O futuro da Inteligência Artificial no Brasil: precisamos de regras?

Com o avanço das tecnologias emergentes, em especial a Inteligência Artificial (IA), os países se depararam com a necessidade de regular o uso dessas ferramentas

A regulamentação busca equilibrar inovação e segurança, garantindo uma experiência positiva para os usuários. É claro que o tema vem carregado de muitas questões, há quem diga, por exemplo, que a regulação pode censurar a liberdade, já outros enxergam o processo como um avanço positivo.


metamorworks_CANVA

No Brasil, as tentativas de regulamentação iniciaram-se em 2021, e contaram com muitas idas e vindas ao longo dos anos até chegarmos em 2023, ano em que o Projeto de Lei (PL) nº. 2.338/2023 foi criado para discutir a norma no país. Com muitos desdobramentos, no final do último ano, o PL passou por mais uma atualização, resultando na aprovação do texto final pelo Senado Federal. Agora, a proposta segue para revisão na Câmara dos Deputados.

A versão aprovada estabelece princípios como transparência, segurança e responsabilidade, além de classificar os sistemas de IA conforme seu nível de risco. O tema ganha relevância não só pelo contexto atual, mas também pela necessidade de não passar a ideia de que a internet é "terra de ninguém". Há uma preocupação de colocar limites dentro desse ambiente que pode, sim, ser usado tanto para o bem quanto para o mal. Neste sentido, a tentativa de regular tem como principal objetivo estabelecer o que pode e não pode, o que é possível e o que não é, além de responsabilizar as empresas de tecnologia e os envolvidos, haja vista os impactos que isso pode gerar na vida das pessoas.

Quando falamos especificamente do Brasil, a população, de maneira geral, não é letrada para o assunto. Por isso, nós temos um desafio específico de educar a sociedade para compreender e lidar melhor com a tecnologia — já que muitos absorvem o que veem na internet como verdade absoluta e não possuem a crítica de identificar o que foi feito numa IA, o que gera a aplicação de vários golpes.

Sem a regulação, existem diversos riscos envolvidos, como golpes, danos à reputação, questões de segurança, privacidade, tomada de decisões com base em informações erradas e até vieses nos sistemas. Não à toa, o Tribunal Superior Eleitoral (TSE) aprovou uma resolução que estabeleceu regras para o uso da IA durante as eleições municipais de outubro de 2024, que vedou o uso de deep fakes — técnica que manipula fotos, vídeos e áudios para a criação de conteúdos falsos — além de outras medidas para permitir que os eleitores não acreditassem em materiais produzidos pela ferramenta.

Ao mesmo tempo, quanto mais restrições forem impostas à inovação, mais limitador o processo se torna — ou seja, se houver um controle excessivo, a inovação é sufocada. Por outro lado, se for totalmente liberado o uso da IA, abre-se espaço para os usos indevidos, que podem causar grandes impactos. O desafio está justamente em encontrar e estabelecer o meio termo entre controle e liberdade para garantir um uso seguro e ético do recurso.

Outro ponto de atenção é justamente referente ao papel das big techs que desempenham um papel central nesse debate, influenciando diretamente políticas públicas e regulações. Para que esse movimento de regulação aconteça, essas companhias precisam estar alinhadas e ter o que chamamos de responsabilidade social corporativa, assumindo a responsabilidade de mitigar riscos e coibir o uso indevido da IA, interceptar algo que já é reconhecido como uma deep fake ou IAs com comportamentos nocivos.

Por fim, não acredito que devemos encarar essas mudanças como uma limitação, já que toda alteração cria um ambiente de abundância e restrição. Ao longo da história, diversos momentos significativos ocorreram em nossa sociedade e, embora à primeira vista parecesse algo limitador e restritivo, empresas e pessoas souberam enxergar novas possibilidades. Este é, sem dúvida, o momento de encararmos essa nova realidade observando quais novas oportunidades serão criadas.

(Fonte: Caroline Capitani é VP de Estratégia e Inovação da ilegra,empresa global de estratégia, inovação e tecnologia).

