mas essa evolução traz uma pergunta que poucas empresas ainda fazem: quem protege a Inteligência Artificial que passou a proteger o próprio negócio?

Durante anos, as estratégias de segurança concentraram esforços na proteção de servidores, redes, aplicações e identidades. Agora, um simples prompt enviado a um modelo de IA pode consultar bases de conhecimento, acessar informações sensíveis, interagir com sistemas internos e até executar ações de forma autônoma. Em outras palavras, a IA passa a integrar a superfície de ataque da organização. Não por acaso, o Gartner aponta as AI Security Platforms (AISPs) como uma das principais tendências estratégicas para 2026. Essas plataformas surgem para oferecer visibilidade, governança e controles específicos sobre aplicações de Inteligência Artificial, sejam elas desenvolvidas internamente ou contratadas de terceiros. Apesar da crescente preocupação com o tema, a maturidade das organizações ainda é limitada. Segundo um levantamento da Check Point Software Technologies (2025), 68% das empresas consideram as ameaças relacionadas à IA uma prioridade para a segurança cibernética, mas apenas 25% afirmam estar preparadas para enfrentá-las de forma eficaz.

A preocupação faz sentido. Afinal, diferentemente das aplicações tradicionais,

modelos de IA estão sujeitos a riscos próprios, como Prompt Injection, vazamento de contexto, roubo de modelos, manipulação de respostas, envenenamento de dados (Data Poisoning) e exploração de agentes inteligentes. A relevância dessas ameaças é tamanha que a Open Worldwide Application Security Project (OWASP) mantém um projeto dedicado exclusivamente aos principais riscos envolvendo aplicações baseadas em Large Language Models (LLMs), evidenciando que proteger a IA exige controles diferentes daqueles utilizados em aplicações convencionais.

Outro fenômeno que acelera esse desafio é o crescimento do chamado Shadow AI. Assim como ocorreu com o Shadow IT, colaboradores passaram a utilizar ferramentas de Inteligência Artificial por iniciativa própria para resumir documentos, revisar contratos, desenvolver códigos, produzir conteúdo e analisar informações. Muitas vezes, esse uso acontece sem qualquer política corporativa ou supervisão da área de tecnologia. O problema é que informações estratégicas acabam sendo compartilhadas com plataformas externas sem que a empresa tenha conhecimento, aumentando o risco de vazamentos, exposição de propriedade intelectual e descumprimento de requisitos regulatórios, como a Lei Geral de Proteção de Dados (LGPD).

Esse cenário mostra que proteger a IA vai muito além de restringir quem pode acessar um chatbot. Um ambiente moderno de Inteligência Artificial envolve modelos de linguagem, bases vetoriais, pipelines de treinamento, APIs, mecanismos de recuperação de contexto (RAG), agentes inteligentes, integrações com sistemas corporativos e diversas credenciais distribuídas ao longo da operação. É justamente para administrar essa complexidade que surgem as plataformas

de AI Security, capazes de centralizar monitoramento contínuo, auditoria de prompts, prevenção de vazamento de dados, gestão de identidades, detecção de comportamentos anômalos e aplicação de políticas específicas para ambientes baseados em IA.

Para equipes de Cloud Computing, DevOps e Segurança, isso representa uma mudança importante de paradigma. Práticas já consolidadas, como Zero Trust, gerenciamento rigoroso de identidades (IAM), criptografia, observabilidade e monitoramento contínuo, passam a ser complementadas por novas disciplinas, como AI Red Teaming, testes adversariais e validação permanente do comportamento dos modelos. Na prática, o DevSecOps evolui para incorporar uma camada específica voltada à proteção da Inteligência Artificial.

Mas talvez a maior mudança não seja tecnológica. Nos próximos anos, executivos precisarão responder perguntas que até pouco tempo atrás sequer existiam, como: quais modelos de IA estão sendo utilizados pela empresa? Quais dados alimentam esses sistemas? Quem pode acessá-los? Como auditar decisões tomadas por agentes inteligentes? Como garantir que essas respostas sejam confiáveis e estejam em conformidade com normas regulatórias? Afinal, proteger a IA não significa apenas evitar ataques, mas preservar a confiança nas decisões que ela apoia, proteger ativos estratégicos e garantir que a inovação continue sendo uma vantagem competitiva, e não uma nova fonte de riscos para o negócio.

E na sua empresa: alguém já sabe responder quem protege a IA?

(*) **Senior Cloud/DevOps Engineer com mais de 9 anos de experiência em infraestrutura corporativa, AWS Community Builder e detentor de múltiplas certificações AWS nos níveis Professional.**