IA, Cibersegurança e privacidade: como proteger dados sensíveis na era da Inteligência Artificial Generativa

Taxa de crescimento da tecnologia na próxima década deve ser de 42% ao ano – quase dobrando seu alcance

São Paulo, novembro de 2024 – A rápida adoção da Inteligência Artificial Generativa (Gen IA) nas empresas está redefinindo processos, permitindo inovações e impulsionando a automação. Segundo estudo recente da Bloomberg Intelligence, a taxa de crescimento da IA na próxima década deve ser de 42% ao ano – quase dobrando seu alcance. No entanto, o sucesso dessas soluções depende de uma gestão cuidadosa dos dados que alimentam esses modelos. É aqui que entra a cibersegurança, elemento vital para a proteção da privacidade e da integridade das informações.

A IA Generativa vai além dos modelos tradicionais de inteligência artificial, que apenas classificam ou prevêem comportamentos, pois cria novos conteúdos como textos, imagens e códigos. Essa capacidade de inovação abre novas possibilidades em diversos setores, mas exige uma abordagem cuidadosa em relação ao uso e à segurança dos dados e isso é reconhecido pelas pessoas que usam a tecnologia no dia a dia. Segundo a pesquisa da Developer Survey 2024 da Stack OverFlow, um dos principais desafios (31,5%) de se trabalhar com IA é não ter políticas certas para mitigar os riscos de segurança.

Nesse sentido, o *Technical Product Manager* João Batista, responsável pela plataforma StackSpot AI da Zup, explica que para mitigar esses riscos, as empresas devem implementar medidas de segurança rigorosas, tendo em vista que os crimes cibernéticos estão cada vez mais sofisticados e até 2025 podem custar 10,5 trilhões de dólares, de acordo com a Cyber Security Almanac.

"Garantir que modelos de AI operem de forma segura e ética exige uma abordagem multifacetada, que combina criptografia robusta, governança de dados eficaz, práticas de privacidade rigorosas e controles de acesso restritos durante o treinamento dos modelos. Se fizermos um recorte para as empresas que criam tecnologia, ter um assistente de desenvolvimento de software impulsionado por IA treinado em segurança pode apoiar o time para garantir que o código siga as práticas recomendadas de codificação segura. Este, por exemplo, é um mecanismo preditivo de identificação de vulnerabilidade. Cada vez mais, o caminho é pensar em uma estratégia conjunta que considere inovação, segurança e proteção de dados como um tripé essencial para a aplicação desse tipo de tecnologia", ressalta João Batista.

No que tange a legislação, Henrique Flôres, cofundador da Contraktor e líder do desenvolvimento do CK Reader, IA da startup, explica que “enquanto aguardamos uma legislação para melhor regulamentar o uso da I.A. Generativa, compete aos profissionais de tecnologia zelar pela aplicação de boas práticas de criptografia, anonimização de dados e

políticas de governança de t.i. que possam garantir o equilíbrio dos interesses comerciais das partes, a transparência nos mecanismos de treinamento de algoritmos e o uso ético na manipulação dos dados".

Embora reconheça que inovar com tecnologias emergentes, como a Inteligência Artificial Generativa, seja uma oportunidade única de transformação, Giovanna Rossi, CPO da Rethink, consultoria de tecnologia, design e estratégia, reforça que não dá para negar que ela vem acompanhada por riscos significativos, como a exposição de informações sensíveis e a possibilidade de ataques cibernéticos sofisticados. "Como responsável pela área de produtos digitais, vejo o quão fundamental é a liderança priorizar uma abordagem estratégica no uso da IA para mitigar tais riscos. Temos a responsabilidade de moldar essa tecnologia de maneira ética e segura, garantindo que seu impacto seja positivo e sustentável para todos", afirma a executiva.

O Brasil tem um alto volume de dados circulando na internet e um processo de digitalização acelerado. No que se refere a proteção de marca, Diego Daminelli, CEO da BrandMonitor, empresa pioneira e especialista no combate à concorrência desleal no ambiente digital, alerta que a infraestrutura de segurança brasileira ainda caminha a passos lentos, tornando o país um dos maiores alvos de ciberataques do mundo, com uma maior sofisticação dos ataques por parte dos criminosos. "A cultura de segurança ainda é um tópico pouco valorizado por diversas empresas, que não utilizam IA e sim tecnologias desatualizadas, que podem deixá-las vulneráveis a ataques e não são capazes de monitorar a presença digital da marca em toda sua amplitude". O especialista dá o exemplo do *phishing*, grande problema para segmentos como o varejo e prestação de serviços. "Os anúncios são veiculados em plataformas digitais utilizando toda a identidade de uma marca e prometendo descontos impraticáveis. Esse anúncio leva a uma pagina que imita o layout oficial da empresa, mas com um endereço diferente. Nessa página são oferecidos produtos ou serviços com um preço extremamente baixo, induzindo o cliente a compra", finaliza.