Vazamento de dados em instituições de crédito e o afetamento direto ao consumidor

Luiz Carlos Pereira (*)

De que maneira o roubo de dados pode ser capaz de afetar a quem compra? Em novembro do ano passado, vazamentos de dados foram anunciados pela equipe de inteligência da empresa ZenoX, do Grupo Dfense, especializada em soluções baseadas em IA. Cerca de 250 mil brasileiros tiveram seus dados bancários acessados; informações, como documentos pessoais, comprovantes de endereço, números de cartões de crédito e até mesmo selfies foram utilizados para tentativas de fraudes. Infelizmente, situações como essa estão acontecendo com cada vez mais intensidade. Em relação ao PIX, por exemplo, em setembro de 2024, o Brasil teve mais de 50 mil clientes com dados vazados na Qesh, mais de 8 mil em agosto no BTG Pactual, 39 mil em julho na 99Pay, 19 mil em maio na IUGU, 46 mil em fevereiro na Fidúcia, todos no mesmo ano, além de casos menores na Caixa Econômica, Shopee, Unicred, PagCerto, Banpará e até na Sabesp, situações de fraude alastradas, tal qual uma epidemia.

Nota-se que esses são os casos em que as instituições divulgaram o incidente ou que eles foram descobertos por empresas de segurança da informação, o que não denota uma visão completa das ocorrências no setor, pois ainda há o que fica em sigilo. Além disso, a invasão para coleta de dados de clientes é apenas um dos tipos de crimes cibernéticos. Há diversas outras formas de violação de segurança, mesmo em grandes empresas. Um caso famoso é o do Google, que em maio de 2024, teve mais de 2.500 páginas de documentos internos divulgadas sem autorização. Outro exemplo de um caso bem diferente é a prisão, bem recente, de um funcionário do Ministério Público de São Paulo que estaria vazando informações sigilosas de processos para o PCC, também em novembro de 2024.

As razões das ocorrências são variadas. Na verdade, a resposta é uma combinação de fatores tecnológicos, humanos e organizacionais. Em primeiro lugar, hoje em dia as empresas guardam um volume gigantesco de informações, como nunca ocorreu na história da computação. Isso se dá, porque houve uma redução significativa no custo do armazenamento digital, uma digitalização acelerada de operações que antes eram controladas manualmente; também houve um entendimento das empresas de que dados são tão valiosos, que o conveniente é armazenar o que se tem acesso, para só depois pensar sobre o que fazer com eles. O problema é que às vezes não separam os dados sensíveis daqueles mais comuns;

Nessa condição, o que aumentou a insegurança foi o avanço das técnicas de ataque, como phishing mais sofisticado, ransomware e uma maior exploração das vulnerabilidades em softwares. Ou seja, os cibercriminosos têm práticas cada vez mais complexas e estruturadas. Não são apenas hackers solitários, mas há países onde encontraram o que poderia se chamar de "fábrica de invasões", com técnicos especialistas atuando em conjunto como uma empresa.

Além disso, um outro fator que teve um papel importante foi a maior adoção do trabalho remoto. Durante a pandemia muitas empresas ampliaram o seu acesso remoto sem reforçar adequadamente suas infraestruturas de segurança. Isso abriu mais brechas para os ciberataques.

Fatores humanos, como erros de funcionários ou práticas inadequadas, também são oportunidades exploradas pelos criminosos e a pressão para inovação nas empresas, unida ao lançamento de produtos com urgência para ultrapassar a concorrência, muitas vezes também deixa a segurança em segundo plano. Em contrapartida, está cada vez maior o uso da inteligência artificial pelos invasores.

Essa combinação de ameaças mais sofisticadas, práticas inadequadas e infraestrutura vulnerável criou um cenário onde os vazamentos de dados e outros tipos de ataques são cada vez mais frequentes; no entanto, muitas empresas só dão a devida atenção e fazem o investimento adequado em cibersegurança após sofrer a sua primeira invasão.

(*) Executivo em Operações e Tecnologia e Vice-Presidente de Tecnologia e Governança da Pagos, Associação de Fintechs de Meios de Pagamento.

Na era dos dados, gerar insights confiáveis é o novo desafio

Milton Ribeiro (*)

Vivemos a era dos dados. Diariamente, segundo a IBM, o mundo gera 2,5 quintilhões de dados

No entanto, diante dessa quantidade massiva de informações geradas, uma pesquisa da Salesforce mostra que muitos líderes não se sentem preparados para encontrar, analisar e interpretar esses registros, resultando na falta de confiança no uso desses indicadores para tomadas de decisão.

Segundo o estudo, que foi realizado com 500 líderes empresariais nos EUA, fatores desde a economia incerta até corte de custos têm gerado a demanda por insights mais precisos para orientar as estratégias da empresa. Porém, apenas metade dos participantes afirmaram que a extração de dados está alinhada com as prioridades da organização.

A pesquisa ajuda a ilustrar os desafios que os gestores enfrentam atualmente na geração de dados, relacionados principalmente à qualidade, integração e governança. Isso é, ainda hoje, muitas empresas ainda operam com sistemas legados e, com isso, armazenam dados de forma fragmentada em planilhas ou diferentes plataformas – o que dificulta a execução de um processo claro de validação e identificação da real utilidade do material coletado.

Diante desse contexto, dificilmente os dados serão confiáveis e, sem dúvida, acarretarão prejuízos para o negócio, uma vez que os líderes, ao tomarem decisões com base em suposições ou percepções parciais, podem traçar estratégias equivocadas, investimentos errados e, consequentemente, perder competitividade. E, tendo em vista que, no ambiente de negócios dinâmico atual, a agilidade e precisão são essenciais, a falta de confiança nos dados compromete diretamente a capacidade de inovar e reagir rapidamente.

Neste contexto, o que diferencia empresas que são bem-sucedidas das demais é a capacidade de transformar esses dados em valor. A pesquisa da Salesforce ainda mostra que 76% dos líderes empresariais se sentem cada vez mais pressionados a apoiar seus argumentos e afirmações em dados. Em outras palavras, esse comportamento ajuda a enfatizar a importância insights confiáveis para ajudar otimizar operações, entender clientes, reduzir riscos e antecipar tendências.

Em um cenário altamente competitivo, dados confiáveis se tornaram uma vantagem estratégica. Entretanto, ainda estamos em um momento transição, em que muitas empresas reconhecem a importância de implementar uma governança dessas informações, mas poucas implementaram, de fato, uma estrutura robusta para isso.

Sem dúvida, a tecnologia é o principal habilitador desse processo. Através de ERPs e plataforma de Business Intelligence, como exemplo, é possível centralizar e padronizar os dados, tornando-os acessíveis em tempo real e com confiabilidade. Isso porque soluções de integrações ajudam a eliminar silos, enquanto recursos de validação automatizada e dashboards visuais facilitam a interpretação e o uso prático dos dados pelos gestores.

Entretanto, de nada adianta ter recursos que ajudem na confiabilidade dos registros, sem que a cultura organizacional esteja alicerçada. Ou seja, para que a tecnologia cumpra o seu propósito, é fundamental que as pessoas confiem nos dados e saibam utilizá-los de forma correta. Para isso, as organizações também precisam realizar o trabalho de educar, capacitar e engajar os times, mostrando as razões pelas quais as decisões orientadas por dados trazem melhores resultados.

As organizações ainda têm pela frente o desafio de conseguir fazer uma gestão assertiva, identificando lacunas e pontos de melhorias para deixar os processos confiáveis. Neste aspecto, ter o apoio de uma consultoria especializada nessa demanda e na aplicação de tais recursos é um importante fator a ser considerado ao longo dessa jornada.

A confiança nos dados nasce quando há clareza, transparência e domínio técnico, o que só é possível com uma cultura forte e o foco contínuo em formação. Cada vez mais, a busca por insights confiáveis se tornará uma necessidade para que as empresas consigam obter vantagem competitiva e sobreviver em um mercado altamente dinâmico. Por isso, quanto antes começarem a se preparar, melhor, afinal, o futuro não espera e, para sair na frente, é preciso estar preparado.

(*) Co-CEO da SPS Group.